UNIVERSITE D'ORLEANS

Towards Secure Control of Cyber-Physical Systems in the Bounded-Error Framework

Nacim RAMDANI (University of Orléans, at Bourges)

https://agora.bourges.univ-orleans.fr/ramdani

nacim.ramdani@univ-orleans.fr

27 November 2020

JNA 2020

UNIVERSITE D'ORLEANS

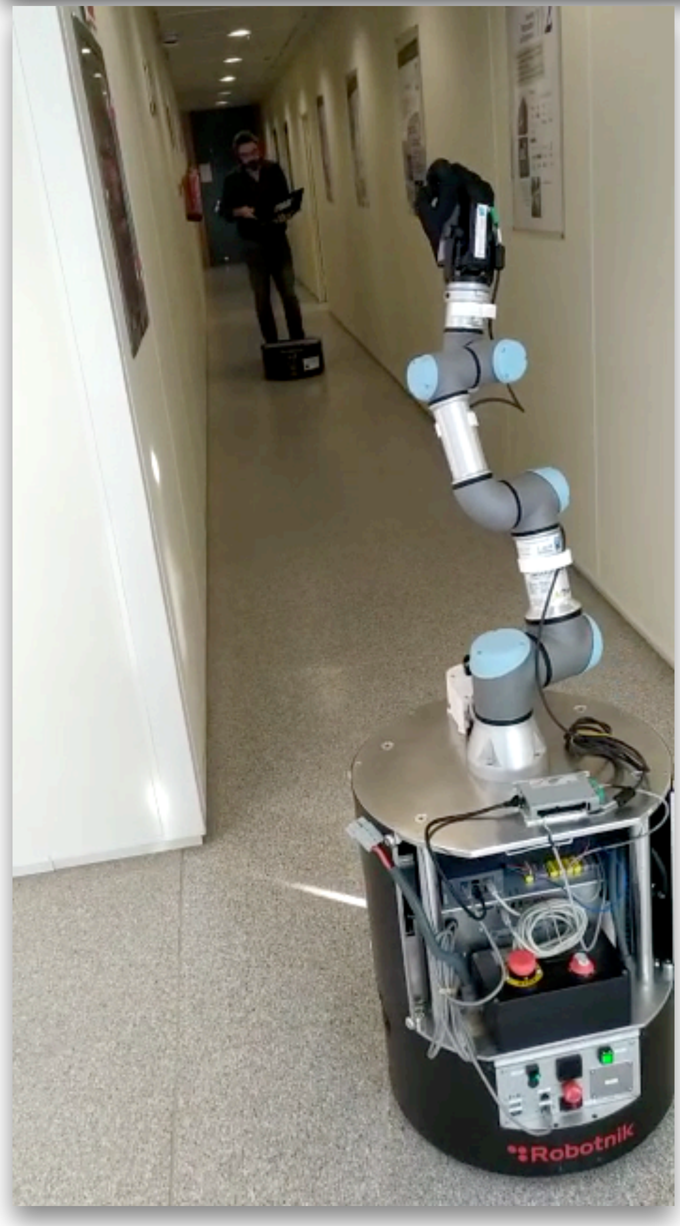
Talk Objective & Outline

- Objectives:
  - Review some of control aspects of cyber-security issues and discuss secure state estimation in the bounded-error framework

- Outline
  - Cyber-physical and network controlled systems
  - Models of cyber-attacks and mitigation strategies
  - Secure state estimation in the bounded-error framework

- **Cyber-Physical and Network Controlled Systems**

Cyber-Physical Systems

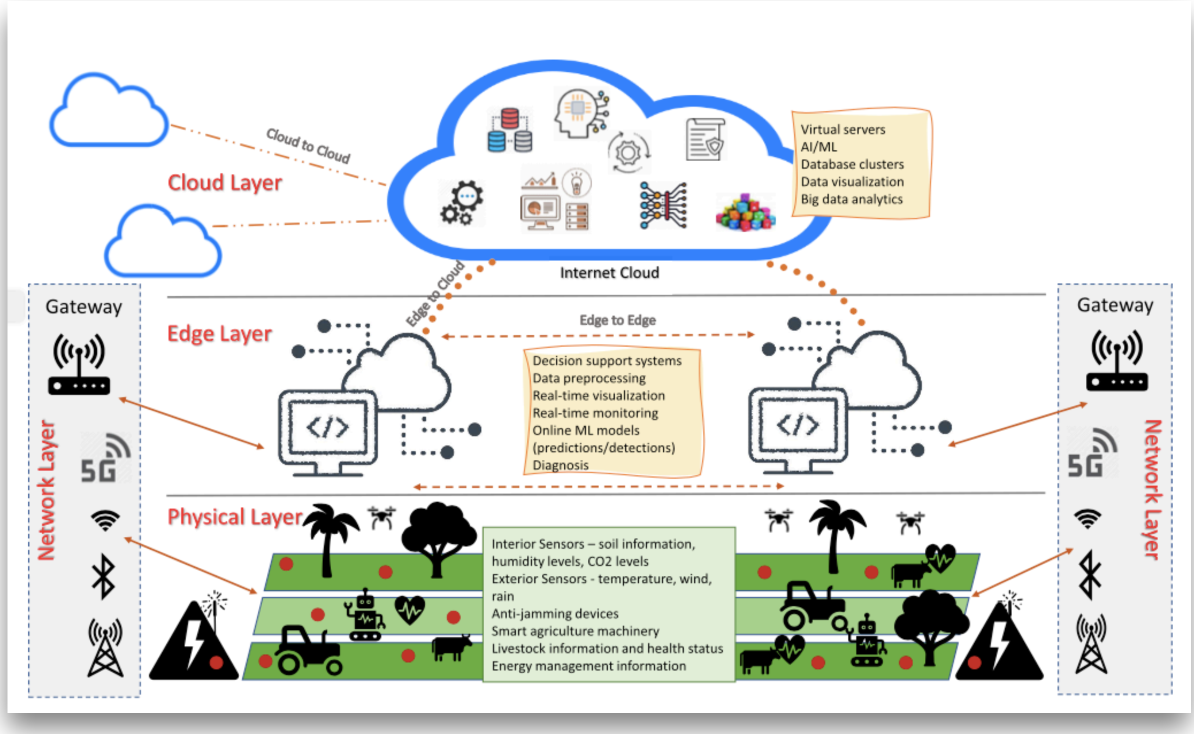


Network Control Systems
Safety-critical systems, pHRI, …

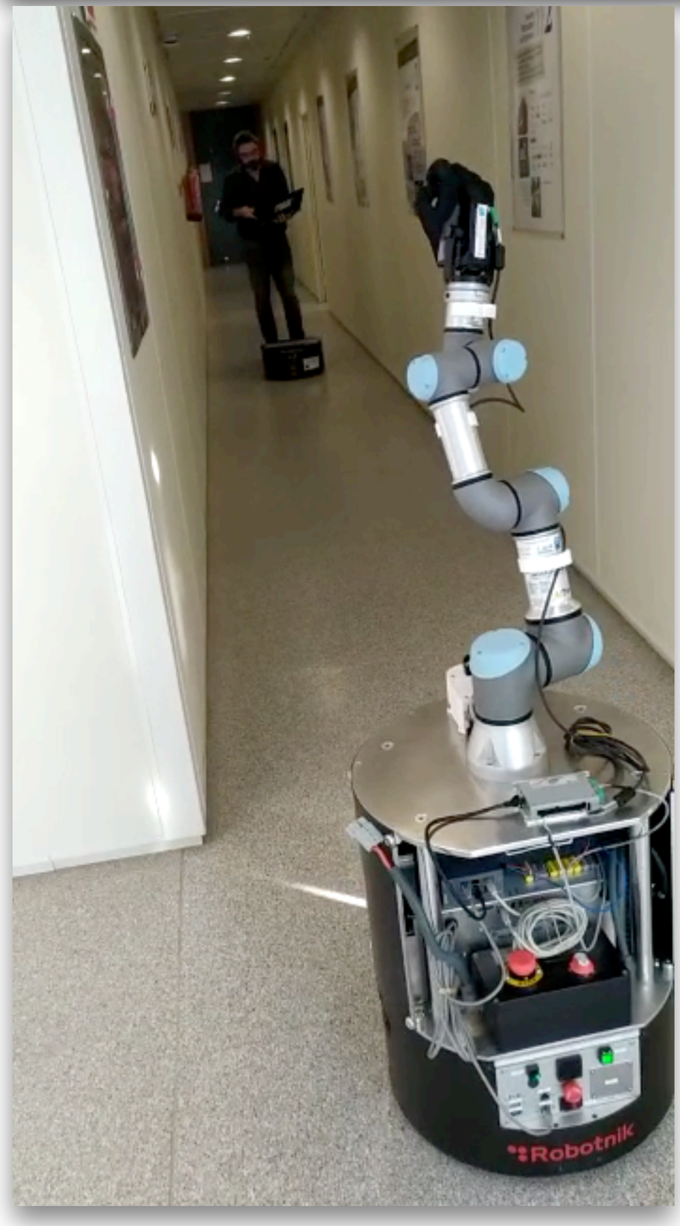
Operation in adversarial environment, requires correct-by-construction synthesis

