Syracuse University
College of Engineering & Computer Science

Adaptive Sensor Attack Detection for Cyber-Physical Systems

* **accepted by** 59th Design Automation Conference (**DAC**), **2022**

#77

Cyber-Physical Systems Lab.

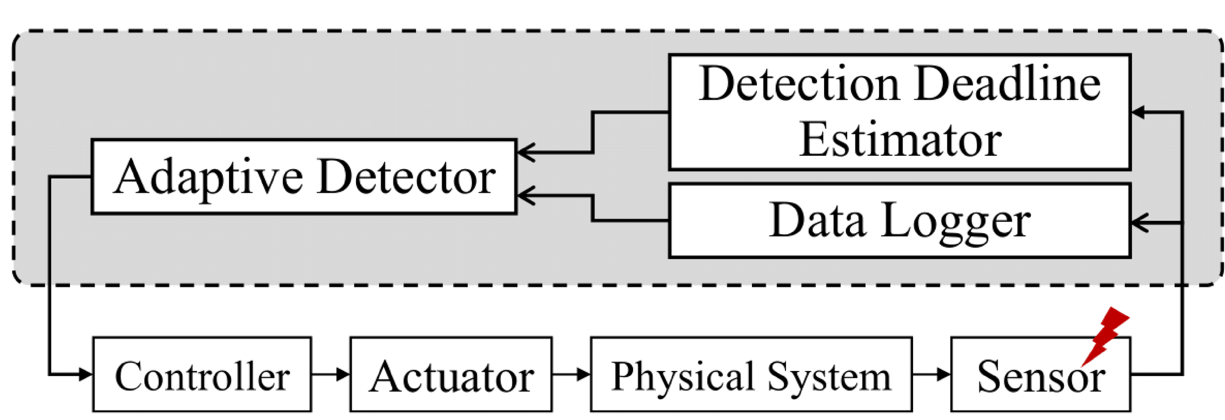
Lin Zhang **Advisor: Dr. Fanxin Kong**
Department of Electrical Engineering and Computer Science

SCAN for PDF

Introduction

- Cyber-Physical Systems (**CPS**) are engineered systems combining computation, communications, and physical resources. e.g. self-driving car, drone, smart grid
- One crucial security risk in CPS is sensor attacks, which have motivated many researches on **attack detection**.
- Existing detection works overlooks the trade-off between **detection delay** and **false alarms**, but we argue that attack detection should **dynamically balance** the two metrics at different physical states.
- **Challenges:**
  - **timing** is essential for safety-critical CPS.
  - it is non-trivial to calculate a safe deadline in an **online** manner.
  - **detection delay** should be less than **deadline**, but a shorter delay is not always favorable.
- **Our contributions:** we propose a real-time **adaptive** attack detection system that can **dynamically** adjust detection delay and thus false alarms according to the varying system state.

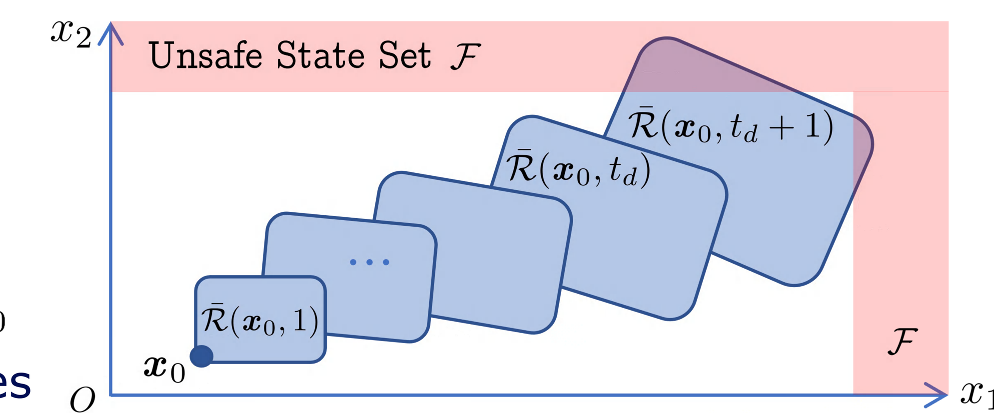
Design Overview



- **Detection Deadline Estimator:**
  - **reachability-based** technique
  - dynamically **estimate** the detection deadline
- **Adaptive Detector:**
  - **window-based** detection algorithm
  - dynamically **adapt** its detection delay
- **Data Logger:**
  - **sliding-window based** data logging protocol
  - keeps trustworthy **data** for the deadline estimation and attack detection

