State Consistencies for Cyber-Physical System Recovery

Fanxin Kong, *Syracuse University*
Oleg Sokolsky, James Weimer, Insup Lee, *University of Pennsylvania*

Syracuse University
Department of Electrical Engineering and Computer Science

April 15, 2019

Cyber-Physical Systems




We are living in a Cyber-Physical System world!

Security

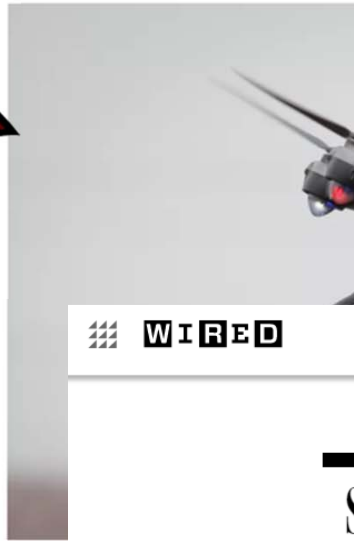
SECURITY DRONES CYBERSECURITY

The U.S. government showed just how easy it is to hack drones made by Parrot, DBPower and Cheerson

Researchers took complete control

By April Glaser | @aprilaser | Jan 4, 2017, 5:07pm EST

TWEET SHARE LINKEDIN



NEWSLETTER I SUBSCRIBE FAST COMPANY

TECHNOLOGY LEADERSHIP ENTERTAINMENT IDEAS VIDE

High-Tech Pirates: Researchers Hack A Yacht Via GPS

Car hackers use laptop to control standard car

WIRED Hackers Gain Direct Access to US Power Grid Controls

ANDY GREENBERG SECURITY 09.06.17 06:00 AM

SHARE

HACKERS GAIN DIRECT ACCESS TO US POWER GRID CONTROLS

BITS | Security Researchers Find a Way to Hack Cars

SECURITY

Security Researchers Find a Way to Hack Cars

BY NICOLE PERLROTH JULY 21, 2015 2:32 PM 101

SHARE

SHARE 206842

TWEET

COMMENT

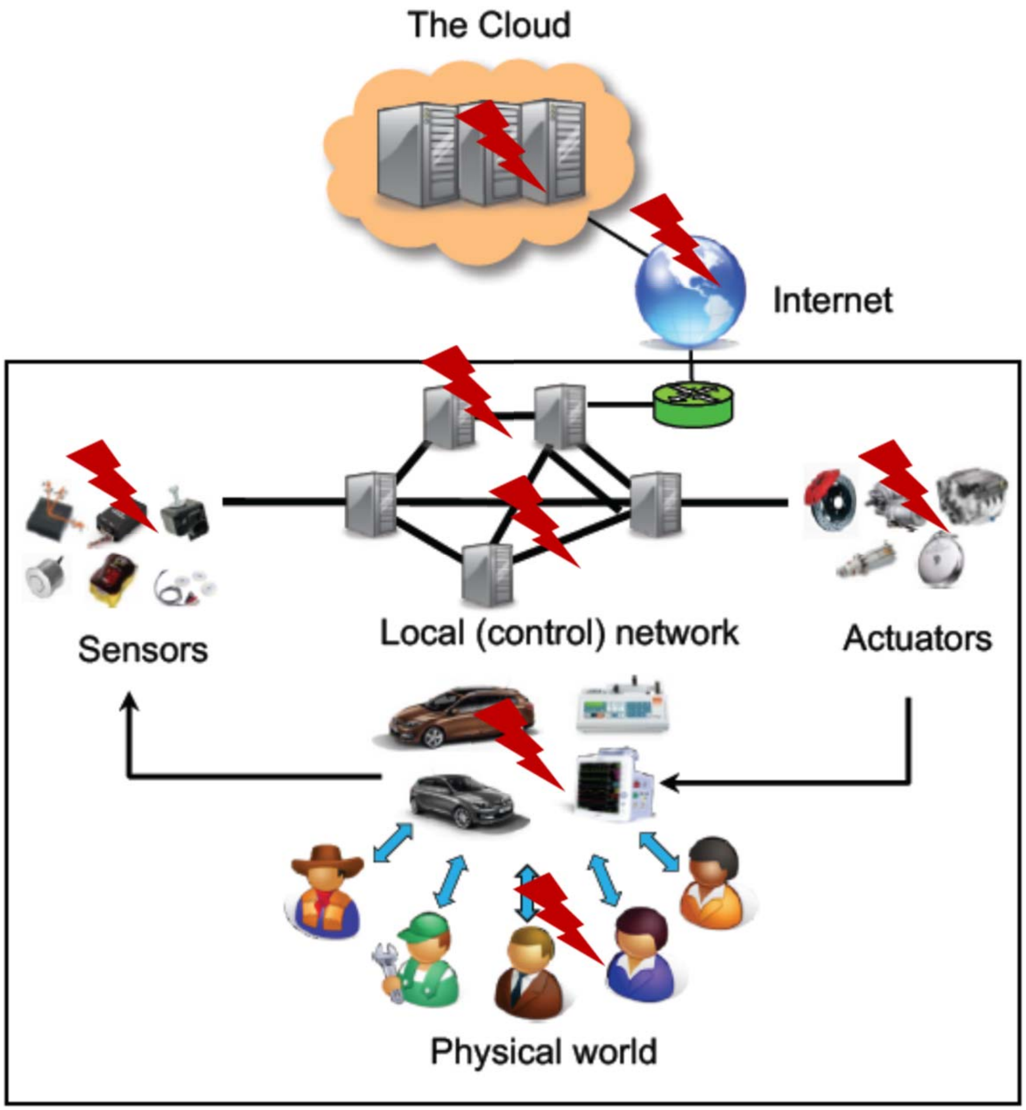
ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me i...