Guarantee certificates

- Safety
- Security



Cyber-Physical Systems



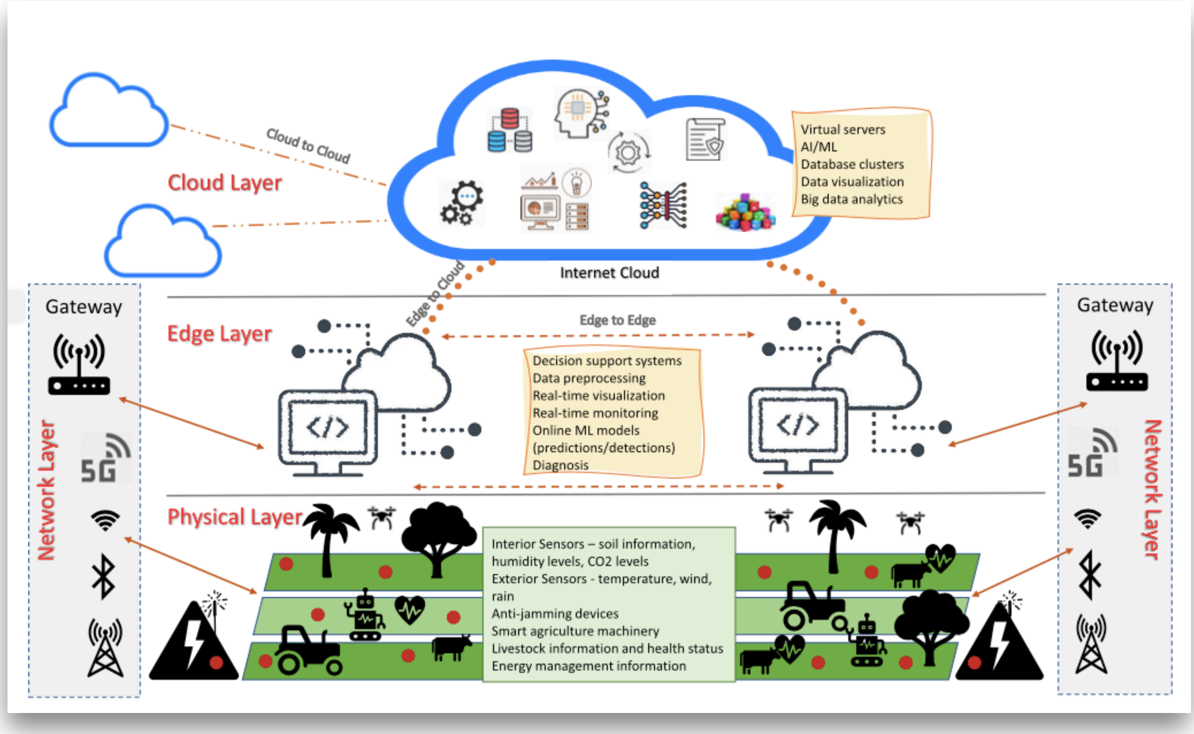
Network Control Systems

Safety-critical systems, pHRI, …

Operation in adversarial environment, requires correct-by-construction synthesis

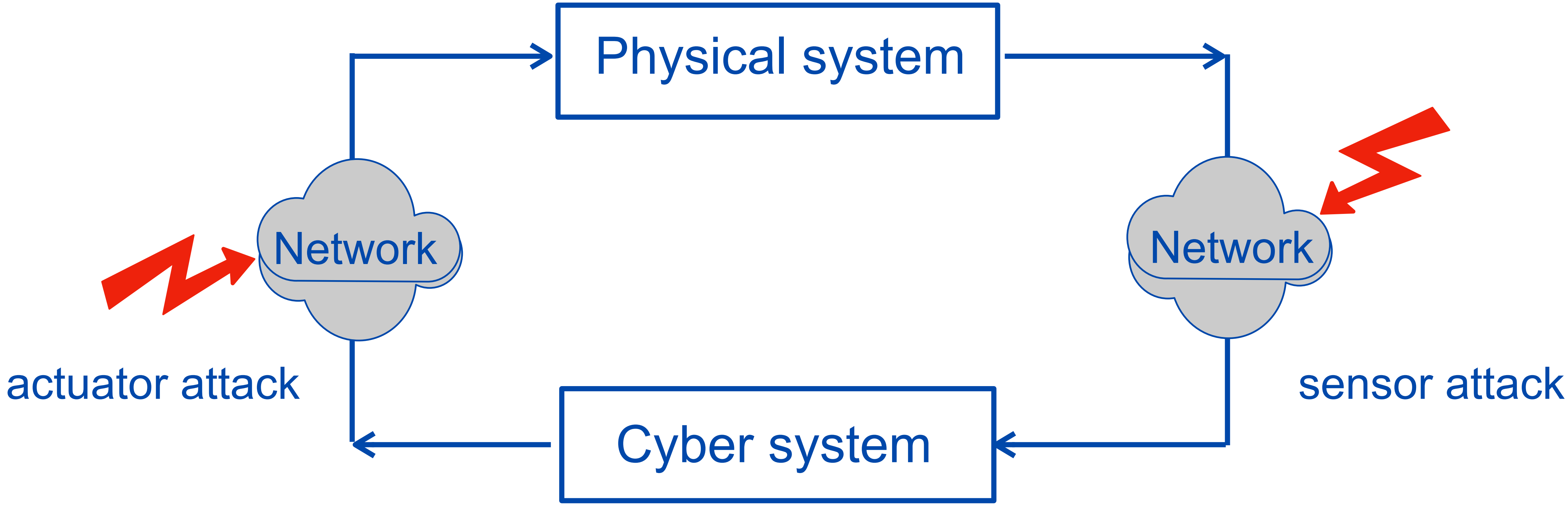
Guarantee certificates

- **Safety**
- **Security**

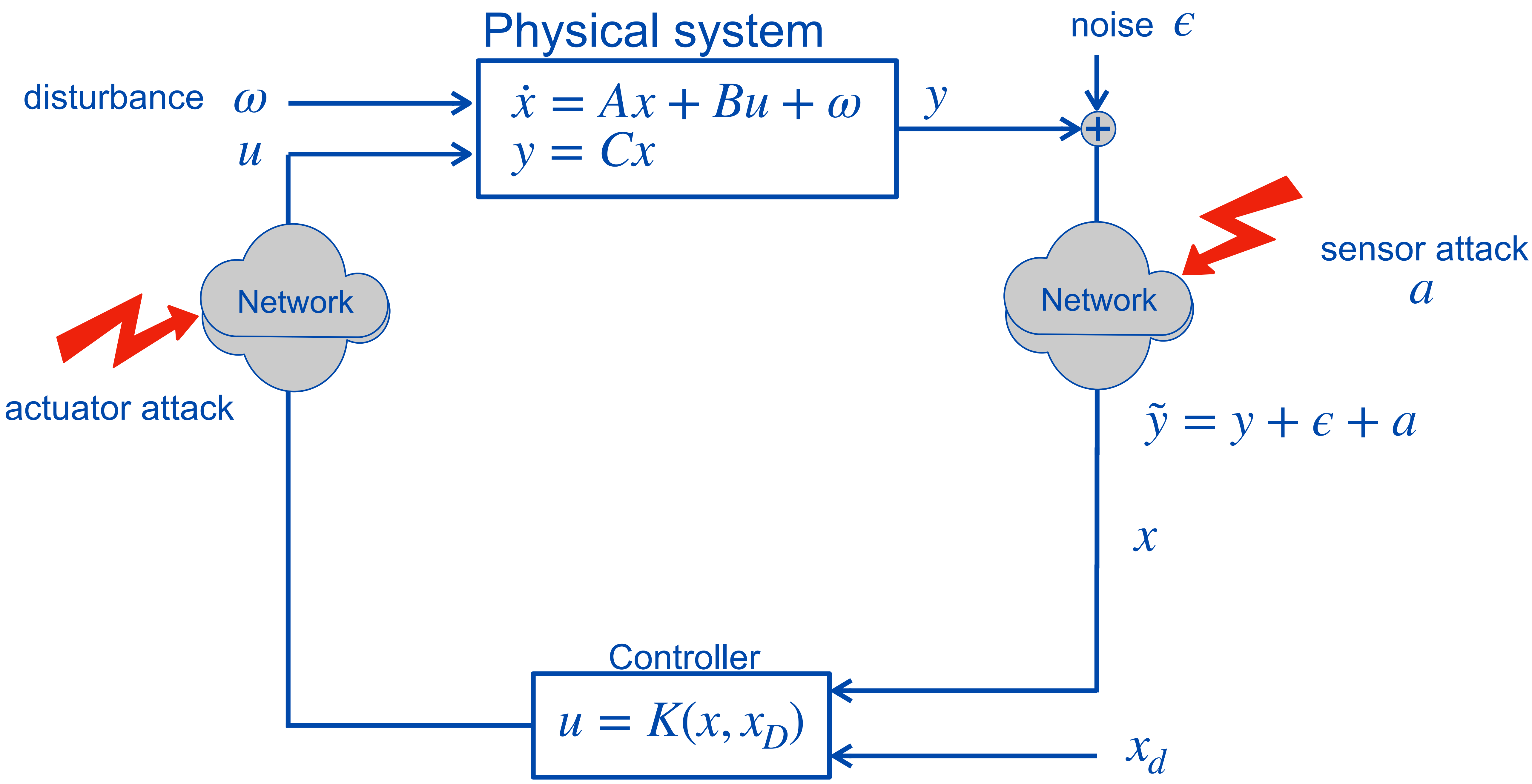


Cyber-Physical Systems

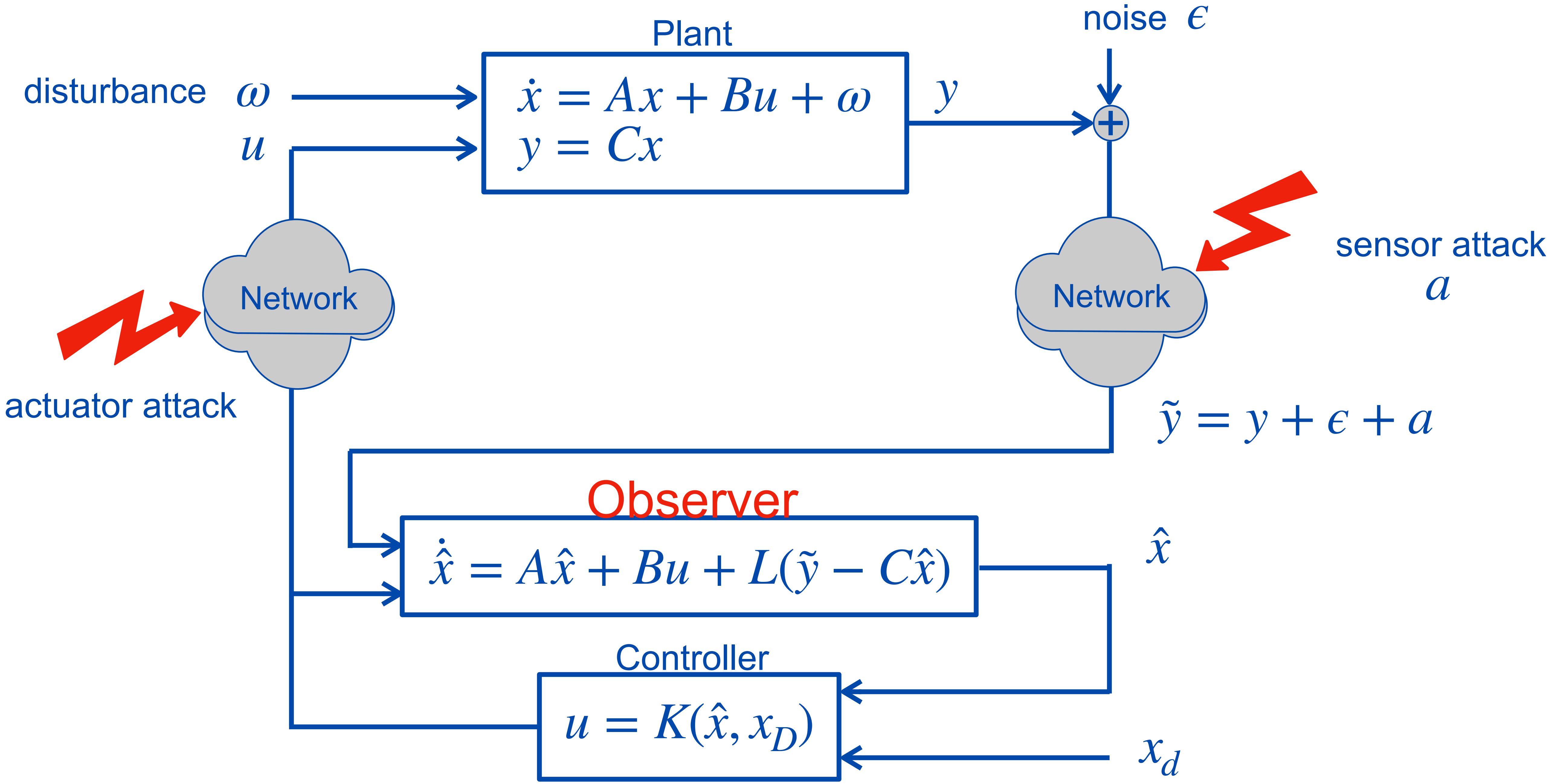
- **Networked controlled systems** are prone to **cyber-attacks**.
  - Under cyber-attacks, corrupted measurement data leads to corrupted control commands



State Feedback Control



Output Feedback Control



- **Models of Cyber-Attacks and Mitigation Strategies**

Resilient control systems

- *« Deploying proven IT security technologies into a control system is **not** an appropriate solution to mitigate the impact of cyber-attacks »*
  - [Kuipers & Fabro, 2006]
  - Retard, DoS …

- Need to develop **secure control components** for CPS, and **secure navigation solutions** for robotics systems
  - [Ding, et al., Neurocomputing 2018], [Lun, et al., J. Syst. Soft. 2019], [Debaji, et al., Annual Reviews in Control, 2019], …

Cyber-attacks

- **Disclosure** attacks => **Confidentiality** breach
  - Intrusions (eavesdropping, …) ;.

- **Deception** attacks => **Integrity** breach
  - Corruption of signals: spoofing attack, false-data or bias injection …
  - Deceptive-bias-injection attacks can remain undetected, or **stealthy** (similar to noise, or exploit zero-dynamics pathways).
    - ***Stealthy*** *attacks may be* ***characterized*** *=> robot trajectory planners or CPS controllers may be modified to design control inputs that allow the detection of any attack, with guarantee certificates [Bianchin, el al., IEEE CSL 2020]*

- **Disruption** attacks => **Availability** breach
  - Intrusion where signal is blocked or delayed, (denial of service attack, ..)

Models of cyber-attacks

Sensor attacks

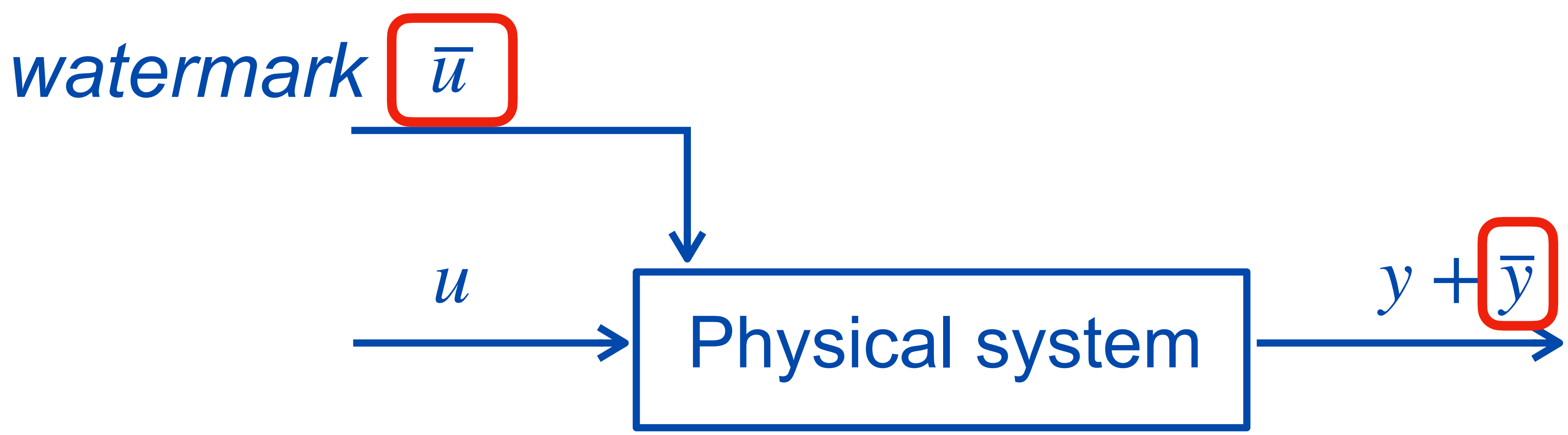
- Denial of Service (DoS) attack $y_a(t) = \varnothing$
- Replay attack $y_a(t) = y(t - T)$
- **Deception** attack $y_a(t) = y(t) + a(t)$
- **Stealthy** attack: produce plausible output signals.
  - change in output smaller than impact of noise/disturbance

Mitigation strategies I

- **Mitigation** of cyber-attacks
  - **FDI FTC** methods and algorithms are good candidates
    - [Debaji, et al., Annual Reviews in Control, 2019] …
  - Cyber-attacks <> 'Random' faults

Mitigation strategies I

- **Detection** of cyber-attacks
  - **Watermarking**-like method to improve detectability of **actuator attacks** on sUAV
  - ***Unknown input observer***
  - **Variable** frequency pulse-width modulated signals, to improve the ***resilience*** of the actuator
  - (Muniraj & Farhood, CEP, 2019)



Mitigation strategies I

Mitigation strategies I

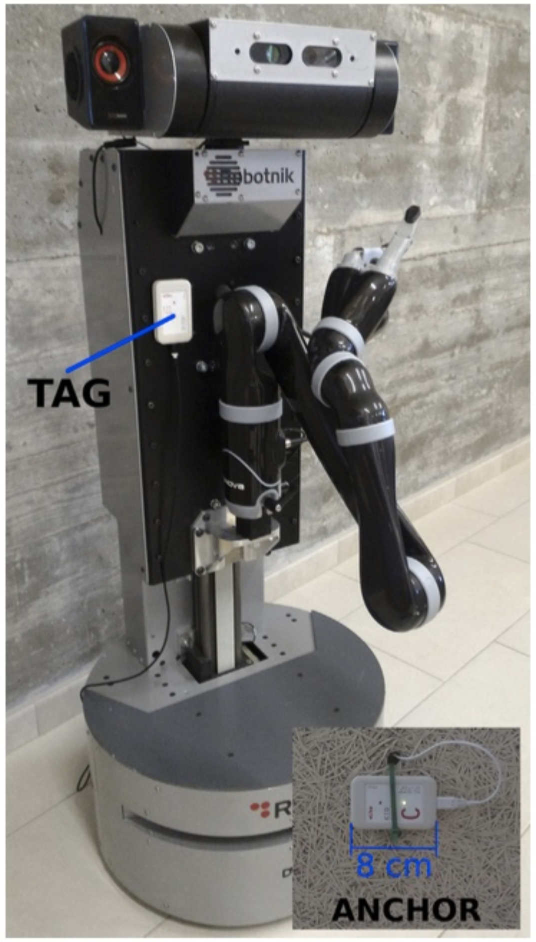
- **Detection** of cyber-attacks
  - **Classification** of measurement data in real-time localisation systems (**RTLS)**
    (Gerrero-Higueras et al., RAS, 2018.)

Detection of cyber-attacks in real-time localisation systems

(Gerrero-Higueras et al., *Robot. Autonom. Syst.* 2018.)

- **Indoor** navigation systems via **Multilateration**
  - Uses **distance** to beacons (anchors) with known position.
  - Prone to **DoS** and **spoofing** cyber-attacks on beacons.

- Detection using only data received ?
  - **Supervised learning**: Training with ground truth data, **with** and **without** cyber-attacks.
  - Machine learning techniques for **classification**
    - Test of several classifiers
  - Positive evaluation via thorough analysis of KPI (accuracy, precision, recall) from **actual data**.
  - Mixed conclusions …



Mitigation strategies II

- Control using **encrypted** data
  - Paillier encryption (semi-homomorphic encryption scheme). Control computation with encrypted data.

    *They provides **strong privacy and security guarantees** for the closed-loop system at the cost of **extra computations*** (Farokhi, et al., CEP, 2017).

Mitigation strategies III

- **Passive resilience** via **secure state estimation**
  - Directly estimate the state from the corrupted measurements, and/or altered actuation

    (Lu & Yang, Automatica 2018), (Xie & Yang, IJRNC 2018), (Shoukry & Tabuada, IEEE TAC 2016), (Shoukry, et al., ACM TCPS 2018, IEEE TAC 2018) ….

Secure State Estimation

$$\dot{x} = Ax + Bu + \omega$$
$$y_i = Cx + \epsilon_i + a_i, \quad i \in \{1,\ldots,n\}$$

- Working scenario:
  - System with ***n*** sensors,
  - up to ***s*** sensors potentially under cyber-attack,
  - but **attacked sensors are not known**.

- Secure Estimation:
  - **Reconstruct whole state vector** from ***n*** sensors under ***s***-sparse (sensor/actuator) attack vector
  - System is then ***s-sparse observable***

Secure State Estimation

$$\dot{x} = Ax + Bu + \omega$$
$$y_i = Cx + \epsilon_i + a_i, \quad i \in \{1,\ldots,n\}$$

- Theorem (Chong, et al., ACC 2015)
(Shoukry & Tabuada, IEEE TAC 2016)

System is ***s-sparse observable,*** if and only if

(i) ***n > 2s***, and

(ii) system is **observable** for any subset of ***n - s*** sensors.

Secure State Estimation

$$\dot{x} = Ax + Bu + \omega$$
$$y_i = Cx + \epsilon_i + a_i, \quad i \in \{1,\ldots,n\}$$

- Brute force algorithms are **combinatorial**:
  - Work with **bank** of $\dfrac{n!}{s!(n-s)!}$ observers

    using all possible subsets of ***s*** out of ***n*** sensors !

- Effective solution technique for MMSE
  - SMC: **Satisfiability modulo convex programming** as a new framework (Shoukry, et al., Proc. IEEE, 2018)

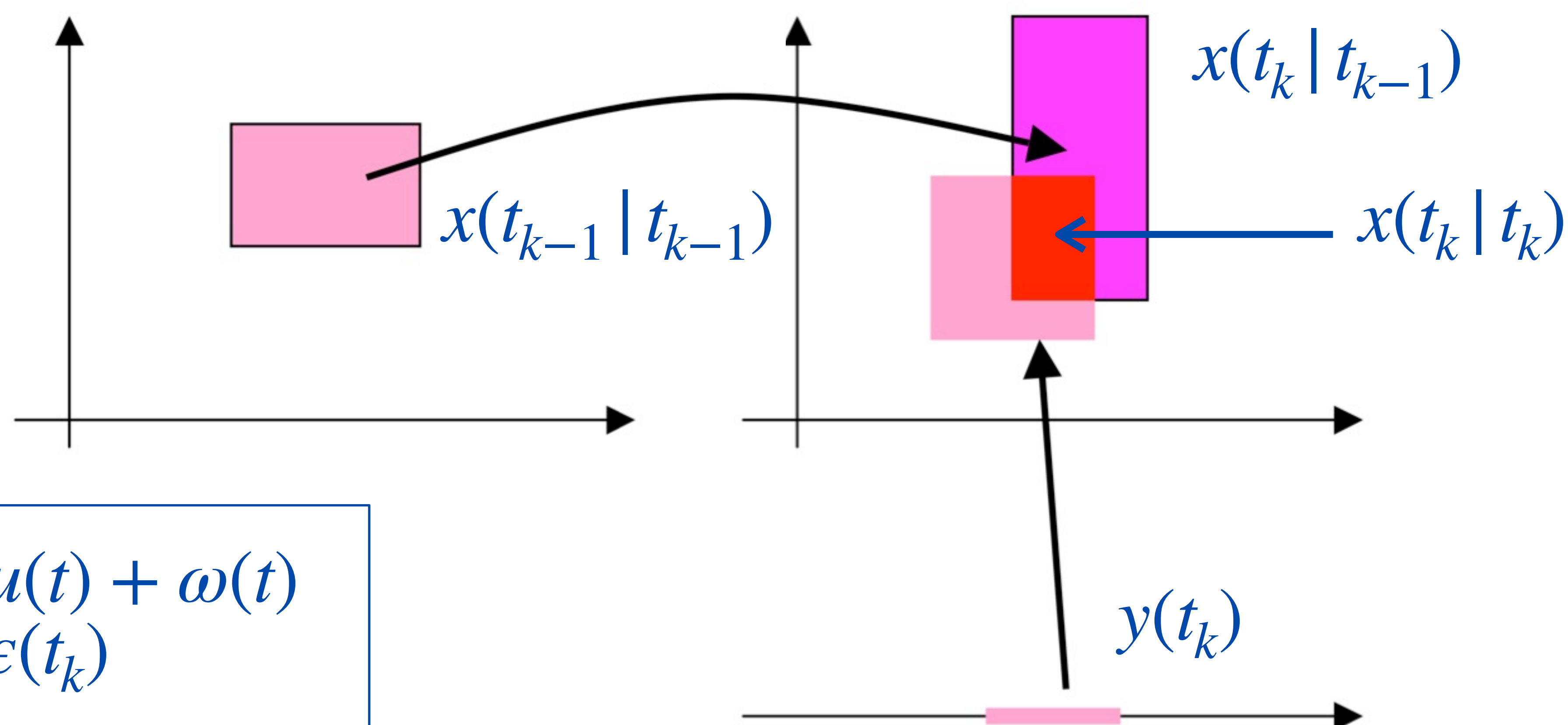
- **Secure state estimation in the bounded-error framework**

State Estimation

- State estimation the bounded-error framework
  - **Set membership predictor-corrector algorithms**
    - Can handle corrupted data as outliers.
  - **Interval observers**
    - Have been extended to handle cyber-attacks.