Detection Deadline Estimation

- Safety Analysis
  - System dynamics $x_{t+1} = Ax_t + Bu_t + v_t$
  - **Reachable set** $\mathcal{R}$ includes all possible system states evolving from initial state x_0
  - If reachable set **over-approximation** does **not intersect** with unsafe set, i.e. $\bar{\mathcal{R}} \cap \mathcal{F} = \emptyset$, the system is guaranteed to be safe
- Over-approximation of the Reachable Set
  - $$x_t \subseteq \bar{\mathcal{R}}(x_0, t) = A^i \bar{x}_0 \oplus \bigoplus_{j=0}^{i-1} A^j B \mathcal{B}_{\mathcal{U}} \oplus \bigoplus_{k=0}^{i} A^k \mathcal{B}_\epsilon$$
  - $\oplus$ denotes the Minkowski sum



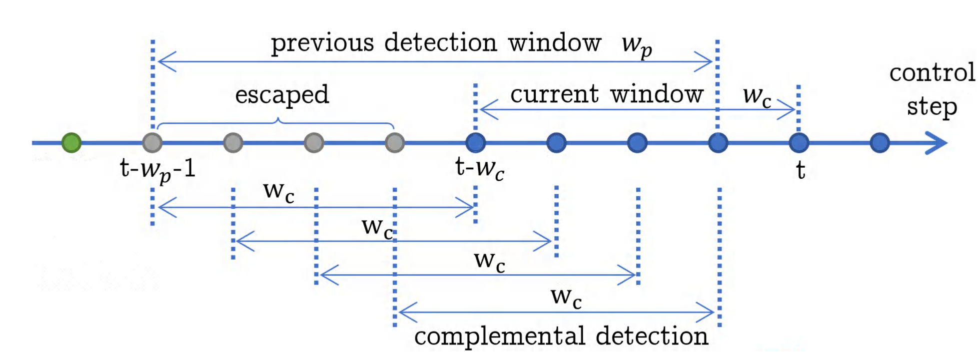
Searching Process for the Detection Deadline t_d

- Bound through Support Function

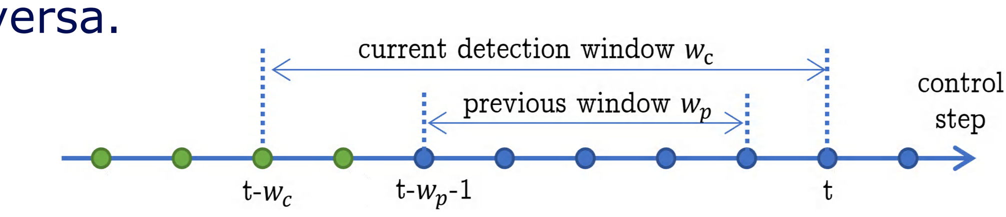
$$l^T A^t x_0 + \sum_{i=0}^{t-1} l^T A^i B c + \sum_{i=0}^{t-1} \|(A^i BQ)^T l\|_1 + \sum_{i=0}^{t-1} \epsilon \|(A^i)^T l\|_2$$
$$l^T A^t x_0 + \sum_{i=0}^{t-1} l^T A^i B c - \sum_{i=0}^{t-1} \|(A^i BQ)^T l\|_1 - \sum_{i=0}^{t-1} \epsilon \|(A^i)^T l\|_2$$

Adaptive Window based Attack Detection

- This basic detection algorithm tracks the **average residual** between predicted and observed states within a detection **window**.
- The detection window should not longer than the detection deadline for safety.
- With a **longer detection delay**, detector tends to have **lower false alarm rates** but may miss the detection deadline; and vice versa.
- We design a protocol that can dynamically **adapt the detection delay** and thus false alarms to meet the detection **deadline** and improve **usability**. The protocol guarantees that **no data escape** from detection due to the change of detection window size.



Decreasing the Detection Window Size



Increasing the Detection Window Size

Data Logging Protocol

- We design a **sliding-window** based logging protocol to record historical **residuals** and **state estimates**. The sliding window moves forward as time ticks.
- At each control step t, the protocol **buffers**, **holds**, and **releases** certain data points. Buffered data can be compromised, and data outside the current window is regarded trustworthy and thus held.