CPS Attack Surfaces

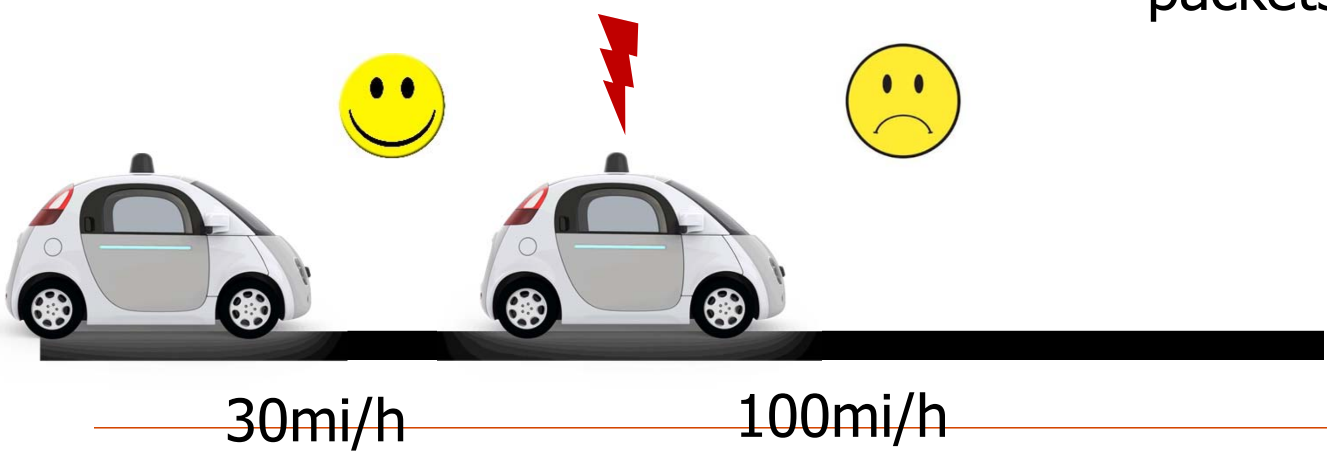
- Cyber attack surfaces
  - e.g., communication, networks, computers, ...
- Environmental attack surfaces
  - e.g., GPS signal, electro-magnetic interference, ...
- Physical attack surfaces
  - e.g., locks, casings, cables, …
- Human attack surfaces
  - e.g., phishing, blackmail, …

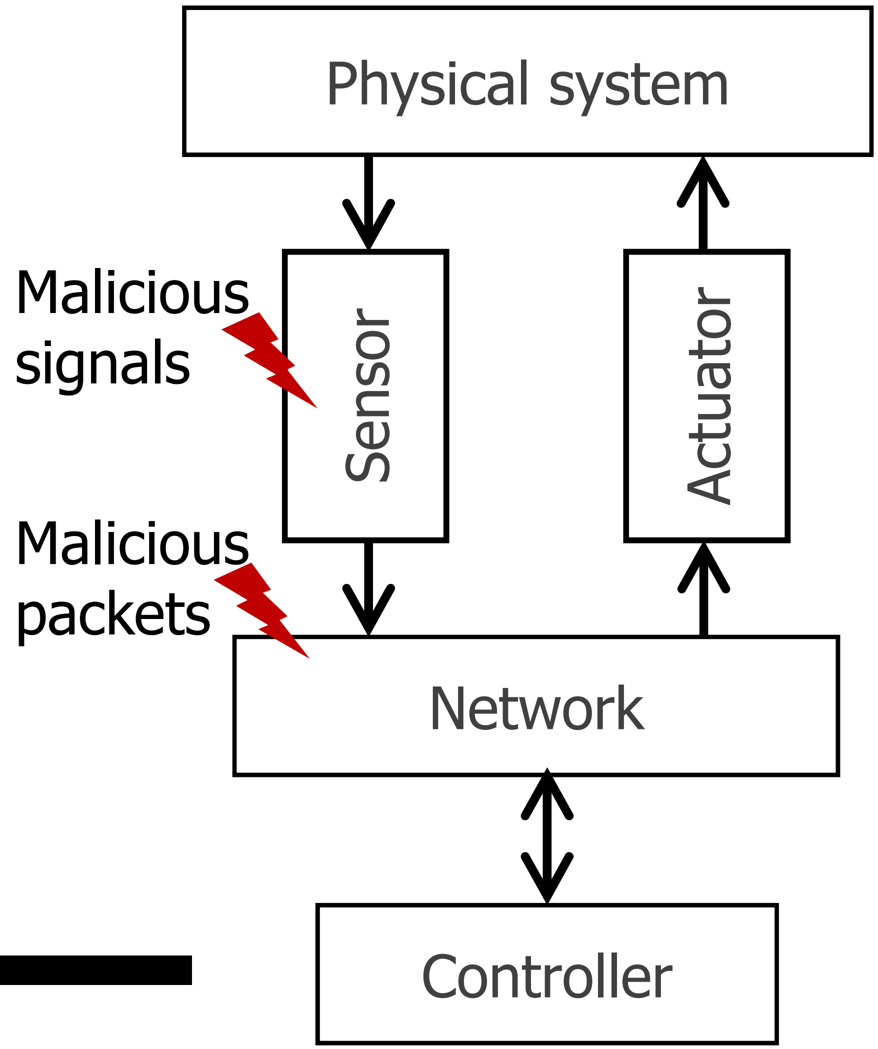


What we study and why?

Target: *Sensor Attacks*

- The attacker can arbitrarily change sensor measurements





What we study and why?