Predictor-Corrector Algorithms

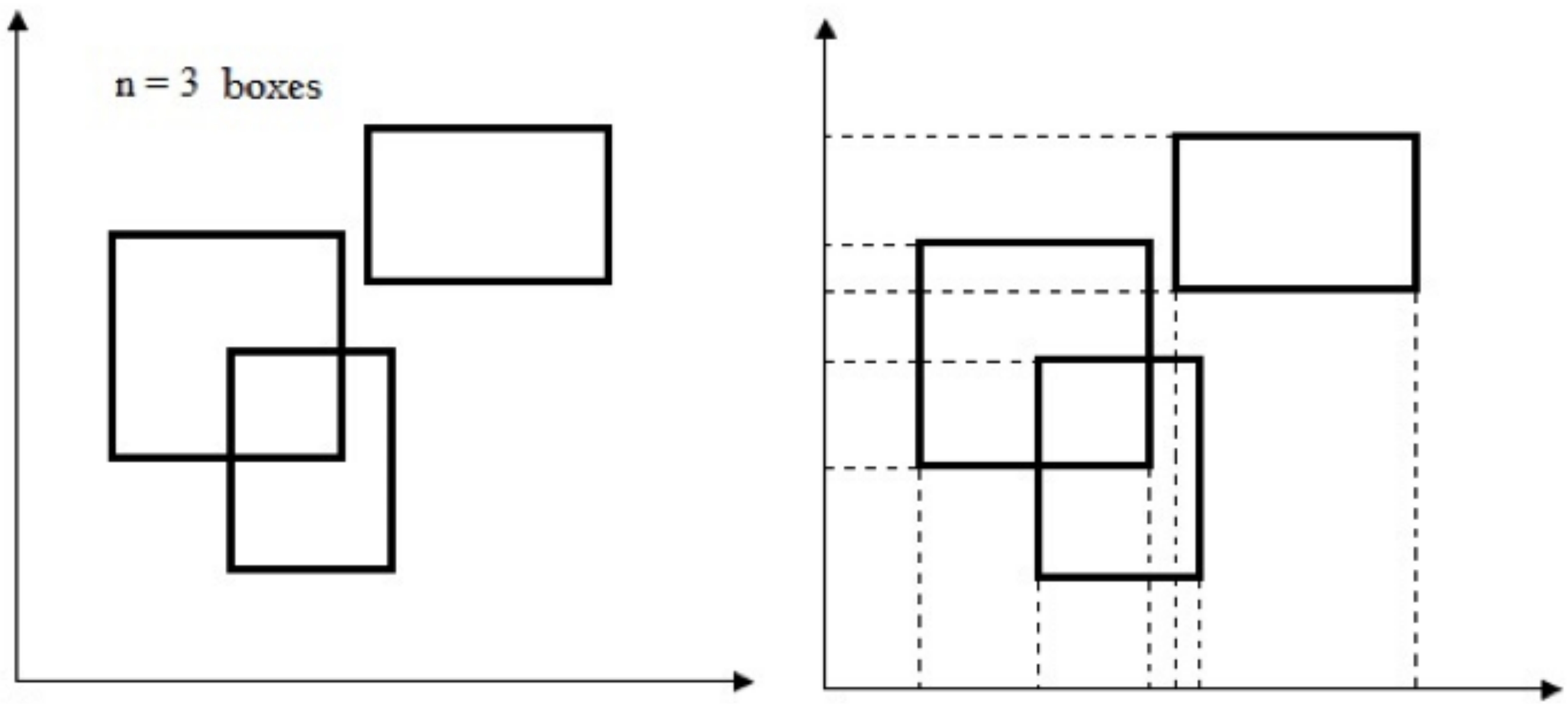
- Set membership estimation with **sampled data**
  - (Schweppe, 68) (Bertsekas & Rhodes, 71) (Kurzhanski & Vályi, 96), (Kieffer, et al., 02) (Jaulin, 02) (Raïssi et al., 04, 05) (Meslem, et al, 10), (Milanese & Novara, 11), (Kieffer & Walter, 11), (Combastel, 15) …
  - **Reachability** + **Set inversion +** Forward backward consistency



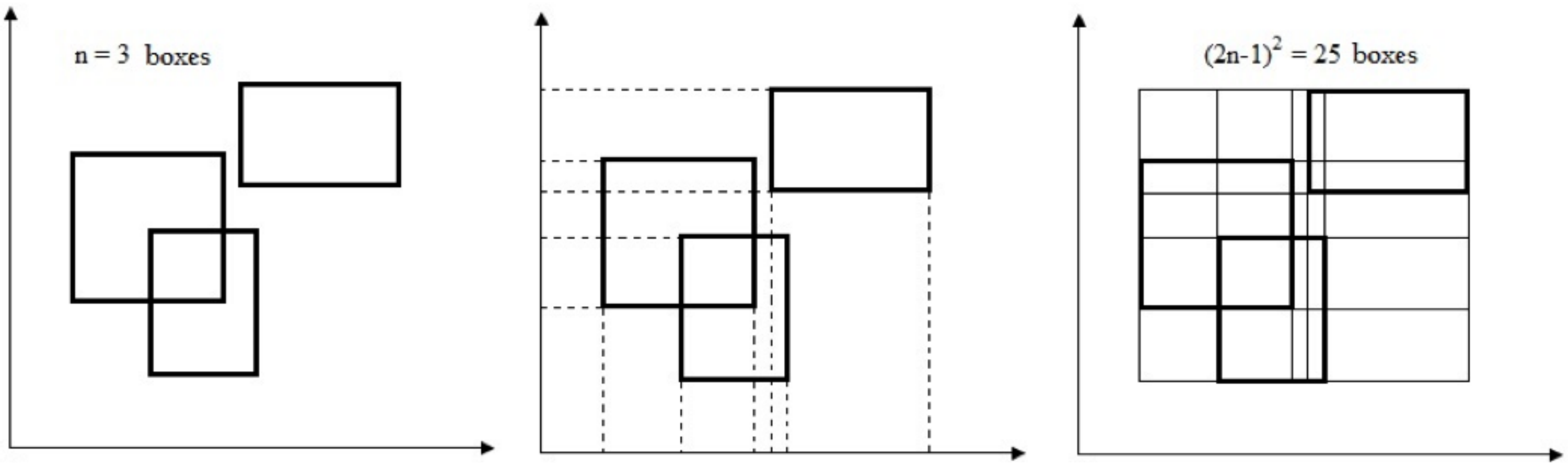
$$\dot{x}(t) = Ax(t) + Bu(t) + \omega(t)$$
$$y(t_k) = Cx(t_k) + \epsilon(t_k)$$

- **Predictor-corrector algorithms in presence of corrupted data**

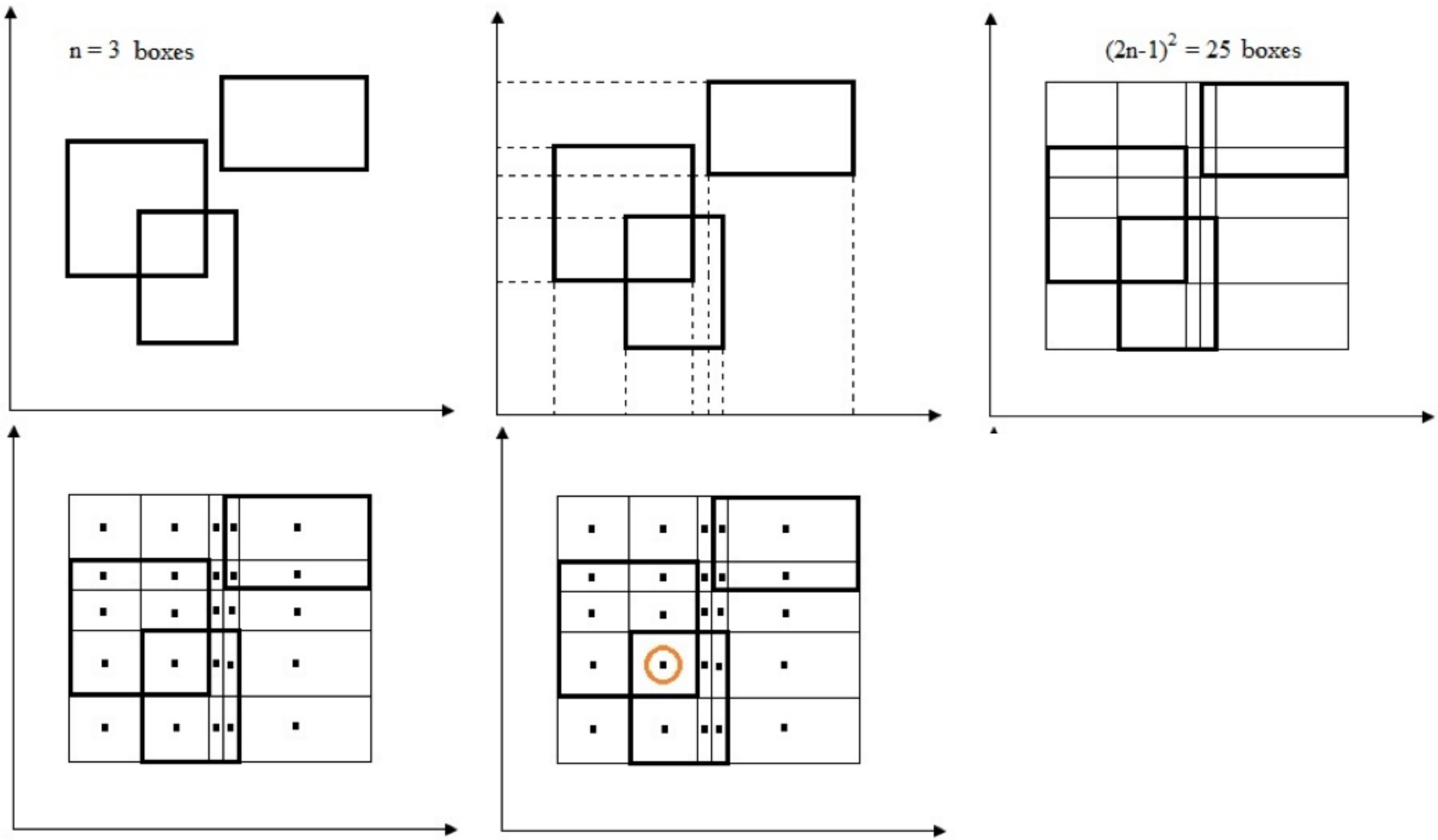
Estimation with outliers. q-Relaxed intersection (Jaulin,09)



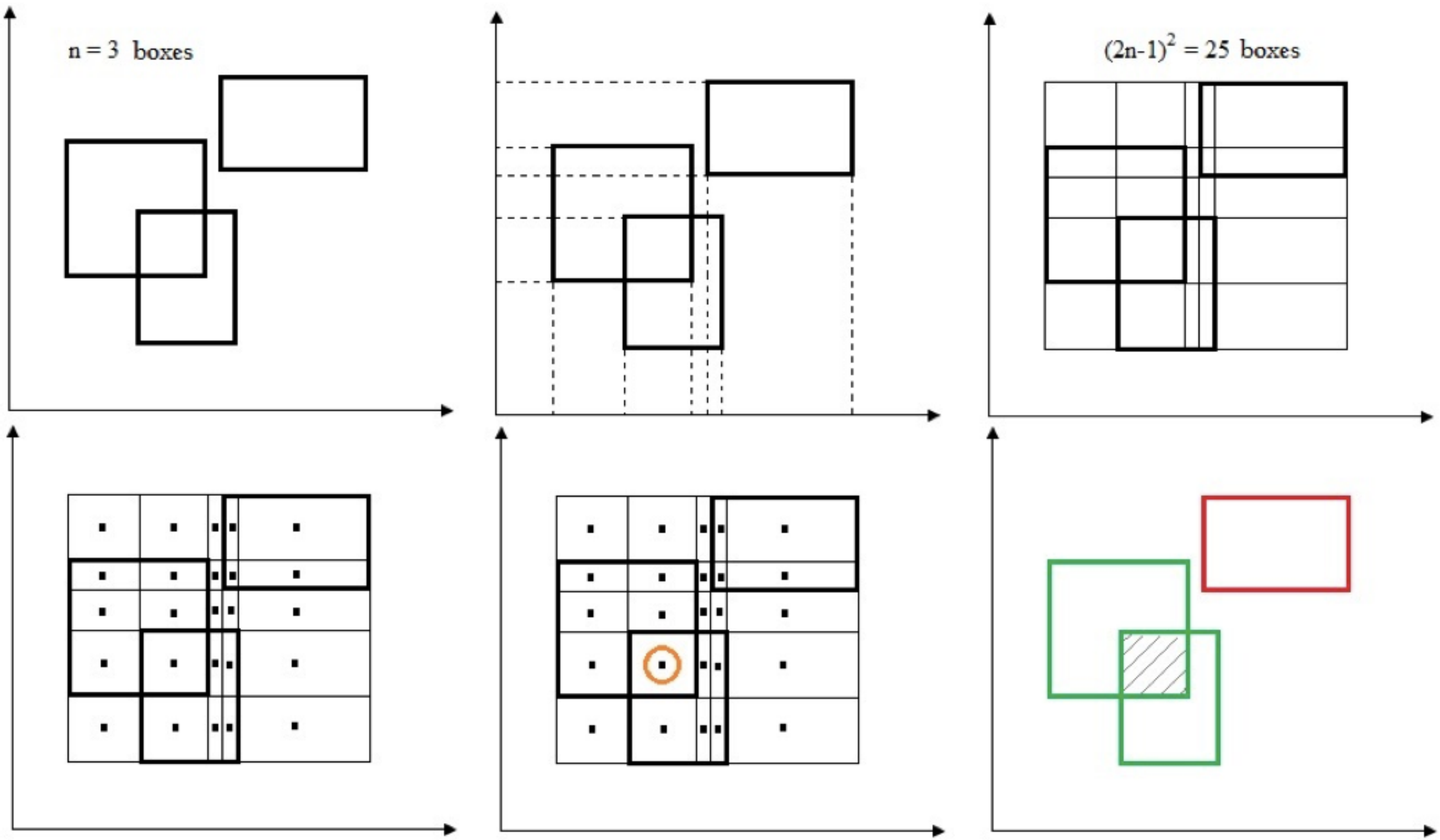
Estimation with outliers. q-Relaxed intersection (Jaulin,09)



Estimation with outliers.
q-Relaxed intersection (Jaulin,09)



Estimation with outliers. q-Relaxed intersection (Jaulin,09)



- **Infrastructure-Based** Localisation Techniques with Interval Data, and Outliers

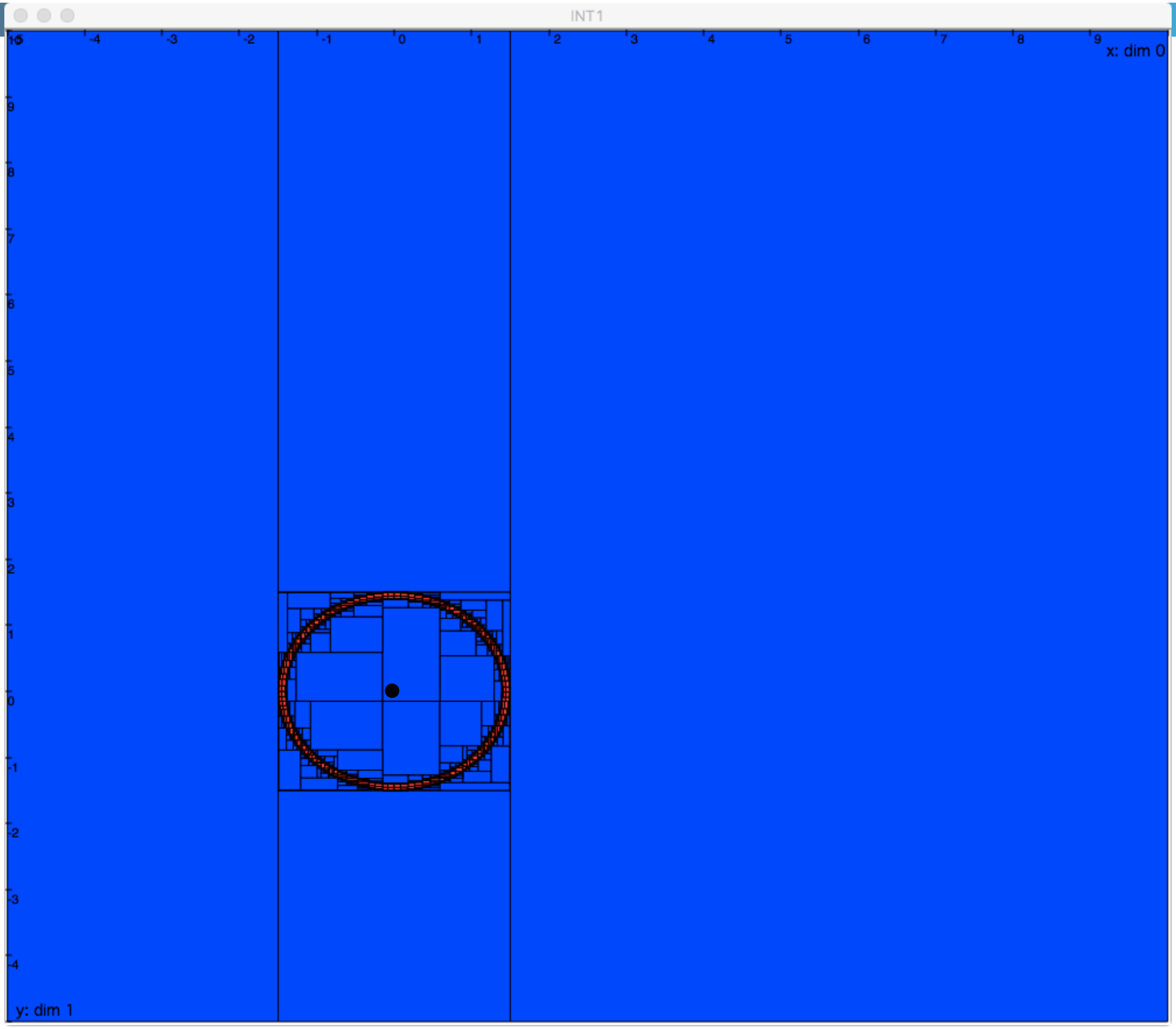
Robust Localization

- **Example #1.**
  Robot localisation via ToF-based Multilateration
  - Can measure the distance to a beacon
  - ToF. **Time of Flight**
  - **Bounded-error** framework

