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
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
Networked controlled systems are prone to cyber-attacks.

- Under cyber-attacks, corrupted measurement data leads to corrupted control commands.
State Feedback Control

Physical system

\[ \dot{x} = Ax + Bu + \omega \]
\[ y = Cx \]

Controller

\[ u = K(x, x_D) \]

Network

- disturbance \( \omega \)
- actuator attack
- sensor attack \( a \)

\[ \tilde{y} = y + \epsilon + a \]

\[ x \]

\[ x_d \]
Output Feedback Control

\begin{align*}
    \dot{x} &= Ax + Bu + \omega \\
y &= Cx
\end{align*}

\begin{align*}
    \hat{x} &= A\hat{x} + Bu + L(\tilde{y} - C\hat{x}) \\
u &= K(\hat{x}, x_D)
\end{align*}

Network

- disturbance \( \omega \)
- actuator attack

Plant

- noise \( \epsilon \)

Sensor attack \( a \)

Observer

Controller

- \( x_d \)
Models of Cyber-Attacks and Mitigation Strategies
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

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
  \[ y_a(t) = \emptyset \]

- 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 of cyber-attacks

- **FDI FTC** methods and algorithms are good candidates
  - [Debaji, et al., Annual Reviews in Control, 2019] …

- Cyber-attacks <> ‘Random’ faults
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

$u \rightarrow \text{Physical system} \rightarrow y$
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 …
Control using **encrypted** data

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

*They provide strong privacy and security guarantees for the closed-loop system at the cost of extra computations* (Farokhi, et al., CEP, 2017).
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 \textit{s-sparse observable}, if and only if

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

(ii) system is \textit{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 \( \frac{n!}{s!(n-s)!} \) 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 the bounded-error framework

- **Set membership predictor-corrector algorithms**
  - Can handle corrupted data as outliers.

- **Interval observers**
  - Have been extended to handle cyber-attacks.
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)

- $n = 3$ boxes
- $(2n-1)^2 = 25$ boxes
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
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/pylbex
Robust Localization

TOF
2 beacons

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

TOF

4 beacons

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

TOF
4 beacons

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

TOF
4 beacons
1 corrupted

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

TOF
1-relaxed
Intersection

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

TOF
1-relaxed
Intersection

Spurious datum identified

Figures obtained using PYIBEX tool.
benensta.github.io/pylbex
Example #2.
Robot localisation via TDoA Multilateration

- Can measure the distance \textit{difference} to beacons
- TDoA. \textit{Time Difference of Arrival}
- \textit{Bounded-error} framework
Robust Localization

TDoA
4 beacons
no corruption

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

TDoA
4 beacons
no 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/pylbex
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/pylbex
Secure 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 $\overline{x}(t)$
  
  $\underline{x}(t) \leq x(t) \leq \overline{x}(t)$

\[
\dot{x}(t) = Ax(t) + Bu(t) + \omega(t)
\]
\[
y(t) =Cx(t) + \epsilon(t)
\]
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
Resilience to *stealthy* attacks

Working assumptions for observer synthesis

- Continuous-time measurement
- Strong assumptions on invertibility
- Strong assumptions $\exists L, A - LC$ 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

resilient
non-resilient
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 \textit{s}-sparse observable
  - Sensor attacks are \textit{distinguishable}

- Build a \textit{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**

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

$x(t_k^+) = x(t_k) + L \left( Cx(t_k) - e(t_k) - y(t_k) \right)$
Interval Impulsive Observer

\[ t \in [t_{k-1}, t_k], \quad \dot{x}(t) = A x(t) + B u(t) \]

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

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

$A = A_M - A_N,$
$A_M$ is Metzler,
$A_N > 0$
Interval Impulsive Observer

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

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

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

\[ \dot{x}(t) = A_M x(t) - A_N \bar{x}(t) + Bu(t) \]
\[ \bar{x}(t) = A_M \bar{x}(t) - A_N \underline{x}(t) + Bu(t) \]