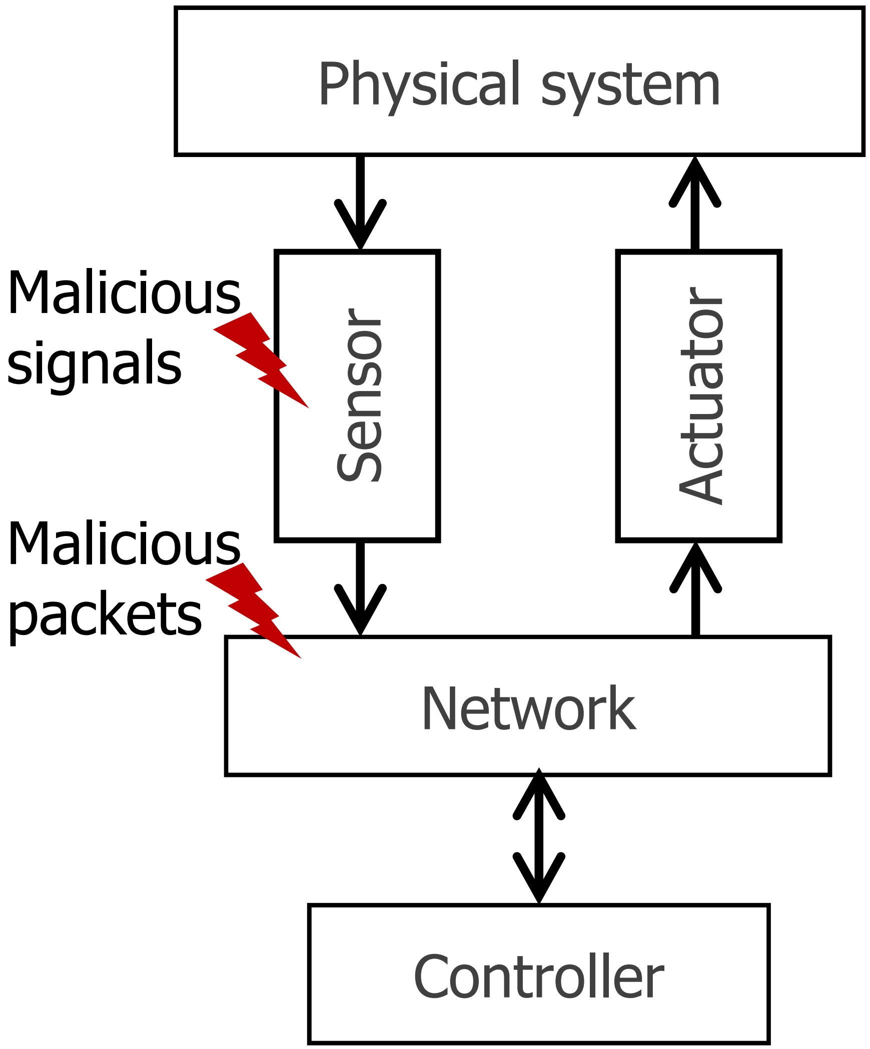
Target: ***Sensor Attacks***

- The attacker can arbitrarily change sensor measurements

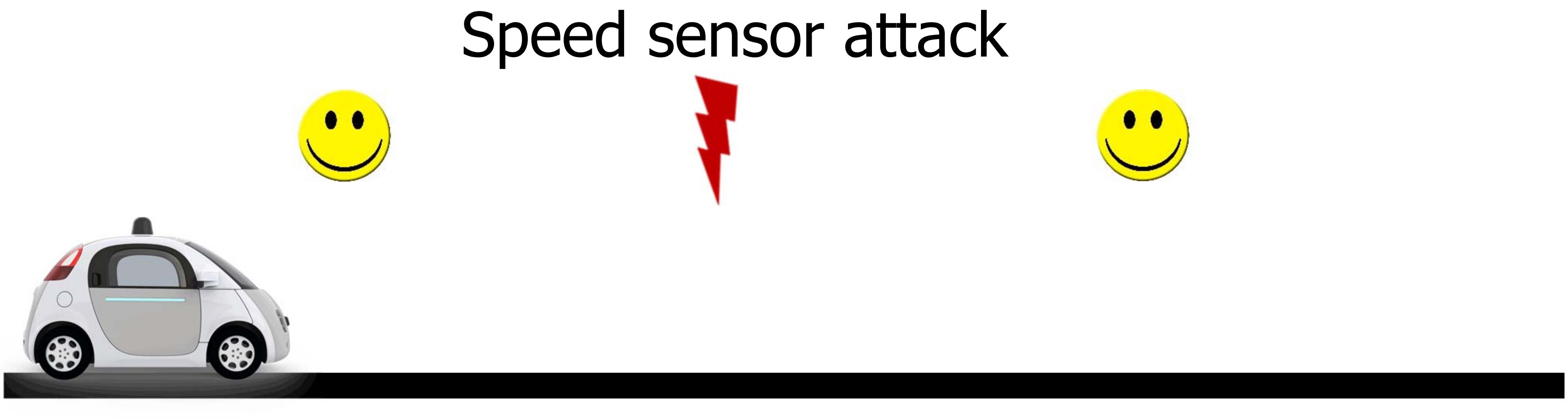
  - environmental attack surfaces
  - cyber attack surfaces

Goal: ***Resilience***

- To ensure control performance under sensor attacks



Ideally…



- Ideally, the system performs (almost) the same as if there is no attack
  - Example: cruise control under a speed sensor attack

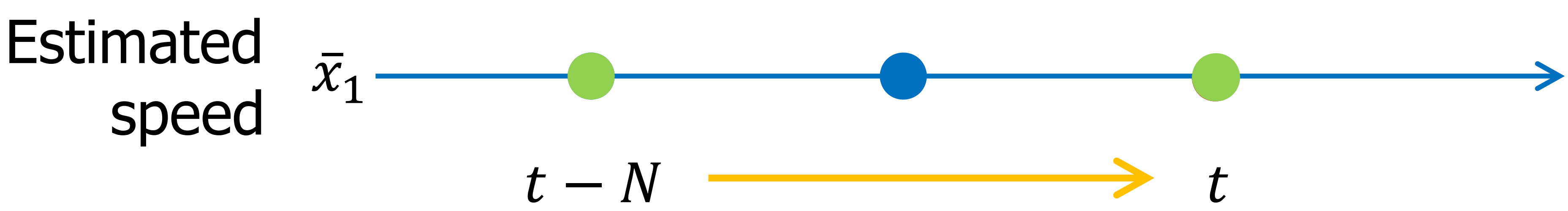
Outline

- Background
- Review on CPS recovery
  - Roll-forward recovery
  - How well does it work
- State consistencies for CPS recovery
  - Consistency definitions
  - Evaluation
- Conclusion

CPS recovery

Roll-forward recovery: Rolling the system to the current time by starting from a consistent cyber-physical-state

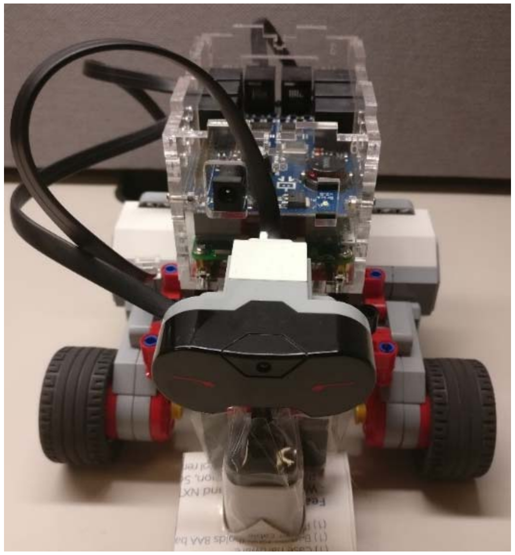
Prediction using historical state



- Example: model-based prediction (ICCPS2018)