Robust Localization

TOF

1 beacon

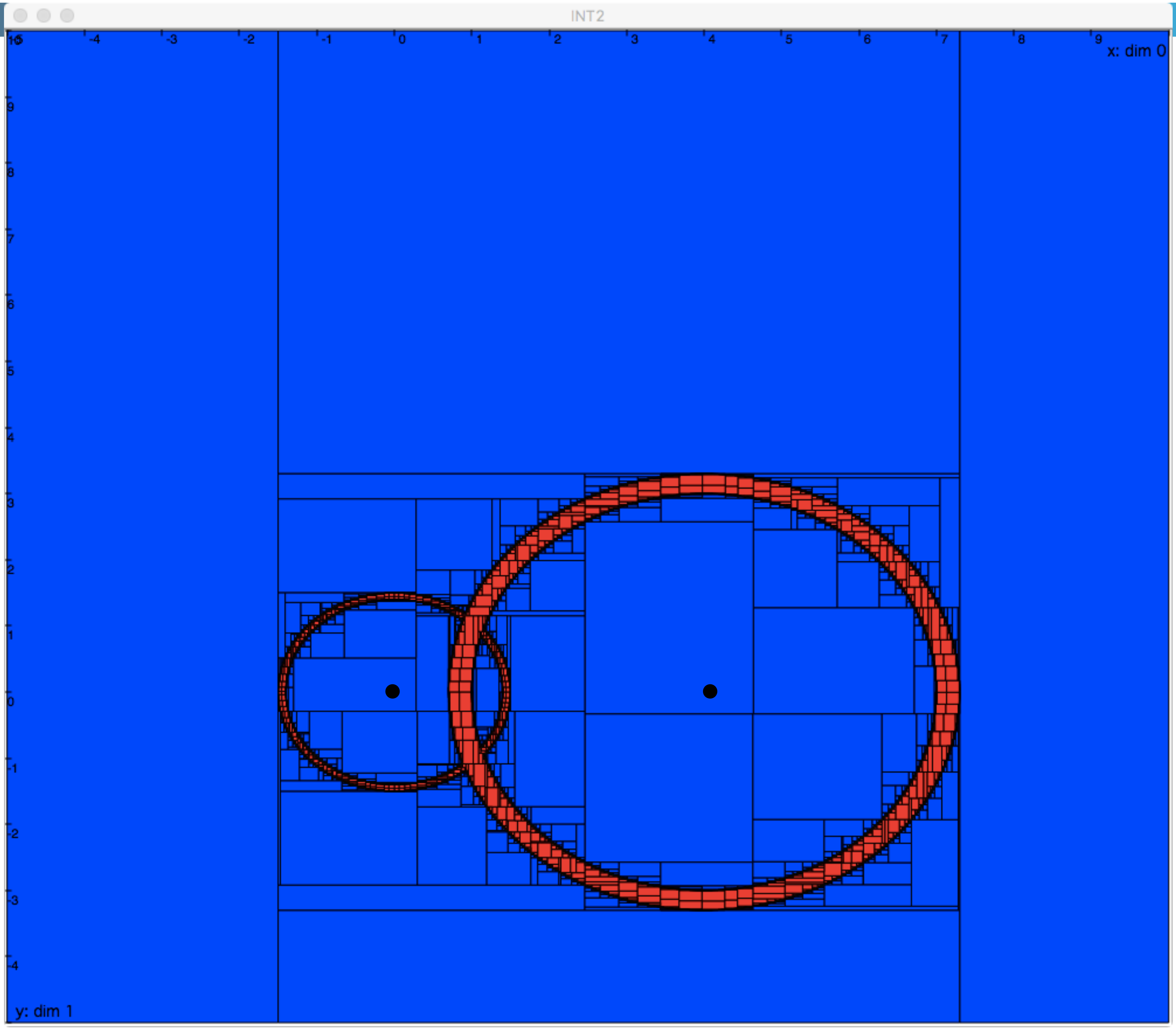


Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

Robust Localization

TOF

2 beacons

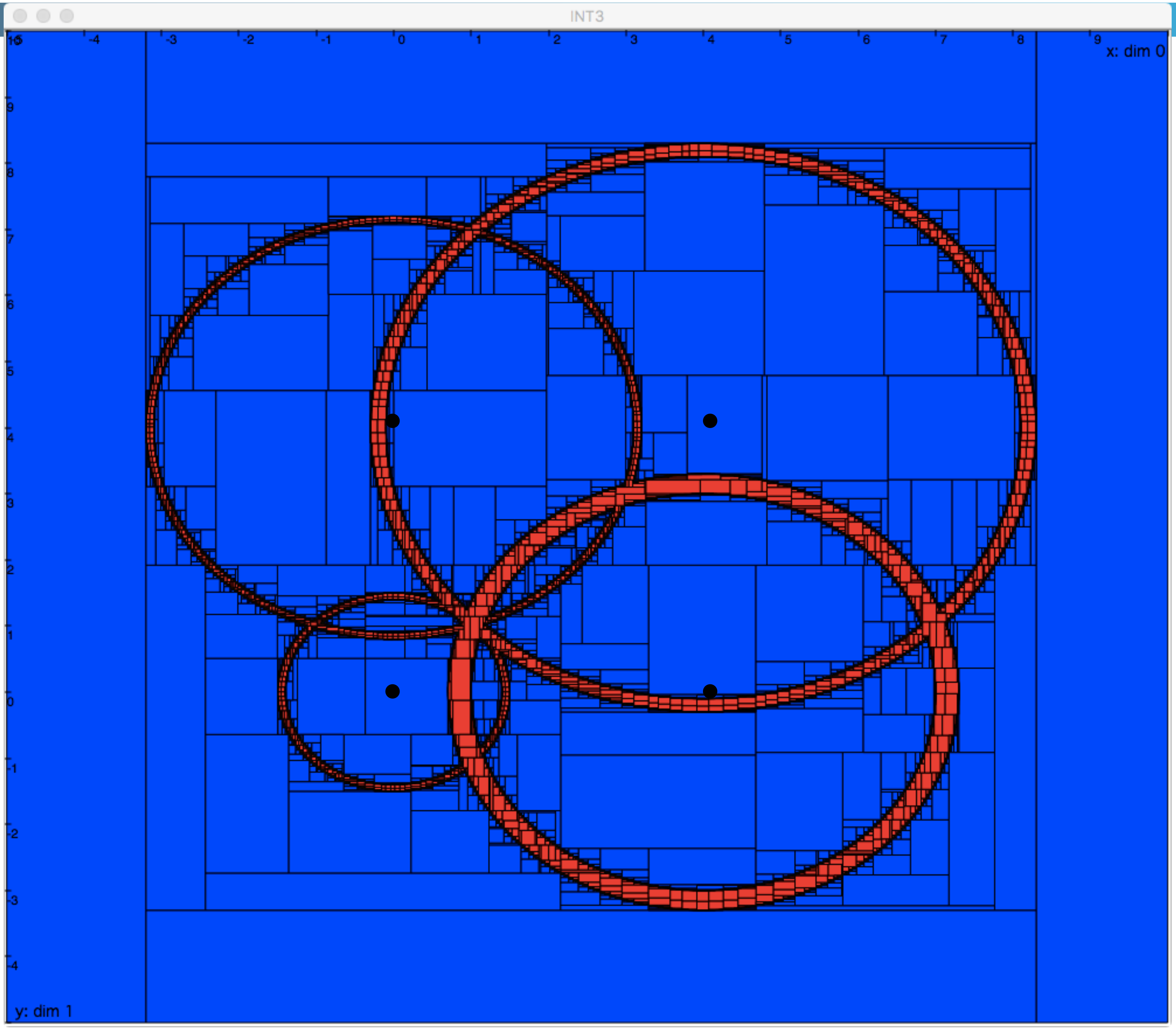


Figures obtained using PYIBEX tool.
benensta.github.io/pyIbex

Robust Localization

TOF

4 beacons

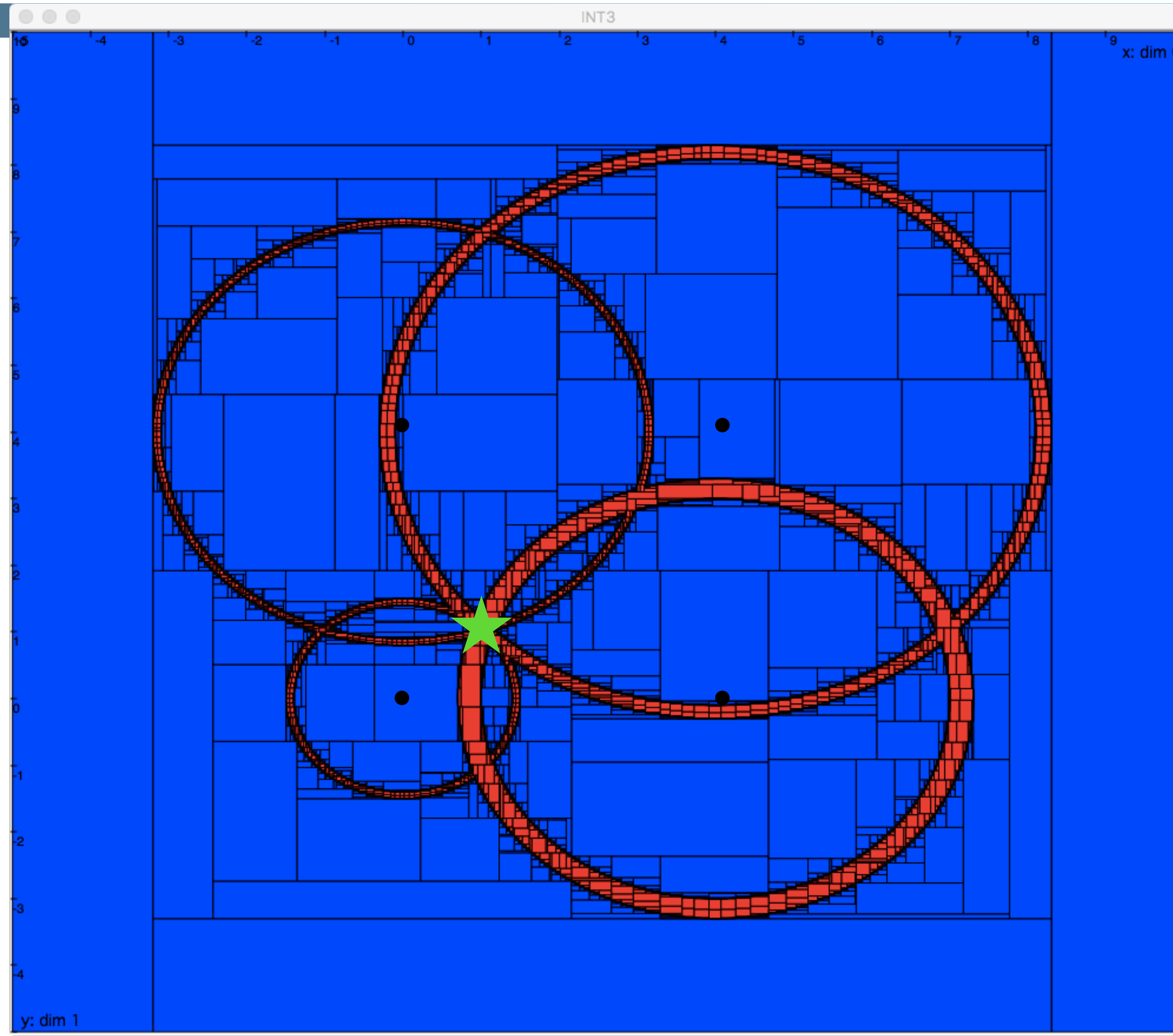


Figures obtained using PYIBEX tool.
benensta.github.io/pyIbex

Robust Localization

TOF

4 beacons



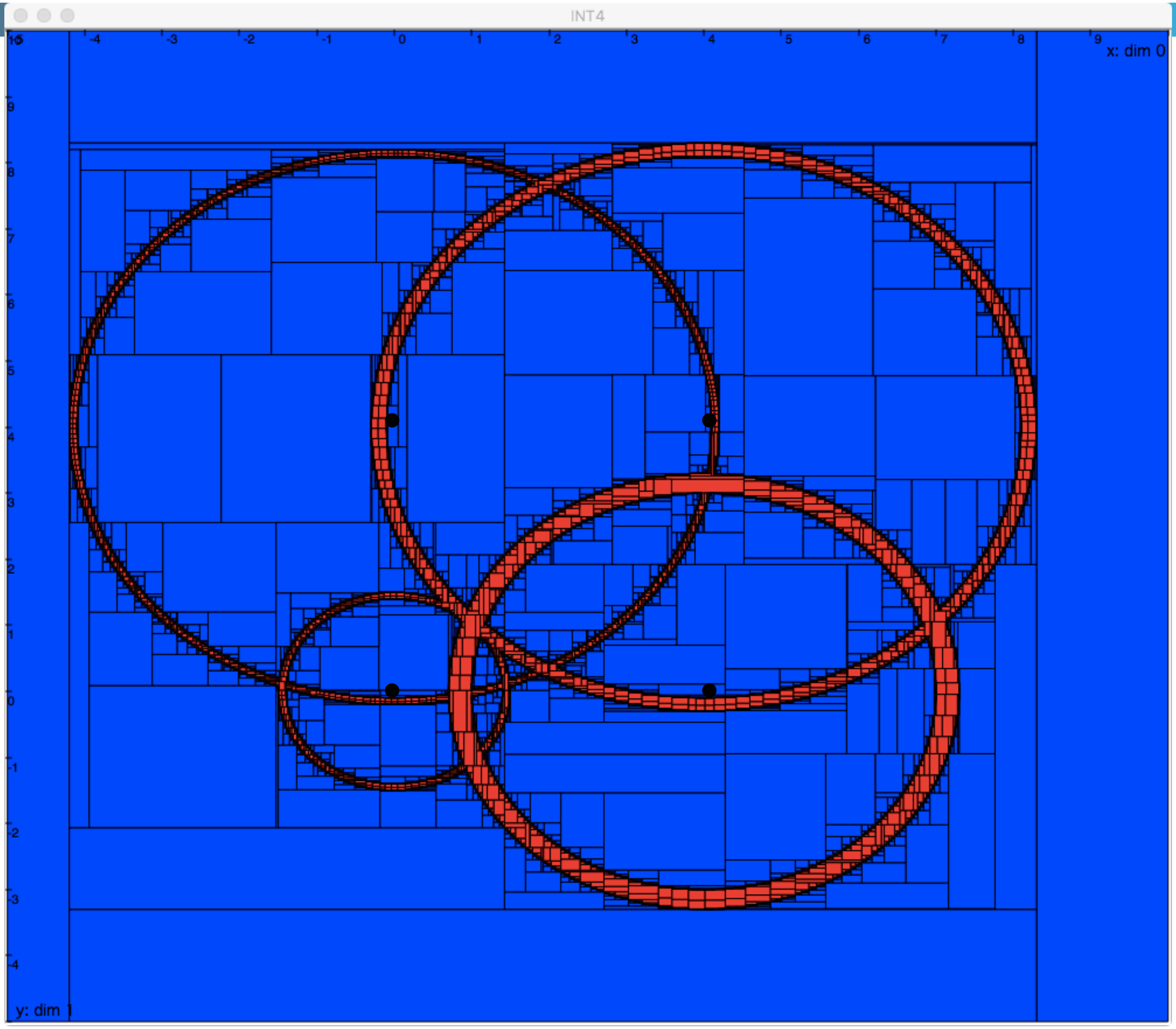
Figures obtained using PYIBEX tool.
benensta.github.io/pyIbex

Robust Localization

TOF

4 beacons

1 corrupted



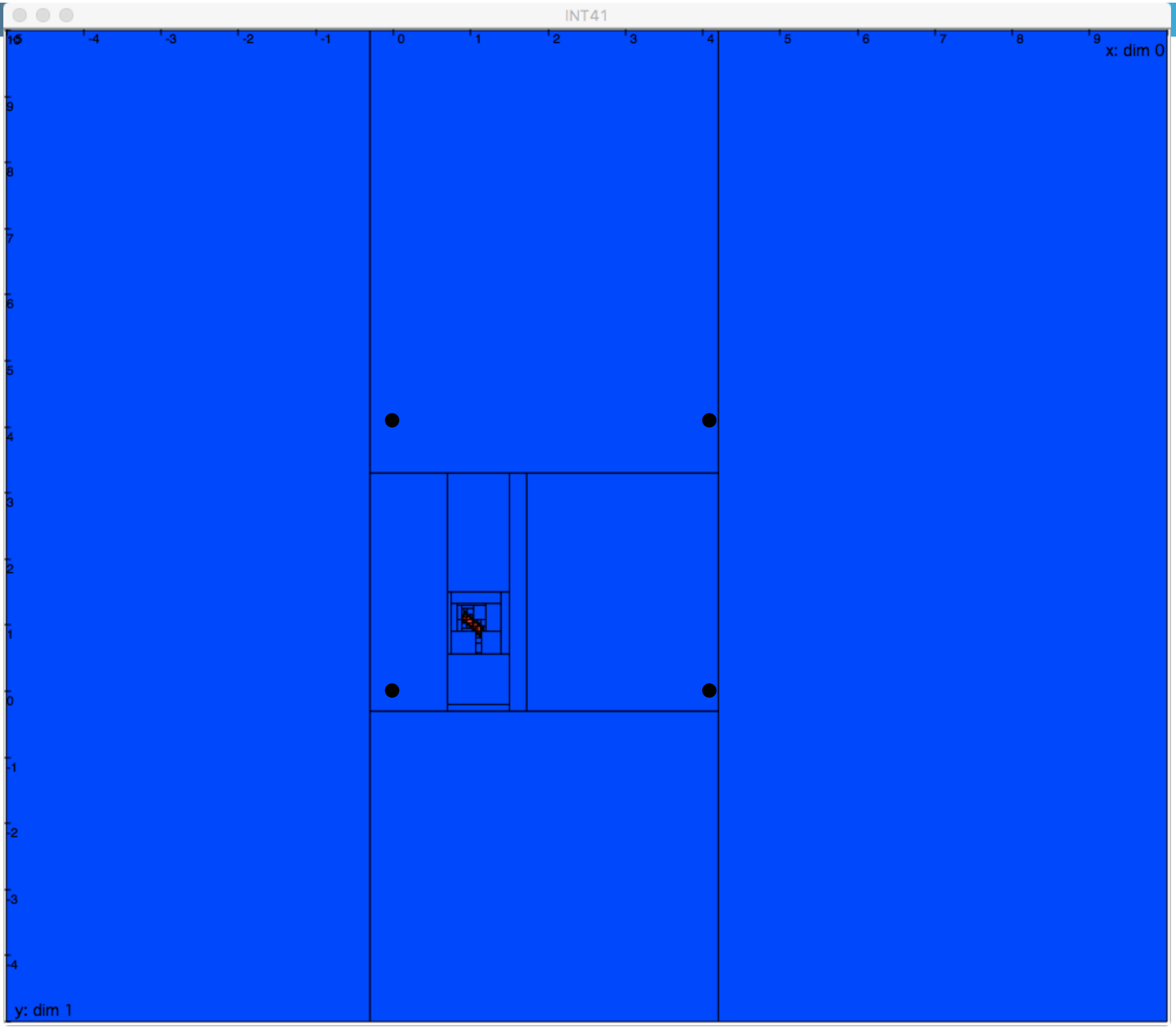
Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