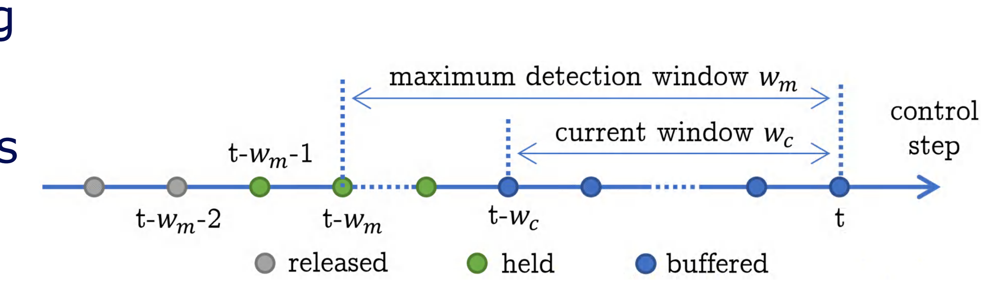
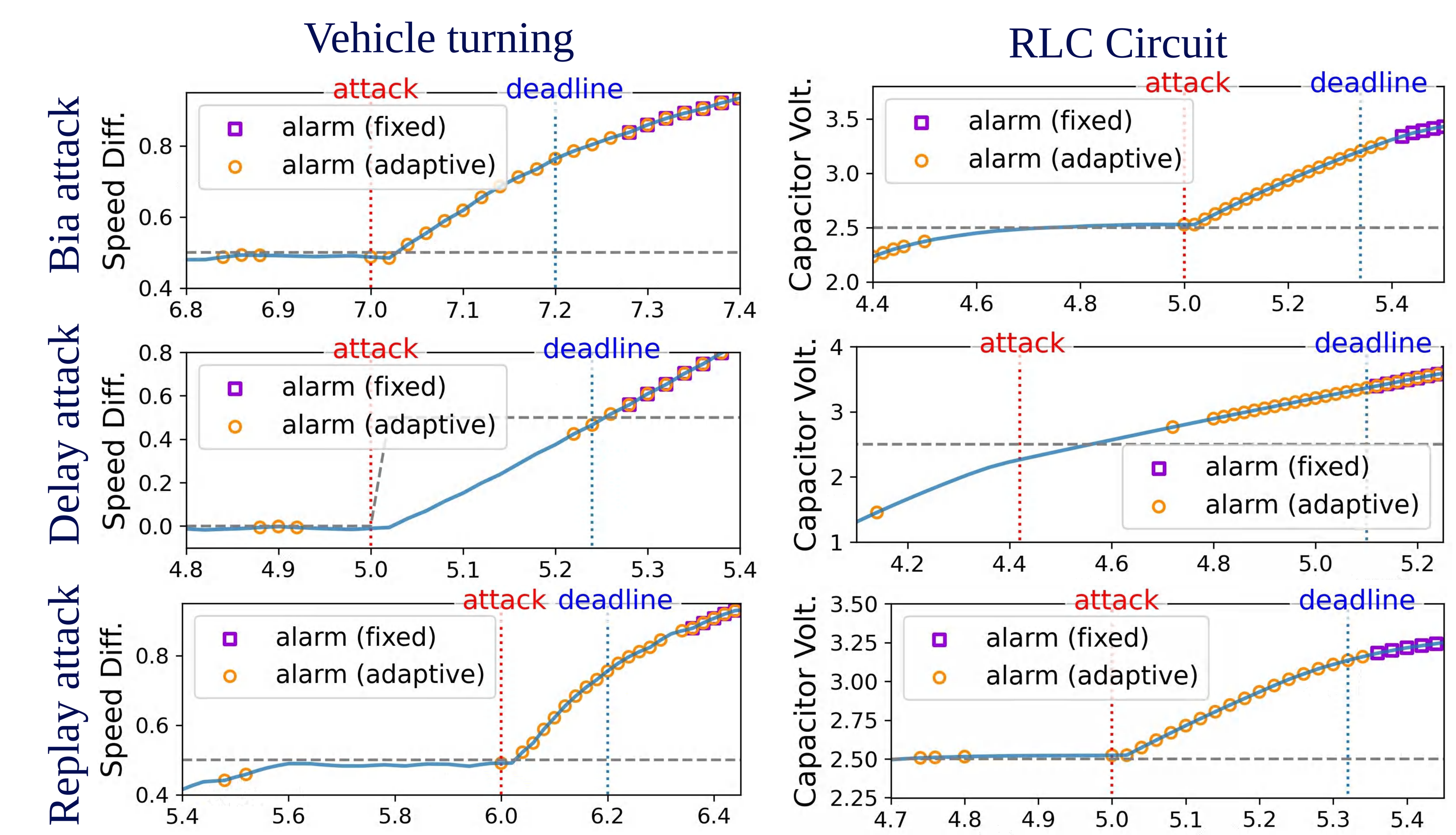


Illustration of the Data Logger

Results of the Adaptive Detector

- Comparison of detection result between adaptive window size and a fixed window size



- false positive and deadline miss numbers out of 100 simulations for each case

Simulator	Attack	Strategy	#FP	#DM
Aircraft Pitch	Bias	Adaptive	73	0
		Fixed	42	96
	Delay	Adaptive	3	0
		Fixed	2	97
	Replay	Adaptive	34	0
		Fixed	8	100
Quadrotor	Bias	Adaptive	73	7
		Fixed	55	99
	Delay	Adaptive	6	0
		Fixed	2	87
	Replay	Adaptive	6	0
		Fixed	2	59

Testbed Results