Scenario: travelling in a straight line

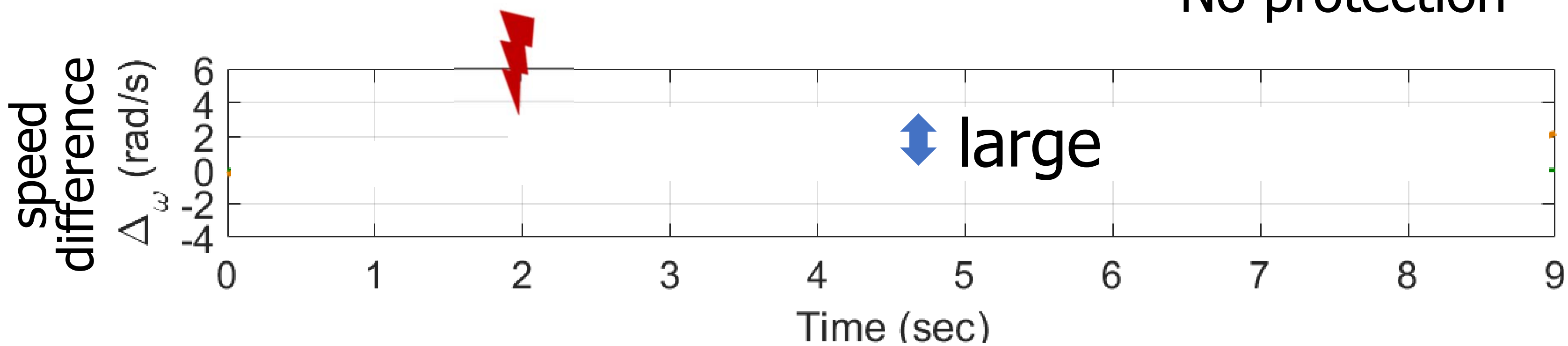
- Testbed: an unmanned vehicle. Each front wheel is driven by a motor, and each motor has a speed sensor



- Goal: to keep a vehicle travel in a straight line, i.e., the two front wheels have the same speed
- Controller: a PID controller supervises and controls the speed difference of the two front wheels
- Attack: the attacker modifies a speed sensor’s measurements to a constant value

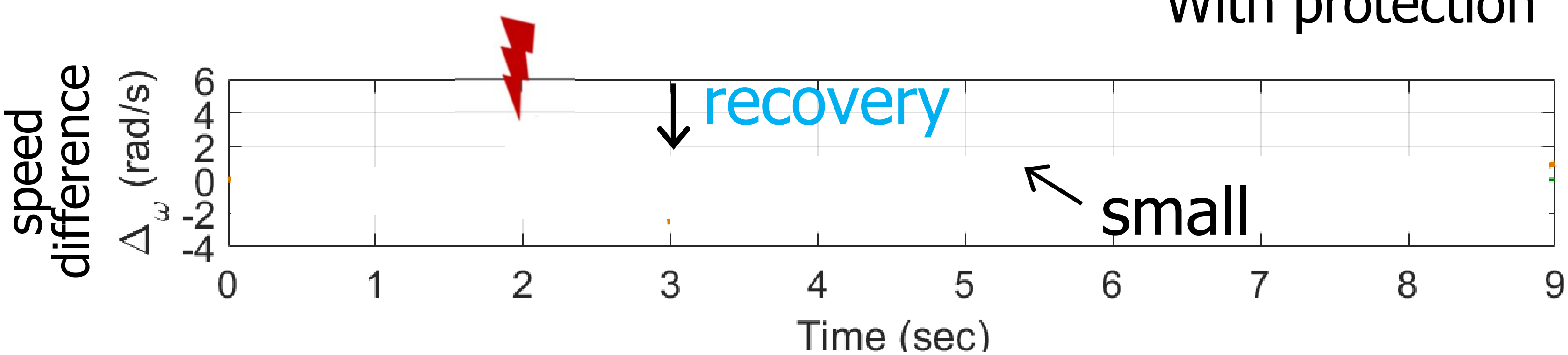
How well does it work?

No protection



The vehicle keeps turning

With protection



The vehicle travels almost straightly

--- desired Δ —actual Δ

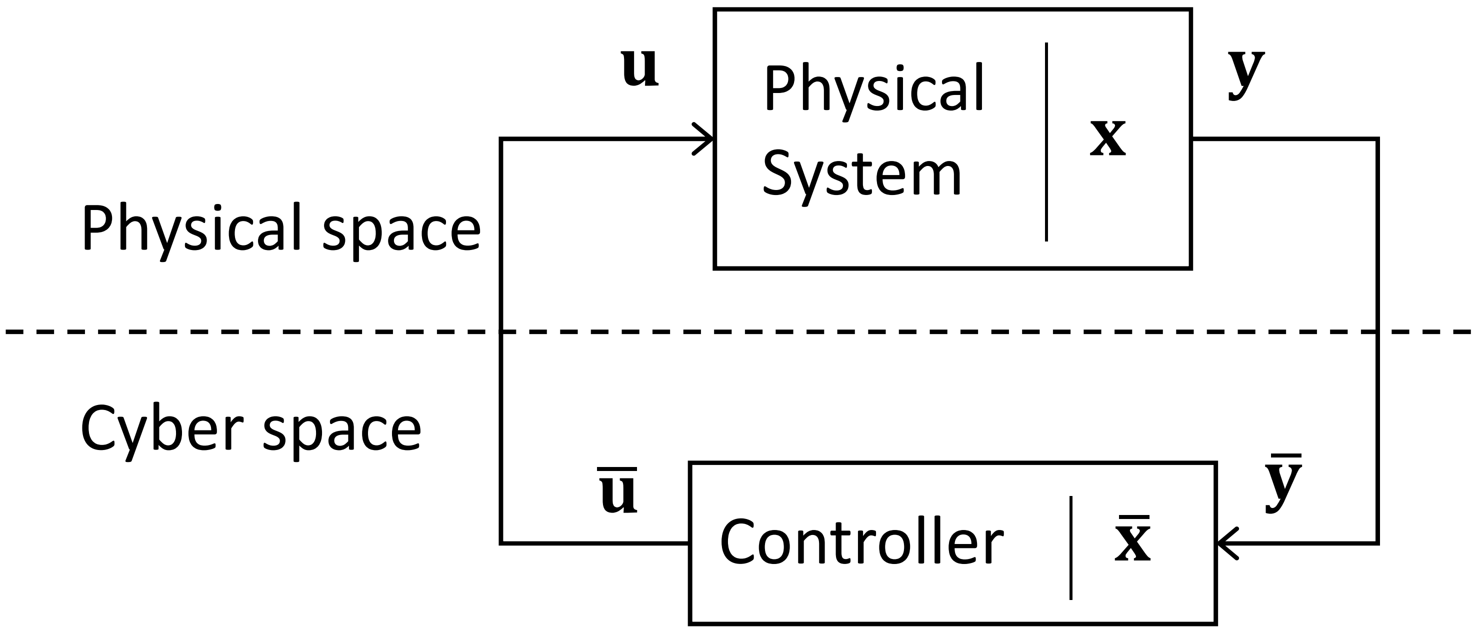
What kind of states is used?