Robust Localization

TOF

1-relaxed

Intersection



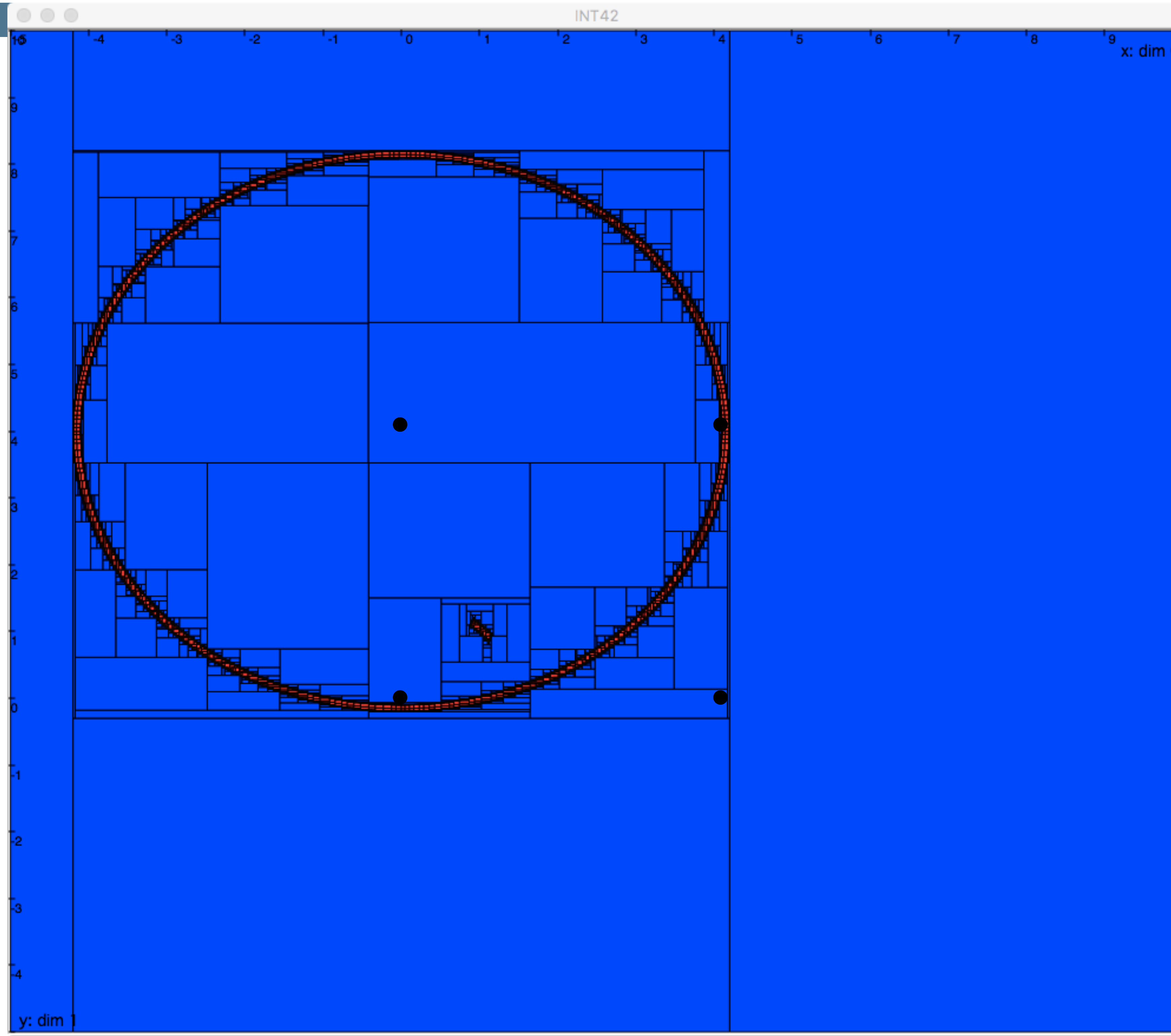
Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

Robust Localization

TOF

1-relaxed

Intersection



Spurious datum identified

Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

Robust Localization

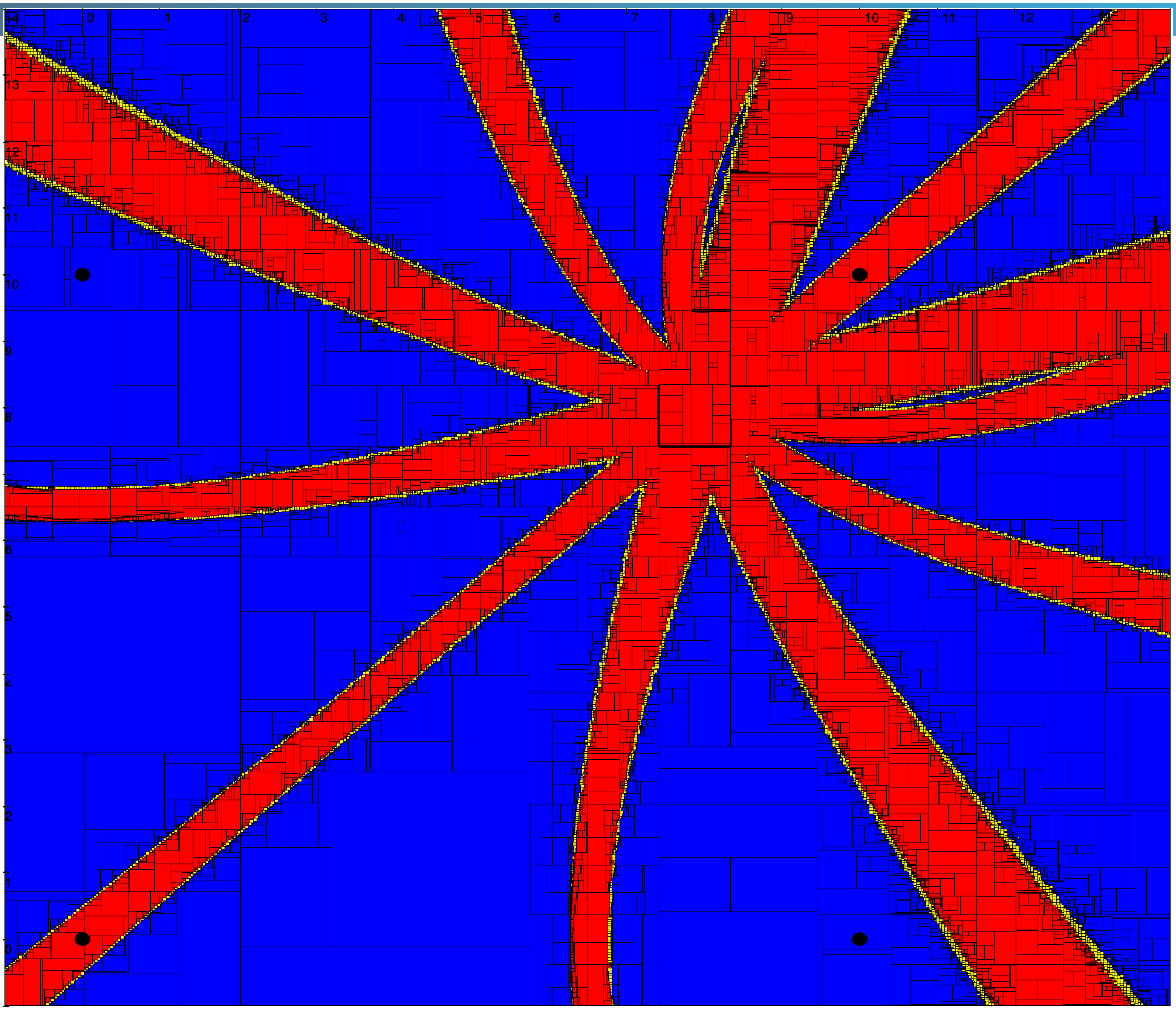
- **Example #2.**
  Robot localisation via TDoA Multilateration
  - Can measure the distance **difference** to beacons
  - TDoA. **Time Difference of Arrival**
  - **Bounded-error** framework

Robust Localization

TDoA

4 beacons

no corruption



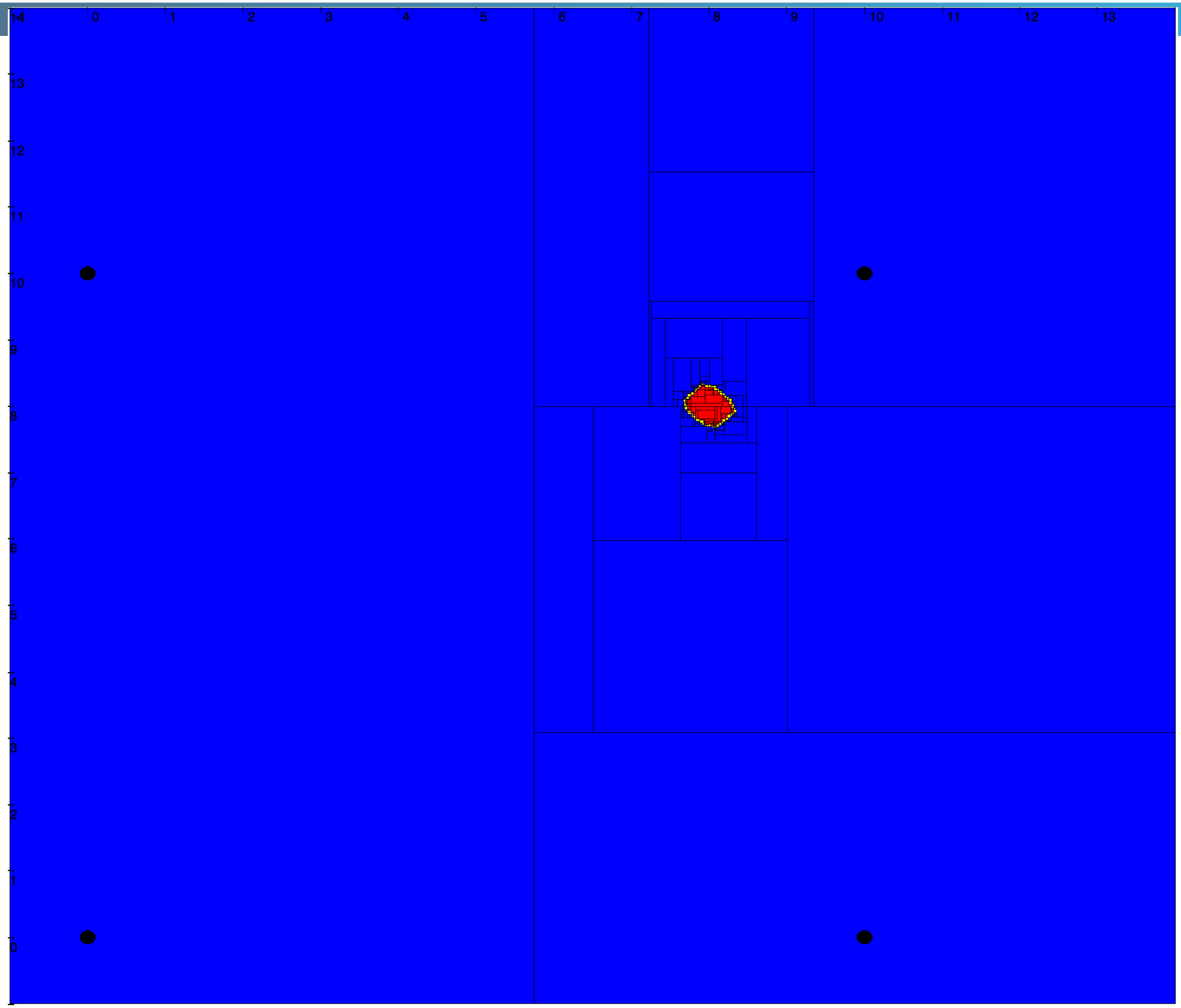
Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

Robust Localization

TDoA

4 beacons

no corruption



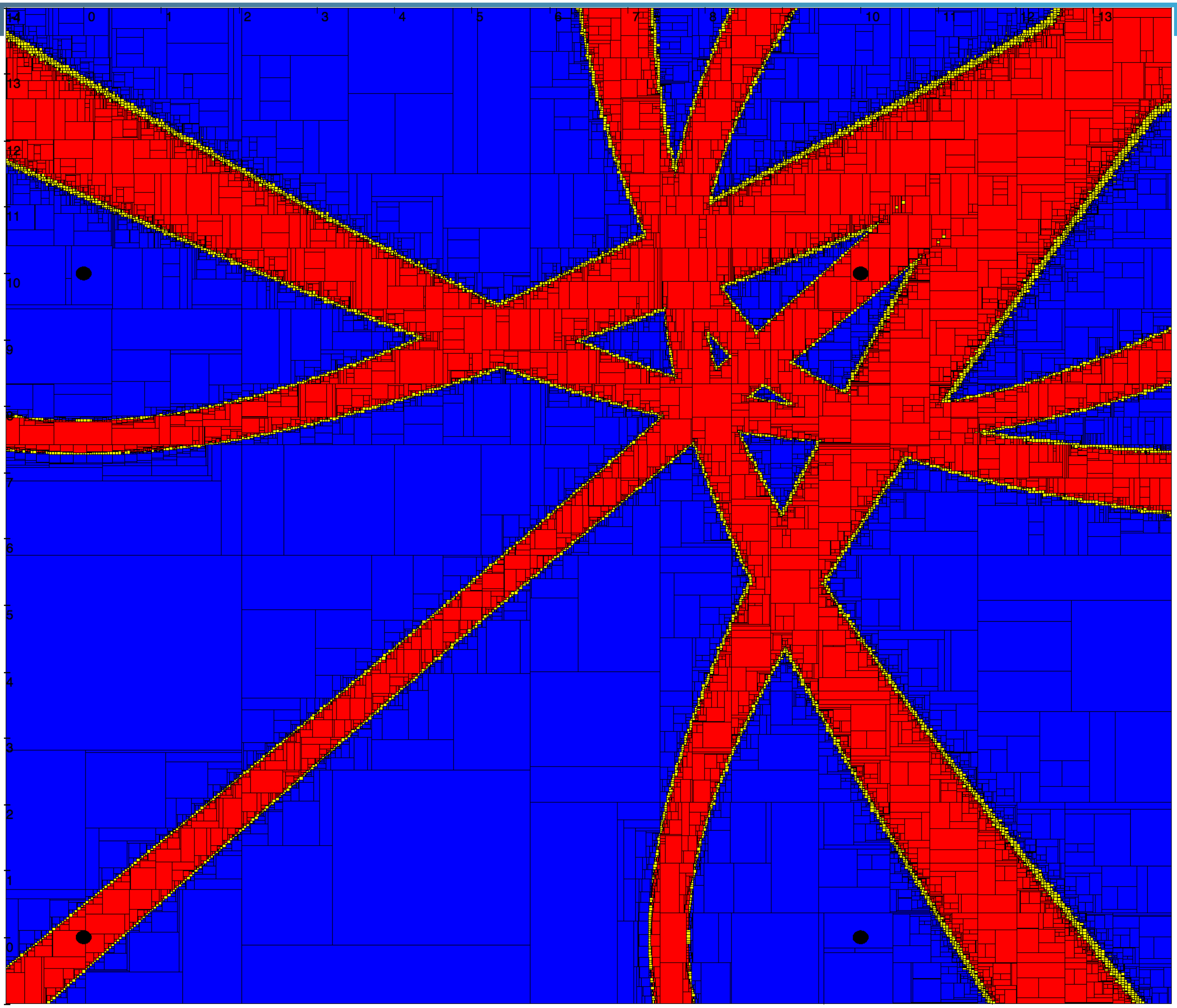
Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