(Rabehi, et al, SYSTOL 2019)
\[ t \in [t_{k-1}, t_k], \quad \dot{x}(t) = Ax(t) + Bu(t) \]

\[ x(t_k^+) = x(t_k) + L \left( Cx(t_k) - e(t_k) - y(t_k) \right) \]

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

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

\[ \dot{x}(t) = A_M x(t) - A_N \bar{x}(t) + Bu(t) \]

\[ \bar{x}(t) = A_M \bar{x}(t) - A_N \bar{x}(t) + Bu(t) \]

(Rabehi, et al, SYSTOL 2019)
Interval Impulsive Observer

\[ A = A_M - A_N, \]
\[ A_M \text{ is Metzler,} \]
\[ A_N > 0 \]

\[
\begin{align*}
\dot{x}(t) &= A_M x(t) - A_N \bar{x}(t) + B u(t) \\
\bar{x}(t) &= A_M x(t) - A_N \bar{x}(t) + B u(t)
\end{align*}
\]

\( t \in [t_{k-1}, t_k] \)

open-loop estimator

(Rabehi, et al, SYSTOL 2019)
Interval Impulsive Observer

\[
\begin{align*}
\bar{x}(t_k^+) &= (I + \underline{L}C)^+ \underline{x}(t_k) - (I + \underline{L}C)^- \overline{x}(t_k) - \|\underline{L}\| \bar{e}(t_k) - \underline{L}y(t_k) \\
\overline{x}(t_k^+) &= (I + \overline{L}C)^+ \underline{x}(t_k) - (I + \overline{L}C)^- x(t_k) - \|\overline{L}\| \bar{e}(t_k) - \overline{L}y(t_k)
\end{align*}
\]

\[
A = A_M - A_N, \\
A_M \text{ is Metzler,} \\
A_N > 0
\]

open-loop estimator \( t \in [t_{k-1}, t_k] \)
\[
\begin{align*}
\dot{\underline{x}}(t) &= A_M \underline{x}(t) - A_N \overline{x}(t) + Bu(t) \\
\dot{\overline{x}}(t) &= A_M \overline{x}(t) - A_N \underline{x}(t) + Bu(t)
\end{align*}
\]

impulsive correction when measurement is available

(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**

\[
\begin{align*}
    t \in [t_{k-1}, t_k], & \quad \dot{x}(t) = A_M x(t) - A_N \bar{x}(t) + B u(t) \\
    \bar{x}(t) = A_M \bar{x}(t) - A_N \hat{x}(t) + B u(t)
\end{align*}
\]

**Impulsive correction when measurement is available**

\[
\begin{align*}
    \underline{x}(t_k^+) &= (I + LC)^+ \underline{x}(t_k) - (I + LC)^- \bar{x}(t_k) - |L| \bar{e}(t_k) - L y(t_k) \\
    \bar{x}(t_k^+) &= (I + LC)^+ \bar{x}(t_k) - (I + LC)^- \underline{x}(t_k) - |L| \bar{e}(t_k) - L y(t_k)
\end{align*}
\]
Secure Interval Observer

Our approach (Rabehi, et al, SYSTOL 2019)

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

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

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

Our approach (Rabehi, et al, SYSTOL 2019)

- **Resilience to deception attacks**
- **Selection strategy** at each time step $t_k$

- Use $\frac{n!}{s!(n-s)!}$ observers on every subset of $n - s$ sensors

- Compute $\frac{n!}{s!(n-s)!}$ 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

![Graph showing Secure Interval Observer results]

- $x_1$
- $\bar{x}_1$
- $\bar{x}_1$
- $x_1$ — attacked
- $\bar{x}_1$ — attacked
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
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 is the most constrained sector
  - Job postings increased 100% since 2013.


- Increased amount of remote work …
- Expectation from robot fleet deployment …
  - Robots are allies during pandemics.
Thank you!


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


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


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