We use ***Consistent Cyber-Physical States***

- *Cyber-physical states*: the cyber information that reflects physical states
- *Cyber-physical consistency*: whether the physical state can be accurately reflected by the corresponding cyber information

Cyber-physical logic-consistency	
Cyber-physical timing-consistency	
Synchronization	Freshness

A system diagram of CPS



A cyber-physical state is denoted as $\bar{\mathbf{c}} = \{\bar{\mathbf{x}}, \bar{\mathbf{u}}\}$

Cyber-Physical Logic-Consistency

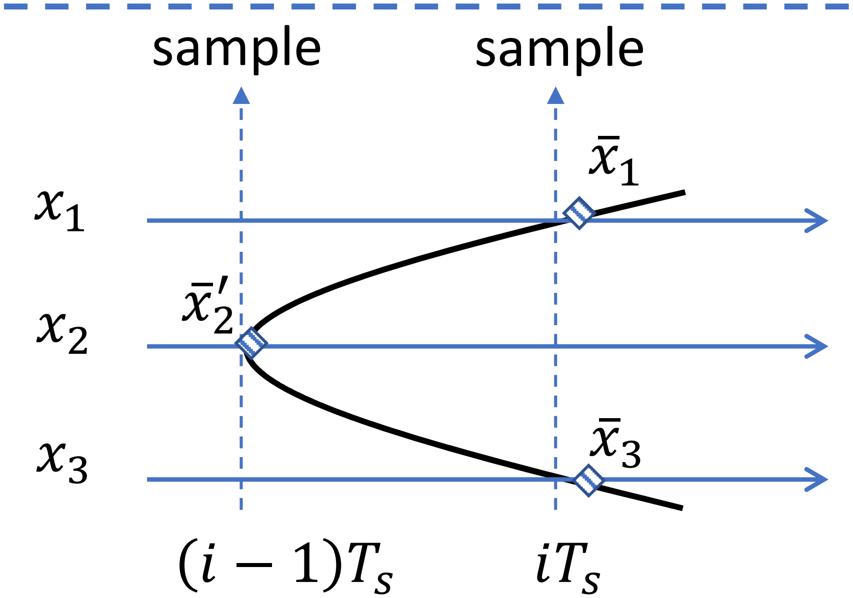
DEFINITION 1 (CYBER-PHYSICAL LOGIC-CONSISTENCY). *A cyber-physical state* $\bar{c} = \{\bar{x}, \bar{u}\}$ *is logic-consistent if*

$$\{|\bar{x} - x| \leq \Delta V_x\} \tag{1}$$

$$\wedge \{|\bar{u} - u| \leq \Delta V_u\}, \tag{2}$$

where ΔV_x *and* ΔV_u *denote the given estimation error and actuation error, respectively, that a system can tolerate.*

The logic-consistency is confined to values, is NOT enough.



Cyber-Physical Timing-Consistency

DEFINITION 2 (CYBER-PHYSICAL TIMING-CONSISTENCY). *A cyber-physical state* $\bar{c} = \{\bar{x}, \bar{u}\}$ *is timing-consistent if it satisfies*

(1) *Syn-Timing-Consistency:*

$$\{|\max_{\forall i} t(\bar{x}_i) - \min_{\forall j} t(\bar{x}_j)| \leq \Delta T_x\} \tag{3}$$

$$\wedge\{|\max_{\forall j} t(\bar{u}_j) - \min_{\forall i} t(\bar{x}_i)| \leq T_s\}, \tag{4}$$

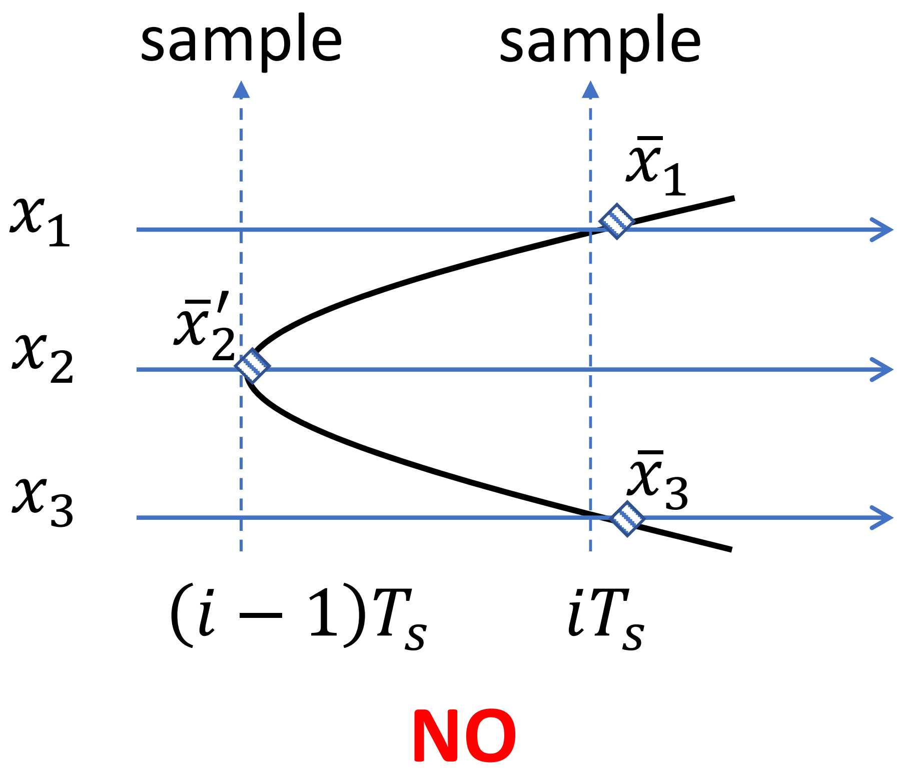
where ΔT_x *denotes the maximum difference of states' time stamps that a system can tolerate;* T_s *is the sampling period.*