Robust Localization

TDoA

4 beacons

1 corruption



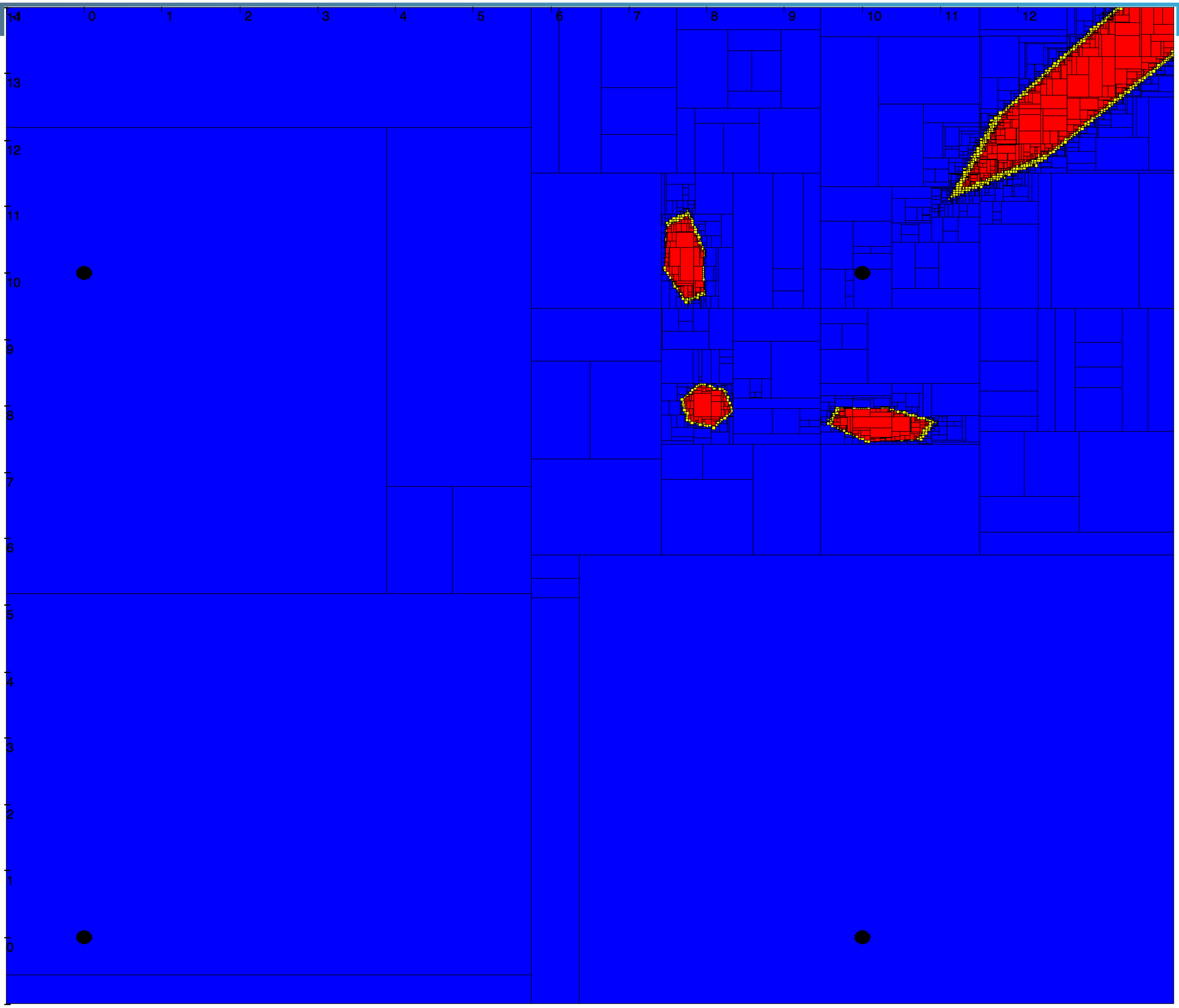
Figures obtained using PYIBEX tool. benensta.github.io/pylbex

Robust Localization

TDoA

4 beacons

1 corruption



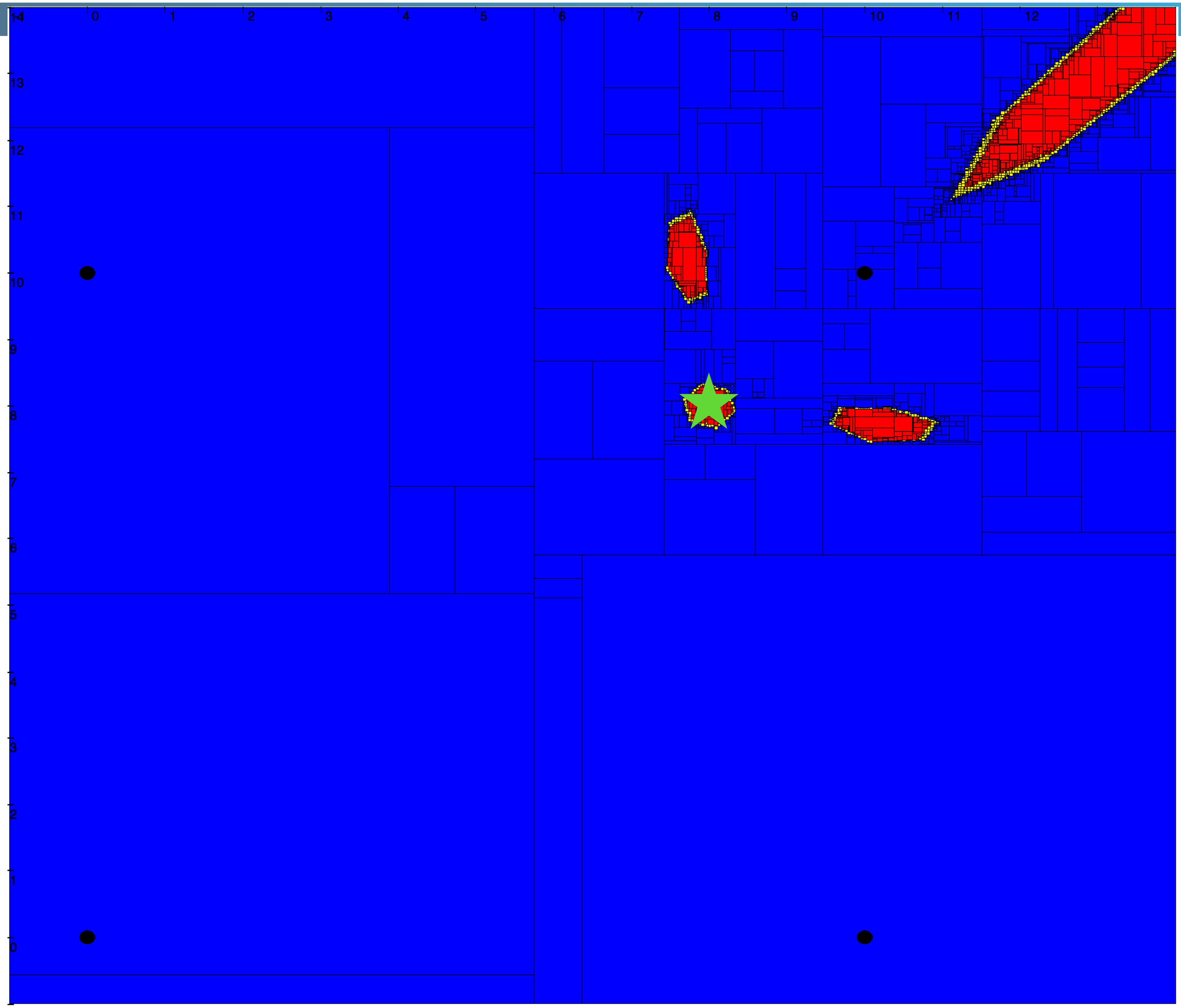
Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

Robust Localization

TDoA

4 beacons

1 corruption



Figures obtained using PYIBEX tool. benensta.github.io/pyIbex

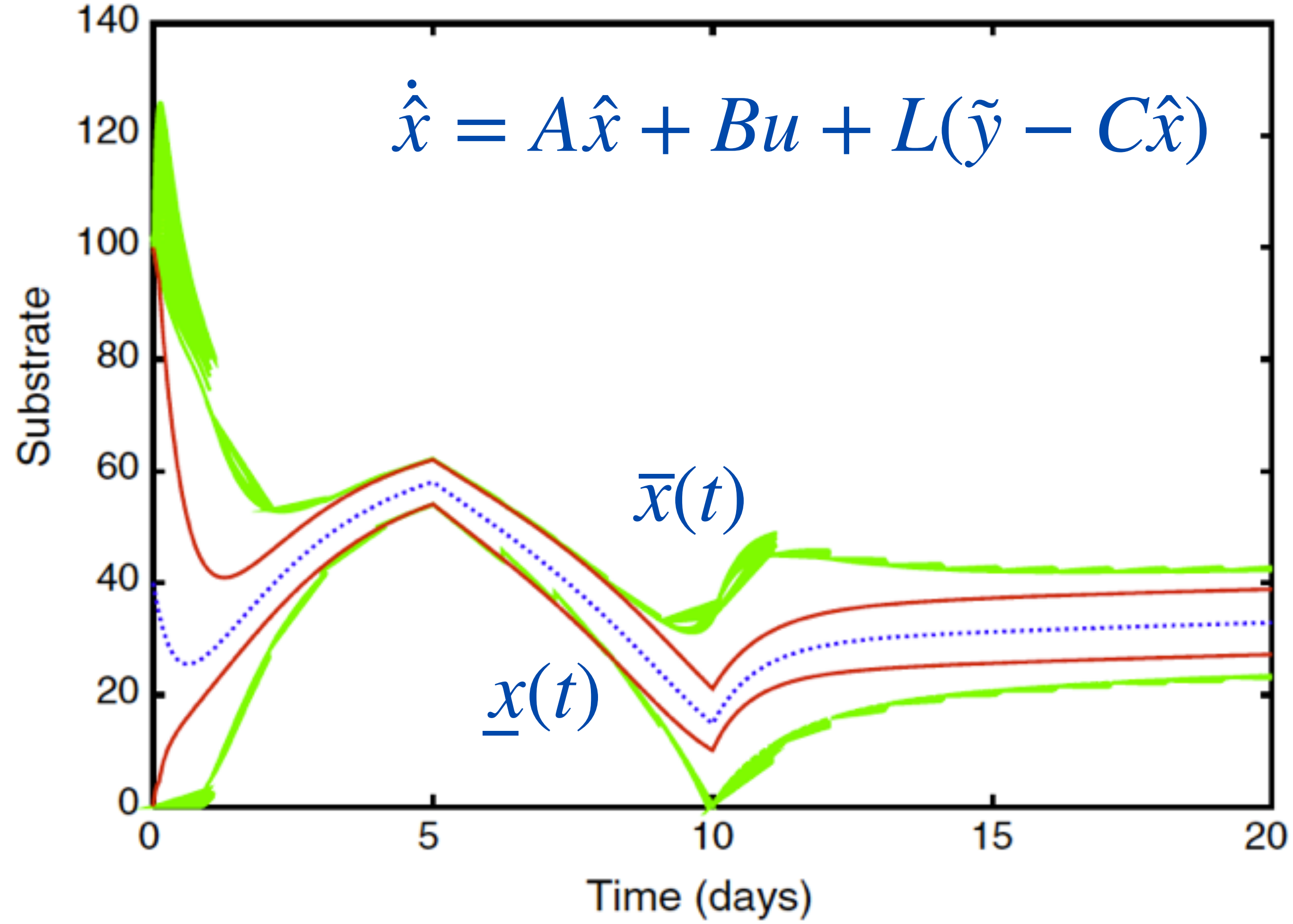
- **Secure Interval Observers**

Interval Observers

Continuous-time data

- **Luenberger-like observers**: (Gouzé et al, 00),(Mazenc & Bernard, 10), (Meslem & Ramdani, 11), (Raïssi, et al., 12) …
- Tune observer **gain** to ensure **Input-to-State Stability (practical stability)**
- Build **framers** $\underline{x}(t)$ and $\overline{x}(t)$

$$\underline{x}(t) \leq x(t) \leq \overline{x}(t)$$



$$\dot{x}(t) = Ax(t) + Bu(t) + \omega(t)$$
$$y(t) = Cx(t) + \epsilon(t)$$

Secure Interval Observer

(Degue, et al., IEEE CDC 2018)

- **Resilience to stealthy attacks**
  - Stealthy attacks produce plausible output signals
    - **sensor**: change in output smaller than impact of noise/disturbance
    - **actuator**: change in output has no dynamic …

- **Observer synthesis**
  - Plays with initial conditions
  - Bounds of attacks = virtual outputs

Secure Interval Observer

(Degue, et al., IEEE CDC 2018)

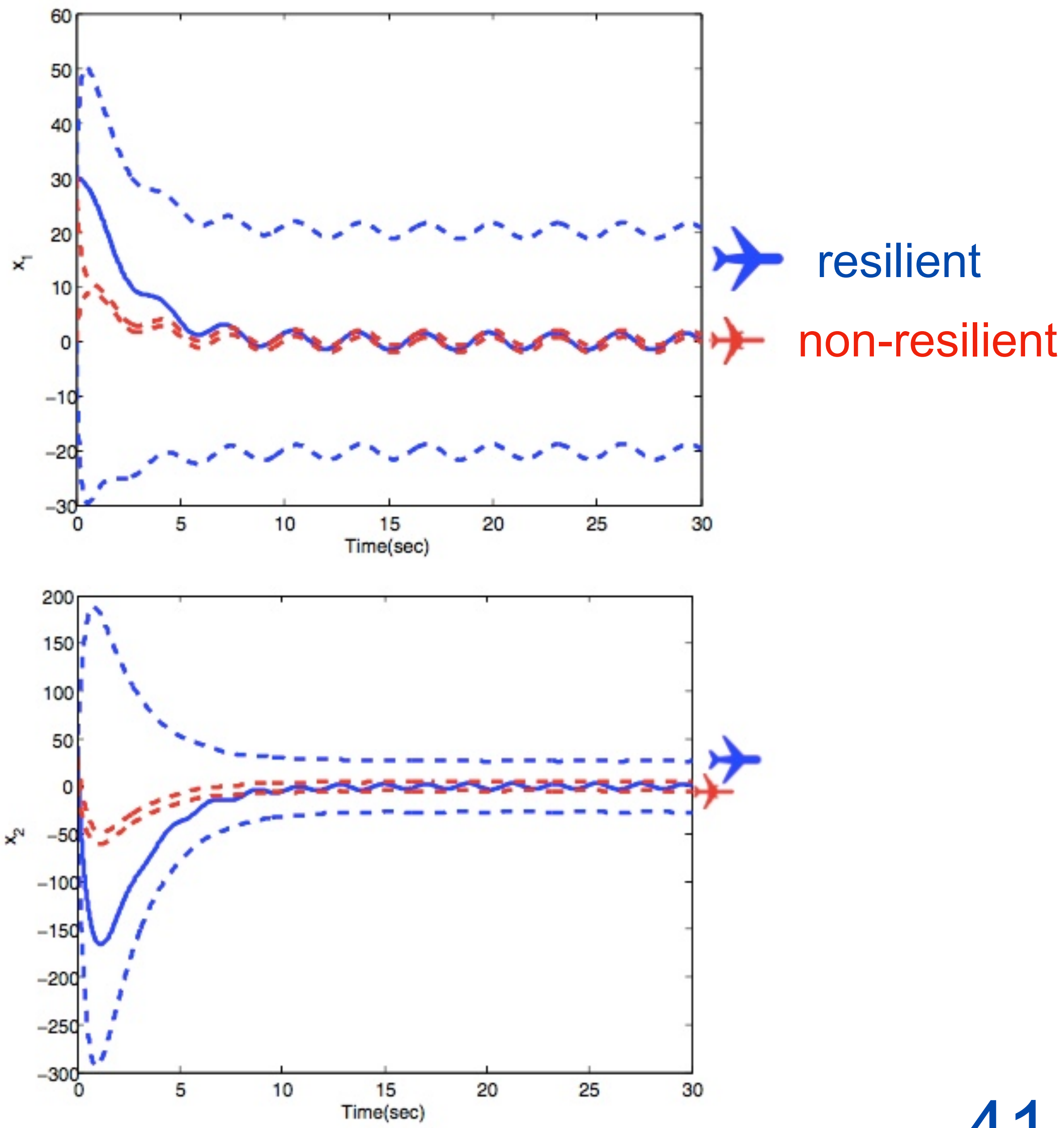
- Resilience to stealthy attacks
- Working assumptions for observer synthesis
  - Continuous-time measurement
  - Strong assumptions on inversibility
  - Strong assumptions $\exists L, \quad A - LC$ is Hurwitz and Metzler

- Build a **secure interval observer** that successfully reconstructs **bounds on sensor/actuator attack vector**

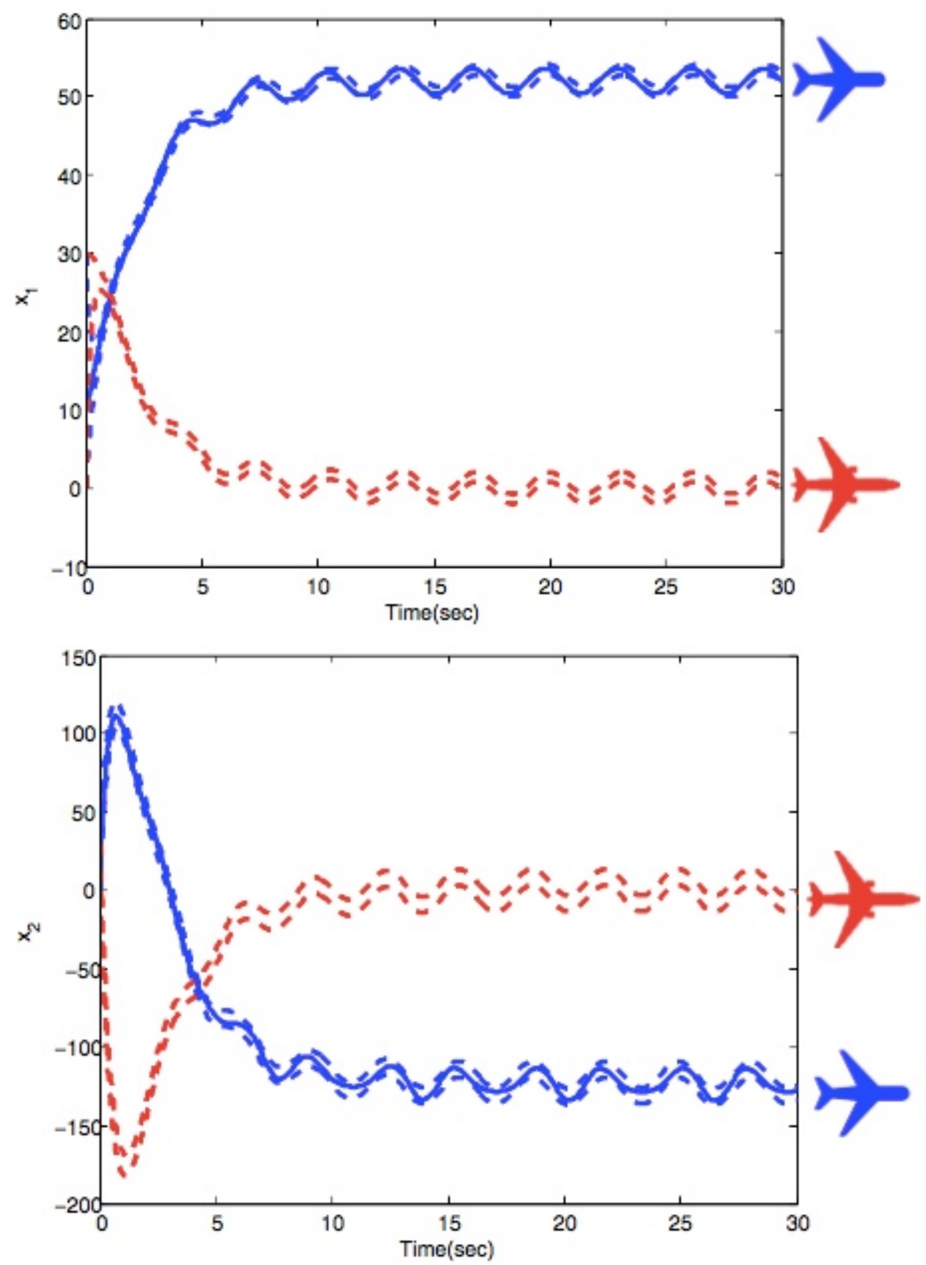
Secure Interval Observer

(Degue, et al., IEEE CDC 2018)

Stealthy Sensor Attack



Stealthy Actuator Attack



- **Secure Interval Impulsive Observers**

Secure Interval Observer

Our approach (Rabehi, et al, SYSTOL 2019)

- **Resilience to deception attacks**
- Working assumptions
  - Discrete-time measurements with continuous-time model.
  - System **s-sparse observable**
  - Sensor attacks are **distinguishable**

- Build a **secure interval impulsive observer** that successfully reconstructs state vector

Secure Interval Observer

Our approach (Rabehi, et al, SYSTOL 2019)

- **Interval Impulsive Observer, as a hybrid system**

$$t \in [t_{k-1}, t_k], \quad \dot{x}(t) = Ax(t) + Bu(t)$$
$$x(t_k^+) = x(t_k) + L\left(Cx(t_k) - \epsilon(t_k) - y(t_k)\right)$$

Interval Impulsive Observer

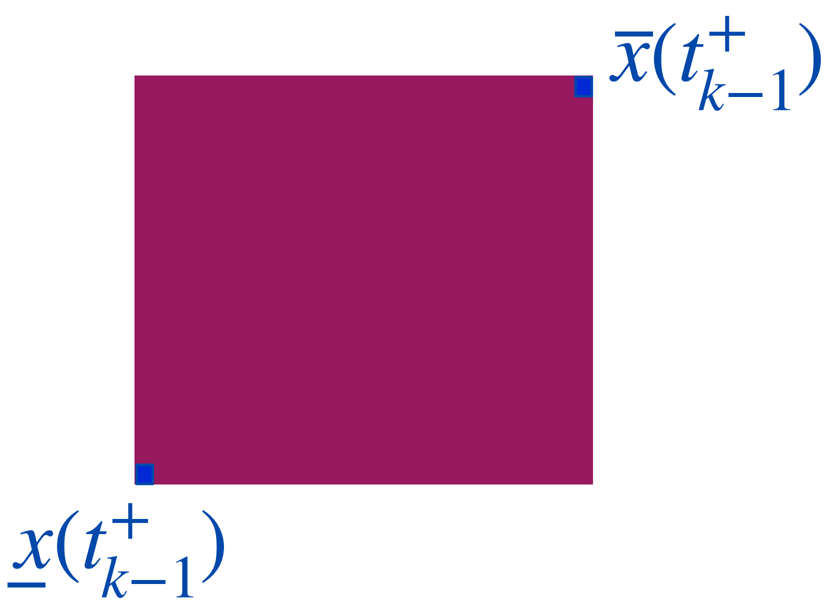
$$t \in [t_{k-1}, t_k], \quad \dot{x}(t) = Ax(t) + Bu(t)$$
$$x(t_k^+) = x(t_k) + L\left(Cx(t_k) - \epsilon(t_k) - y(t_k)\right)$$

(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

$$t \in [t_{k-1}, t_k], \quad \dot{x}(t) = Ax(t) + Bu(t)$$

$$x(t_k^+) = x(t_k) + L\left(Cx(t_k) - \epsilon(t_k) - y(t_k)\right)$$



(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

$$t \in [t_{k-1}, t_k], \quad \dot{x}(t) = Ax(t) + Bu(t)$$
$$x(t_k^+) = x(t_k) + L\left(Cx(t_k) - \epsilon(t_k) - y(t_k)\right)$$

$A = A_M - A_N$,
A_M is Metzler,
$A_N > 0$

(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

$$t \in [t_{k-1}, t_k], \quad \dot{x}(t) = Ax(t) + Bu(t)$$

$$x(t_k^+) = x(t_k) + L\left(Cx(t_k) - \epsilon(t_k) - y(t_k)\right)$$

$A = A_M - A_N$,
A_M is Metzler,
$A_N > 0$

$\overline{x}(t_{k-1}^+)$

$\underline{x}(t_{k-1}^+)$

open-loop estimator $\quad t \in [t_{k-1}, t_k]$

$$\dot{\underline{x}}(t) = A_M \underline{x}(t) - A_N \overline{x}(t) + Bu(t)$$

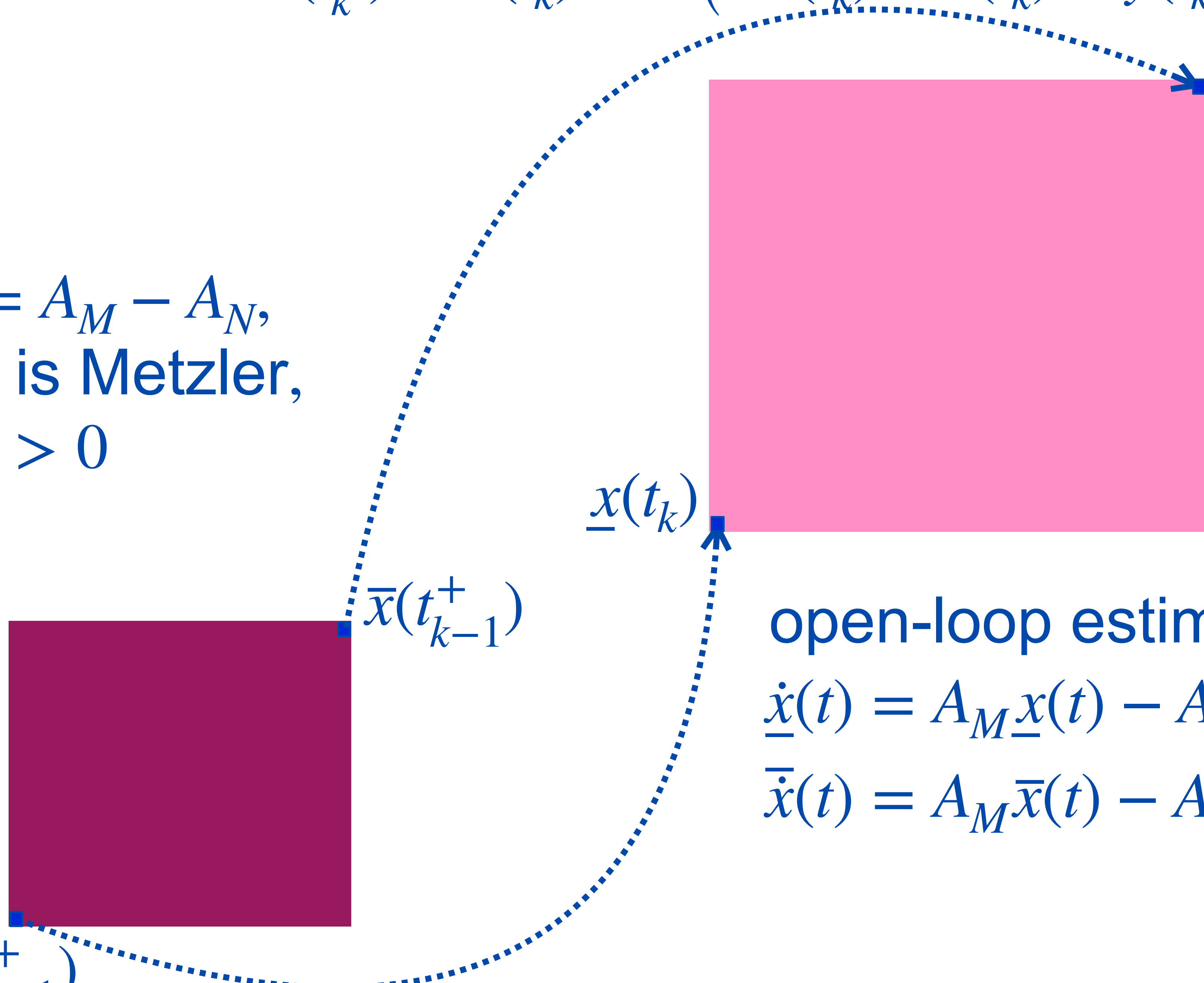
$$\dot{\overline{x}}(t) = A_M \overline{x}(t) - A_N \underline{x}(t) + Bu(t)$$

(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

$t \in [t_{k-1}, t_k], \quad \dot{x}(t) = Ax(t) + Bu(t)$

$$x(t_k^+) = x(t_k) + L\left(Cx(t_k) - \epsilon(t_k) - y(t_k)\right)$$



$A = A_M - A_N$,
A_M is Metzler,
$A_N > 0$

open-loop estimator $\quad t \in [t_{k-1}, t_k]$

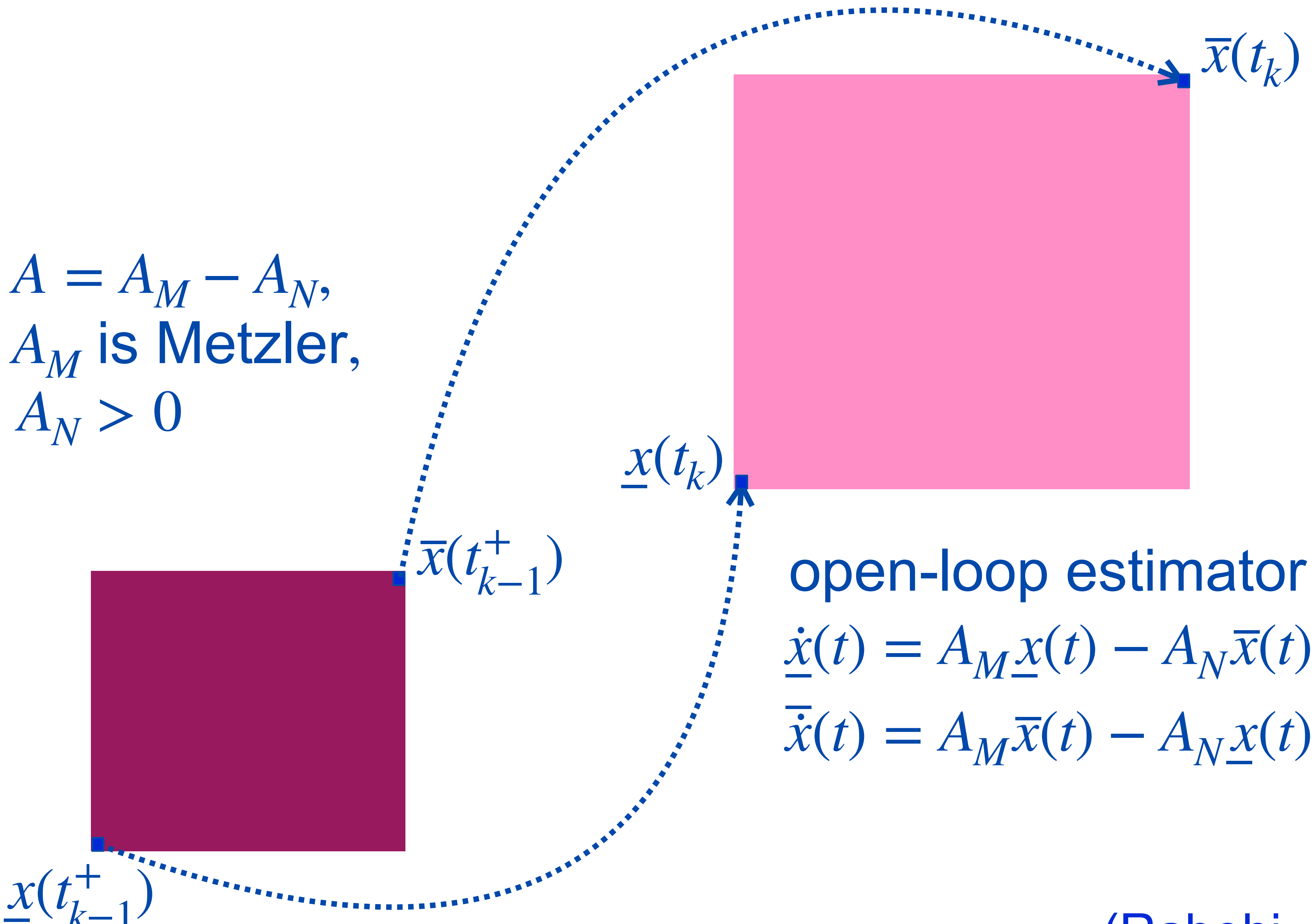
$$\dot{\underline{x}}(t) = A_M\underline{x}(t) - A_N\overline{x}(t) + Bu(t)$$

$$\dot{\overline{x}}(t) = A_M\overline{x}(t) - A_N\underline{x}(t) + Bu(t)$$

(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

$A = A_M - A_N$,
A_M is Metzler,
$A_N > 0$



open-loop estimator $\quad t \in [t_{k-1}, t_k]$

$$\dot{\underline{x}}(t) = A_M \underline{x}(t) - A_N \overline{x}(t) + Bu(t)$$

$$\dot{\overline{x}}(t) = A_M \overline{x}(t) - A_N \underline{x}(t) + Bu(t)$$

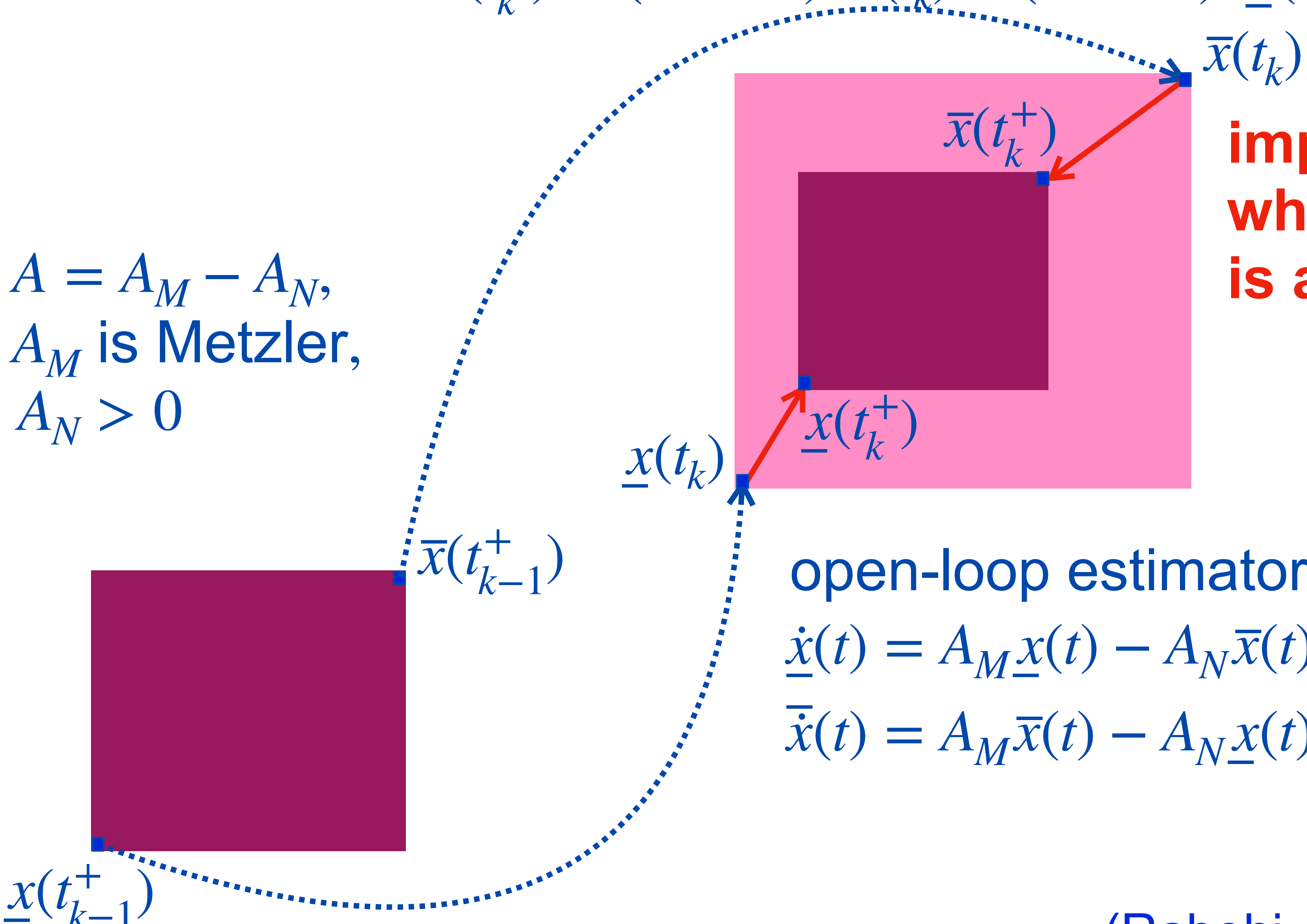
(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

UNIVERSITE D'ORLEANS

$$\underline{x}(t_k^+) = (I + \underline{L}C)^+\underline{x}(t_k) - (I + \underline{L}C)^-\overline{x}(t_k) - |\underline{L}|\overline{\epsilon}(t_k) - \underline{L}y(t_k)$$

$$\overline{x}(t_k^+) = (I + \overline{L}C)^+\overline{x}(t_k) - (I + \overline{L}C)^-\underline{x}(t_k) - |\overline{L}|\overline{\epsilon}(t_k) - \overline{L}y(t_k)$$



impulsive correction when measurement is available

$A = A_M - A_N$,
A_M is Metzler,
$A_N > 0$

open-loop estimator $\quad t \in [t_{k-1}, t_k]$

$$\dot{\underline{x}}(t) = A_M\underline{x}(t) - A_N\overline{x}(t) + Bu(t)$$

$$\dot{\overline{x}}(t) = A_M\overline{x}(t) - A_N\underline{x}(t) + Bu(t)$$

(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

(Rabehi, et al, SYSTOL 2019)

Interval Impulsive Observer

(Rabehi, et al, SYSTOL 2019)

$$A = A_M - A_N, \quad A_M \text{ is Metzler}, \quad A_N > 0$$

Open-loop predictor

$$t \in [t_{k-1}, t_k], \quad \dot{\underline{x}}(t) = A_M \underline{x}(t) - A_N \overline{x}(t) + Bu(t)$$

$$\dot{\overline{x}}(t) = A_M \overline{x}(t) - A_N \underline{x}(t) + Bu(t)$$

Impulsive correction when measurement is available

$$\underline{x}(t_k^+) = (I + \underline{L}C)^+ \underline{x}(t_k) - (I + \underline{L}C)^- \overline{x}(t_k) - |\underline{L}|\,\overline{\epsilon}(t_k) - \underline{L}y(t_k)$$

$$\overline{x}(t_k^+) = (I + \overline{L}C)^+ \overline{x}(t_k) - (I + \overline{L}C)^- \underline{x}(t_k) - |\overline{L}|\,\overline{\epsilon}(t_k) - \overline{L}y(t_k)$$

Secure Interval Observer

Our approach (Rabehi, et al, SYSTOL 2019)

- **Interval Impulsive Observer, as a hybrid system**

$$
\begin{aligned}
t \in [t_{k-1}, t_k], \quad \dot{x}(t) &= Ax(t) + Bu(t) \\
x(t_k^+) &= x(t_k) + L\left(Cx(t_k) - \epsilon(t_k) - y(t_k)\right)
\end{aligned}
$$

- Gain synthesis ensuring **Input-to-state stability**.
- NLMI relaxed to set of LMI.
- Can readily be extended to **sporadic** or **event-triggered controlled** sampling.