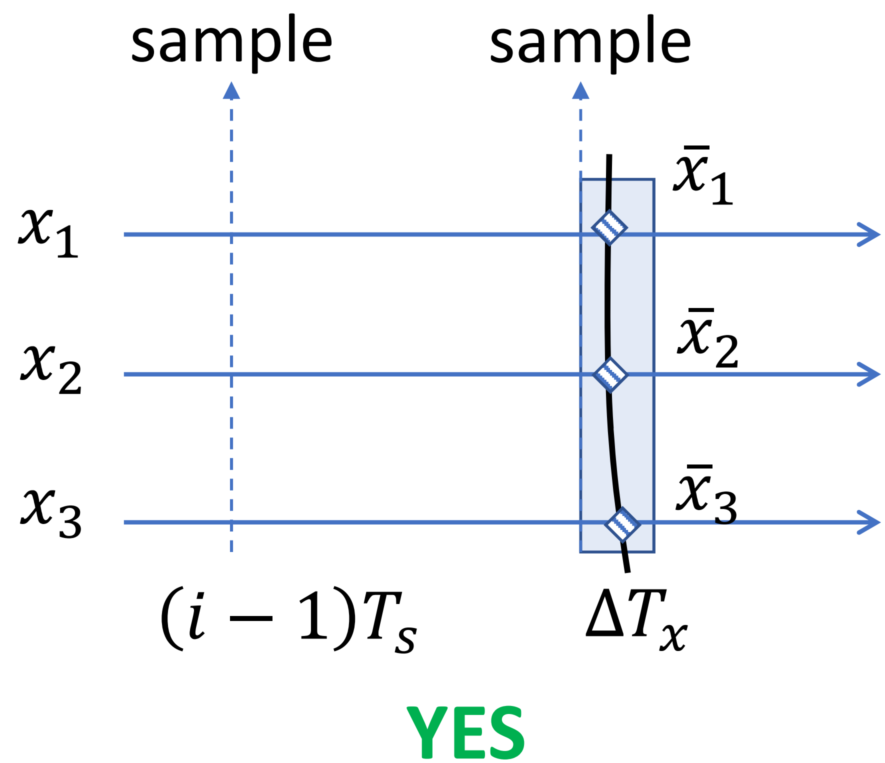
(2) *Exp-Timing-Consistency:*

$$q(\bar{c}) \geq h, \tag{5}$$

where $q(\cdot)$ *is the expire time of a cyber-physical state and* h *denotes the current time.*

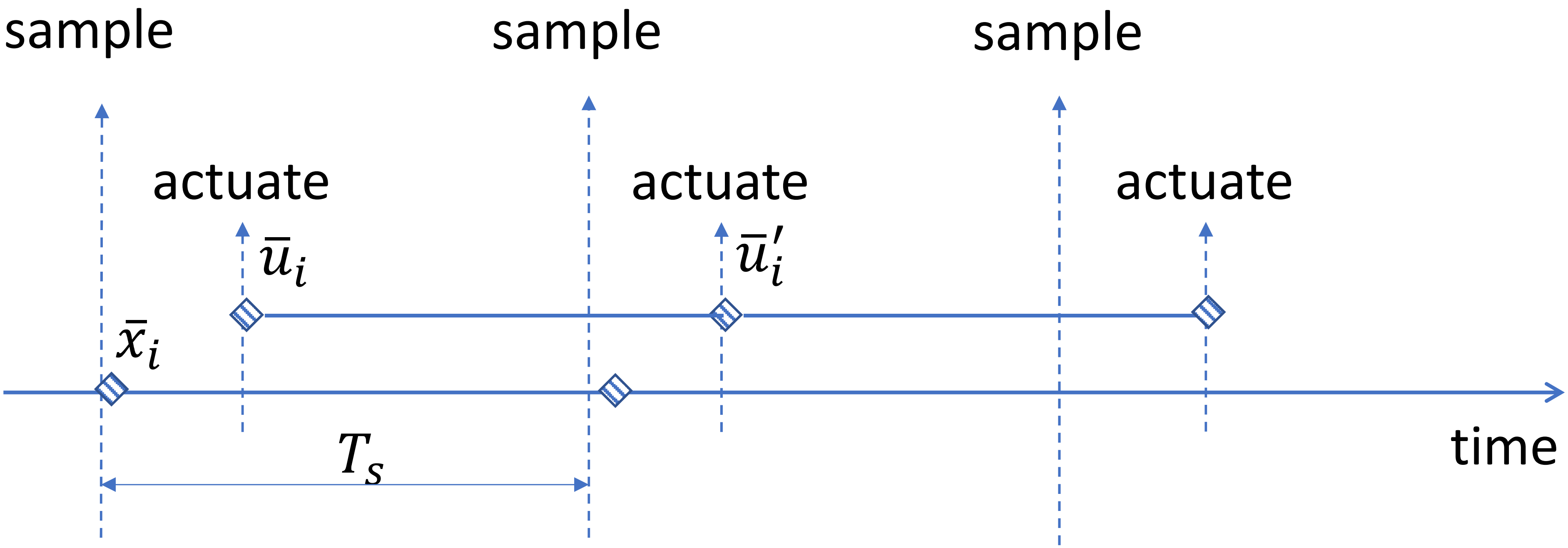
(1) Syn-Timing-Consistency (1/2)





$$\{|\max_{\forall i} t(\bar{x}_i) - \min_{\forall j} t(\bar{x}_j)| \leq \Delta T_x\}$$

(1) Syn-Timing-Consistency (2/2)

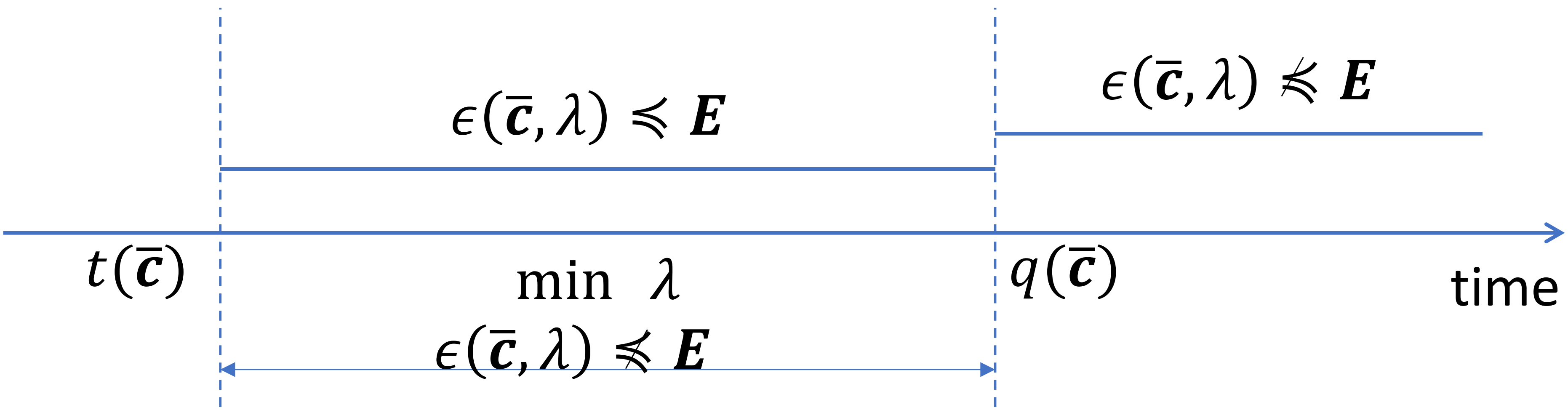


$\{\bar{x}_i, \bar{u}_i'\}$: **NO** $\{\bar{x}_i, \bar{u}_i\}$: **YES**

$$\{|\max_{\forall j} t(\bar{u}_j) - \min_{\forall i} t(\bar{x}_i)| \le T_s\}$$

(2) Exp-Timing-Consistency

Calculating the expire time



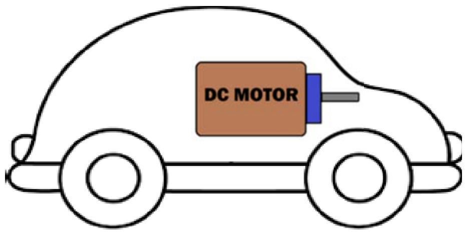
$$q(\bar{c}) = \min_{\epsilon(\bar{c},\lambda) \npreceq E} \lambda + t(\bar{c})$$