UNIVERSITE D'ORLEANS

Secure Interval Observer

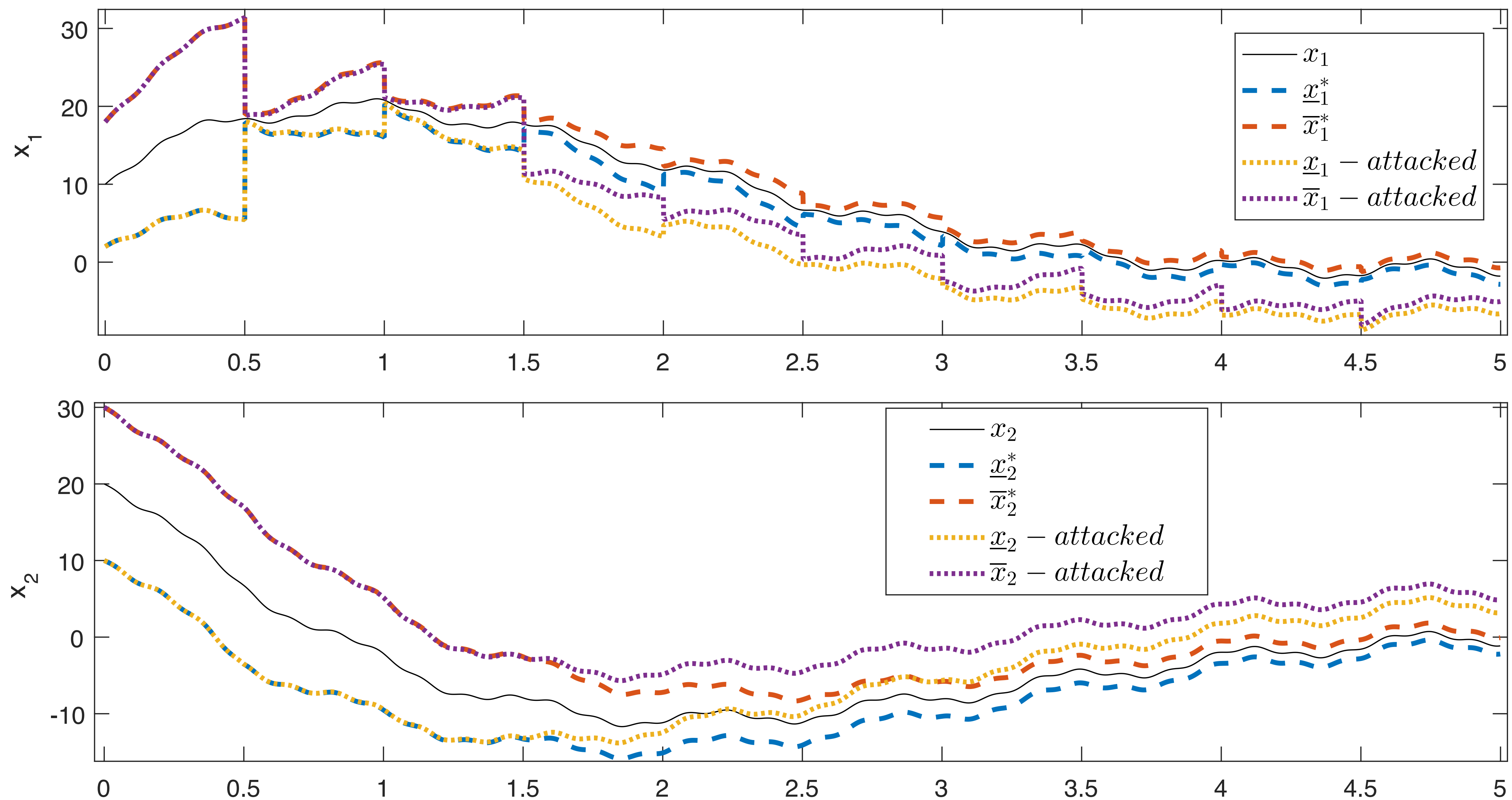
Our approach (Rabehi, et al, SYSTOL 2019)

- **Resilience to deception attacks**
- **Selection strategy** at each time step t_k
  - Use $\dfrac{n!}{s!(n-s)!}$ observers on every subset of *n - s* sensors
  - Compute $\dfrac{n!}{s!(n-s)!}$ intersections of *n - s* estimated sets
  - There should be at least one non-empty solution set.

Secure Interval Observer

Our approach (Rabehi, et al, SYSTOL 2019)

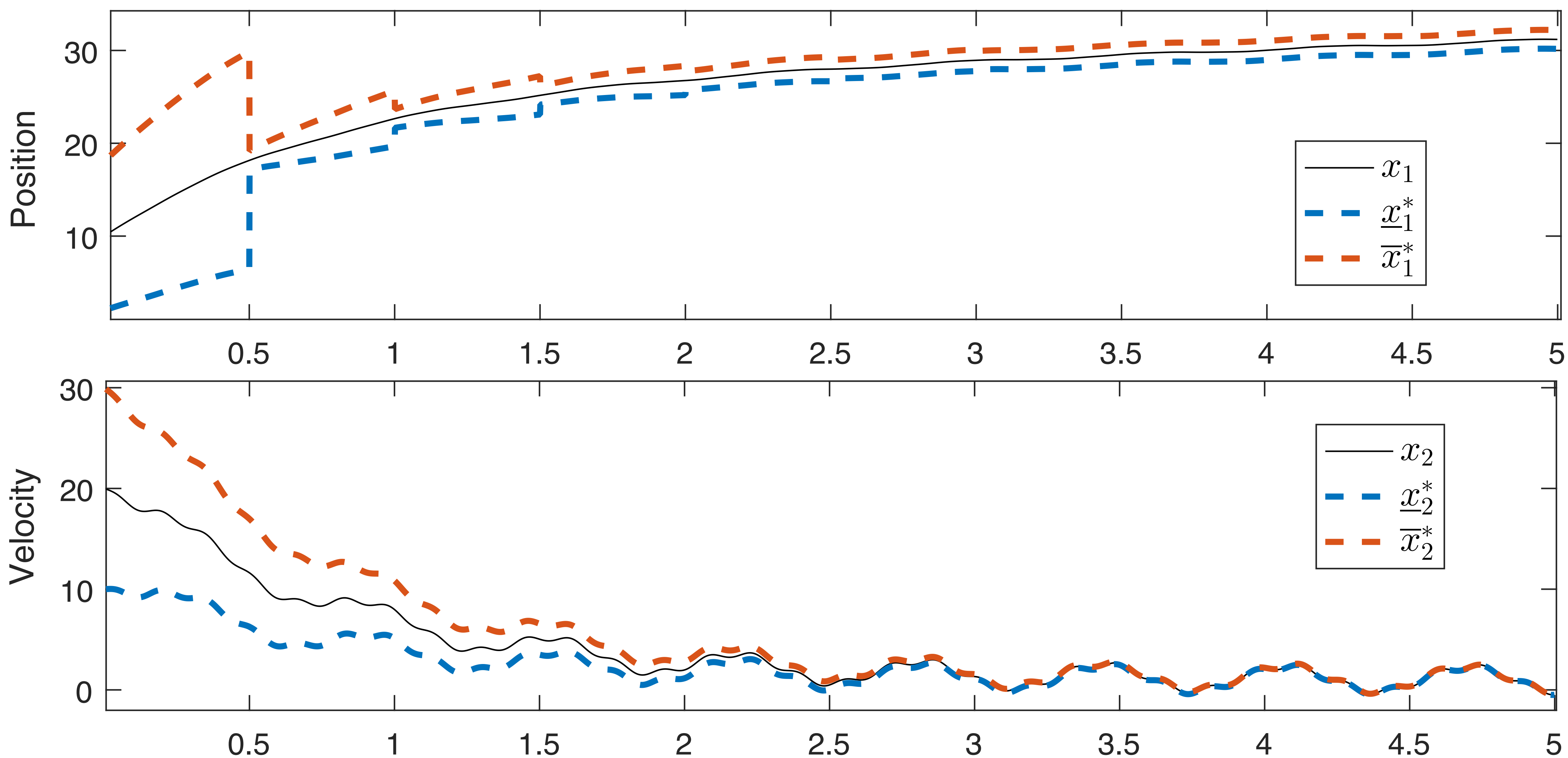
Academic example. Deception attack



Secure Interval Observer

Our approach (Rabehi, et al, SYSTOL 2019)

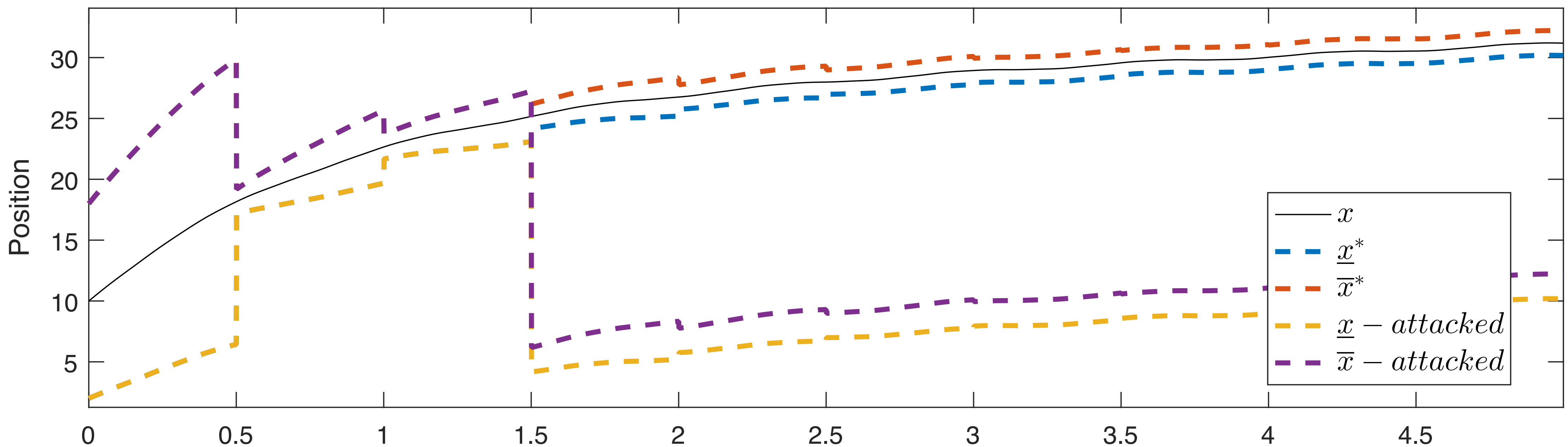
Robot Navigation. n=3 GPS sensors. s=1 deception attack.



Secure Interval Observer

Our approach (Rabehi, et al, SYSTOL 2019)

Robot Navigation. n=3 GPS sensors. s=1 deception attack.



- **Future work**

UNIVERSITE D'ORLEANS

Concluding remarks

- System and control theories can help developing secure (and privacy-preserving) CPS

- Address **secure estimation with stealthy attacks**
- Plan to improve **scalability** of secure estimation
- Plan to further applications in **mobile robotics**

The Cyber-Security Market

- Growing Market
  - Global revenue of the cybersecurity market reached USD 106 billions in 2019, (+11% yearly increase)
  - The global healthcare cybersecurity market was valued at USD 8 billions in 2018 and is expected to reach USD 27 billion by 2026, at a CAGR of 17%
- Employability
  - Cybersecurity if the most constrained sector
    - Job postings increased 100% since 2013.
- Impact of COVID-19.
  - increased amount of remote work …
  - expectation from robot fleet deployment …
    - Robots are allies during pandemics.

- Thank you !

UNIVERSITE D'ORLEANS

Selected Bibliography

Bertsekas, D. and Rhodes, I. (1971). Recursive state estimation for a set- membership description of uncertainty. IEEE Transactions on Automatic Control, 16(2):117–128.

Combastel, C. Zonotopes and Kalman observers: Gain optimality under distinct uncertainty paradigms and robust convergence, Automatica, 2015, 55, 265-273.

Degue K.H., D. Efimov, J. Le Ny,E. Feron. Interval Observers for Secure Estimation in Cyber-Physical Systems. 2018 IEEE Conference on Decision and Control (CDC), 2018, 4559-4564

Farokhi F., I Shames, and N Batterham. Secure and private control using semi-homomorphic encryption. Control Engineering Practice, 67:13 – 20, 2017.

Guerrero-Higueras A.M., N. DeCastro-García, and V. Matellán. Detection of cyber-attacks to indoor real time localization systems for autonomous robots. Robotics & Autonomous Systems, 99:75 – 83, 2018.

Jaulin L.. Robust set-membership state estimation; application to underwater robotics, Automatica, 2009, 45, 202-206

Jaulin, L. Nonlinear bounded-error state estimation of continuous-time systems, Automatica, 2002, 38, 1079-1082

Kieffer M., E. Walter. Guaranteed estimation of the parameters of nonlinear continuous-time models: Contributions of interval analysis. International Journal of Adaptative Control and Signal Processing, 2011, 25, 191-207

Kieffer, M.; Jaulin, L. & Walter, E. Guaranteed recursive non-linear state bounding using interval analysis, International Journal of Adaptative Control and Signal Processing, 2002, 16, 193-218

Kurzhanski, A. B. and Vályi, I. (1996). Ellipsoidal calculus for estimation and control. Birkhaüser Boston.

Lu A.-Y., G.-H. Yang. Secure Luenberger-like observers for cyber-physical systems under sparse actuator and sensor attacks Automatica, 2018, 98, 124 - 129

Mazenc, F. & Bernard, O. Interval observers for linear time-invariant systems with disturbances. Automatica , 2011, 47, 140 - 147

Meslem N., N. Ramdani. Interval observer design based on nonlinear hybridization and practical stability analysis. International Journal of Adaptive Control and Signal Processing, 2011, 25, 228-248

Meslem, N.; Ramdani, N. & Candau, Y. Using hybrid automata for set-membership state estimation with uncertain nonlinear continuous-time systems, Journal of Process Control, 2010, 20, 481-489

Milanese, M. & Novara, C. Unified Set Membership theory for identification, prediction and filtering of nonlinear systems, Automatica, 2011, 47, 2141 - 2151

Muniraj D. and M. Farhood. Detection and mitigation of actuator attacks on small unmanned aircraft systems. Control Engineering Practice, 83:188 – 202, 2019.

Rabehi D., N. Meslem, N. Ramdani. Secure interval observer for linear continuous-time systems with discrete measurements subject to cyber-attacks. IEEE SYSTOL'19, 2019,

Raïssi, T.; Efimov, D. & Zolghadri, A. Interval State Estimation for a Class of Nonlinear Systems, Automatic Control, IEEE Transactions on, 2012, 57, 260-265

Raïssi, T.; Ramdani, N. & Candau, Y. Bounded-error moving horizon state estimator for non-linear continuous-time systems : application to a bioprocess system, Journal of Process Control, 2005, 15, 537-545

Raïssi, T.; Ramdani, N. & Candau, Y. Set membership state and parameter estimation for systems described by nonlinear differential equations, Automatica, 2004, 40(10), 1771-1777

Schweppe, F. (1968). Recursive state estimation: Unknown but bounded errors and system inputs. IEEE Transactions on Automatic Control, 13(1):22–28.

Shoukry Y., P. Nuzzo, A.L. Sangiovanni-Vincentelli, S. A. Se- shia, G. J. Pappas, and P. Tabuada. SMC: Satisfiability modulo convex programming. Proceedings of the IEEE, 106:1655–1679, 2018.

Shoukry Y., P. Tabuada. Event-Triggered State Observers for Sparse Sensor Noise/Attacks. IEEE Transactions on Automatic Control, 2016, 61, 2079-2091