The error of state prediction is unacceptable

Evaluation

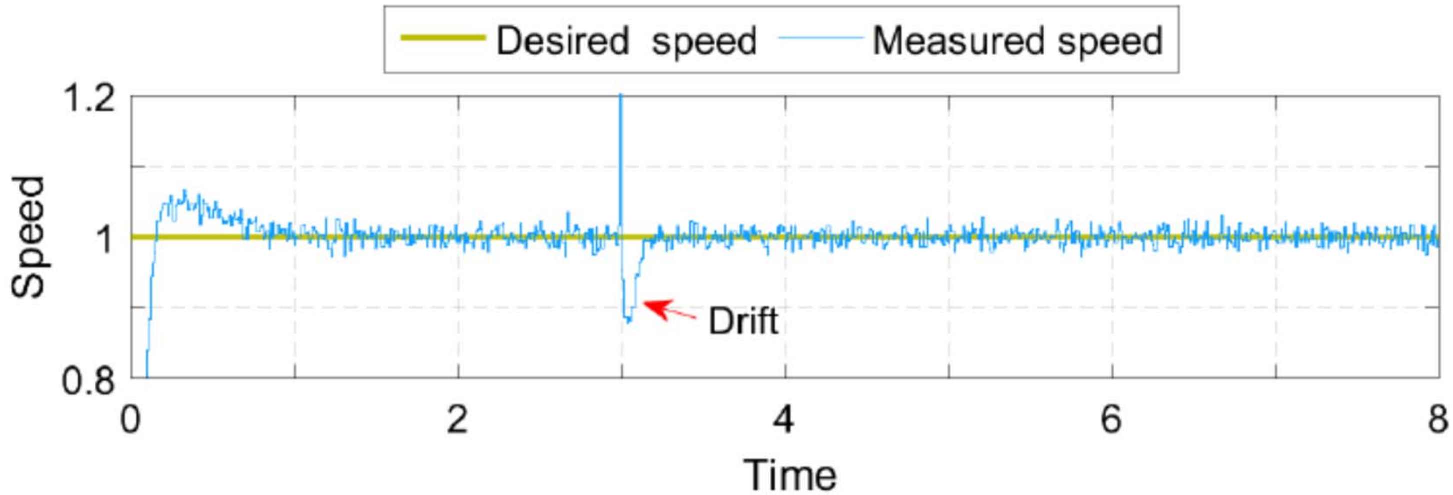
- Goal: to keep a vehicle travel at a constant speed
- Simulator: DC motor speed control using PID controller

$$\begin{bmatrix} \dot{i} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} -\frac{R}{L} & -\frac{K_b}{L} \\ \frac{K_m}{J} & -\frac{K_f}{J} \end{bmatrix} \begin{bmatrix} i \\ \omega \end{bmatrix} + \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix} v$$



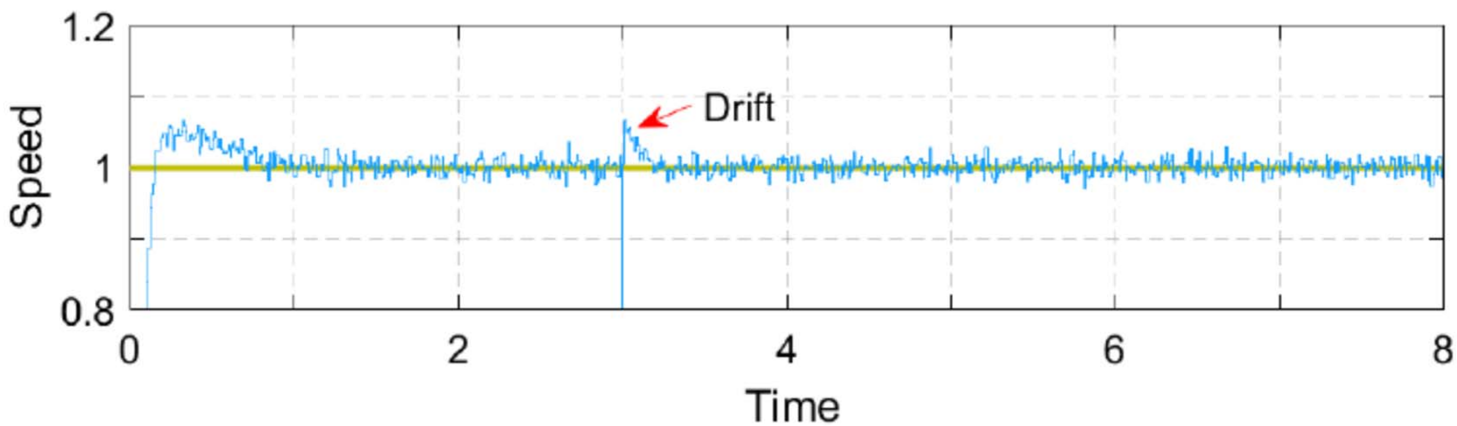
- Scenario: an attack is found out and the system performs recovery ONCE to predict the current state

Violating Logic-Consistency



$$\{|\bar{x} - x| \leq \Delta V_x\}$$

(a) Violating Eqn. (1), one sampling period back recovery.

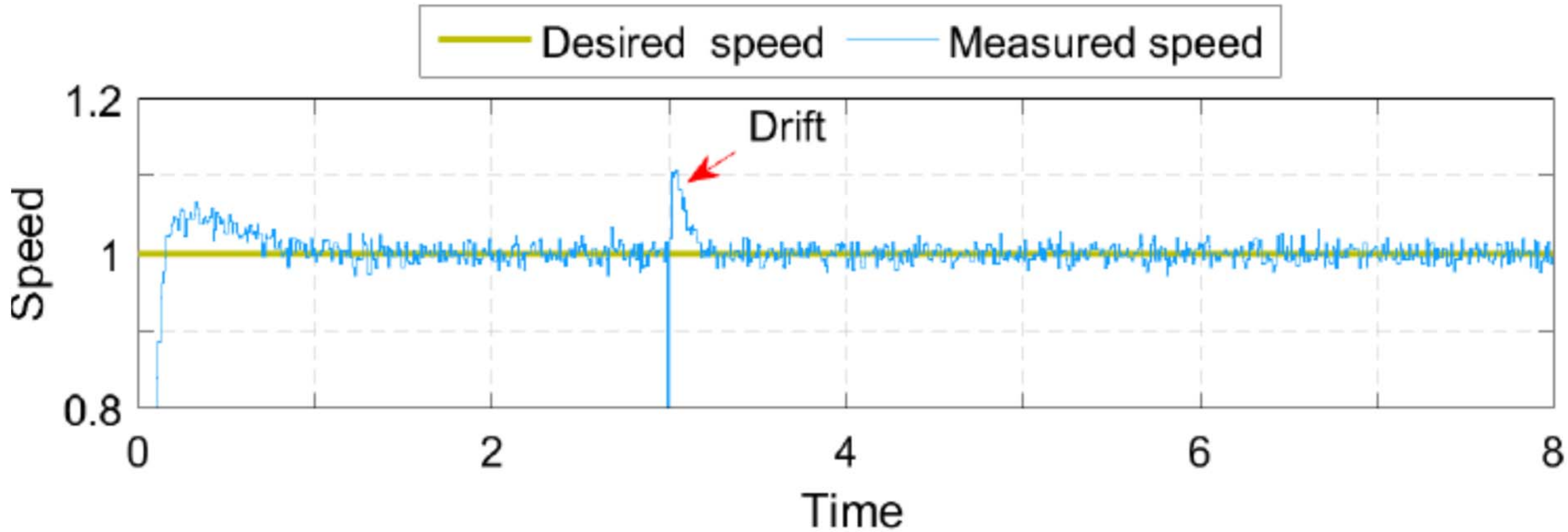


$$\{|\bar{u} - u| \leq \Delta V_u\}$$

(b) Violating Eqn. (2), one sampling period back recovery.

Violating Syn-Timing-Consistency

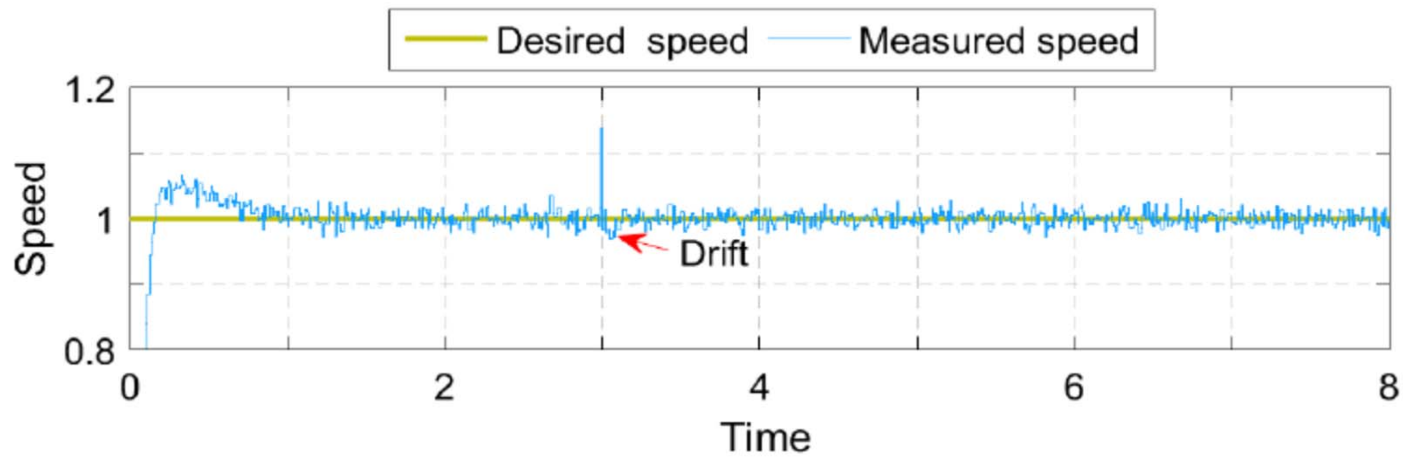
Current (i) and speed (ω) have different time stamps



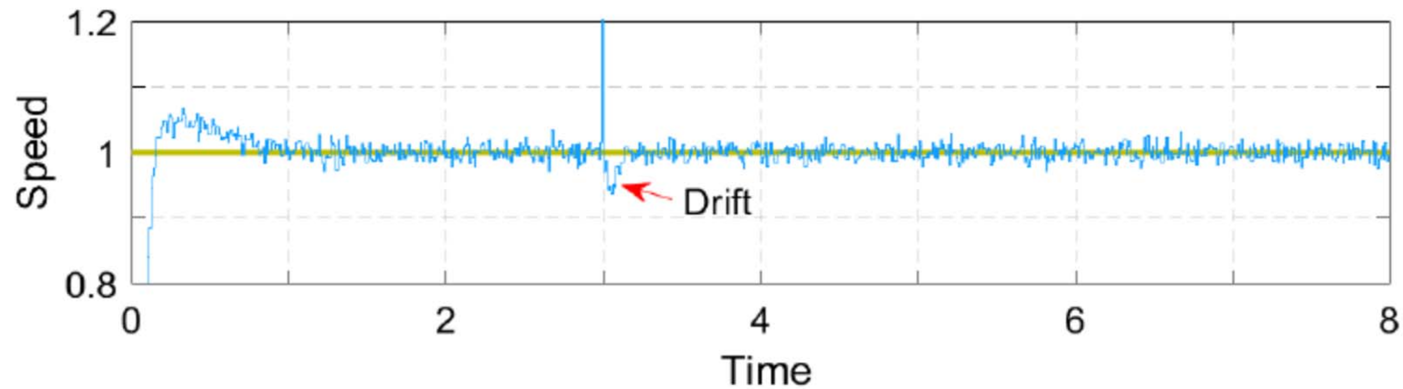
$$\{|\max_{\forall i} t(\bar{x}_i) - \min_{\forall j} t(\bar{x}_j)| \leq \Delta T_x\}$$

Need of Exp-Timing-Consistency

Using older states for recovery resulting in larger drifts



(a) Ten sampling period back recovery.



(b) One hundred sampling period back recovery.

Conclusion

- Review on CPS recovery
  - Model-based roll-forward recovery
  - How well does it work
- State consistencies for CPS recovery
  - Defined logic and timing consistencies
  - Why the consistencies is needed

Thank you!
Q&A