How to Protect Cyber-Physical Systems against Malicious Intruders?

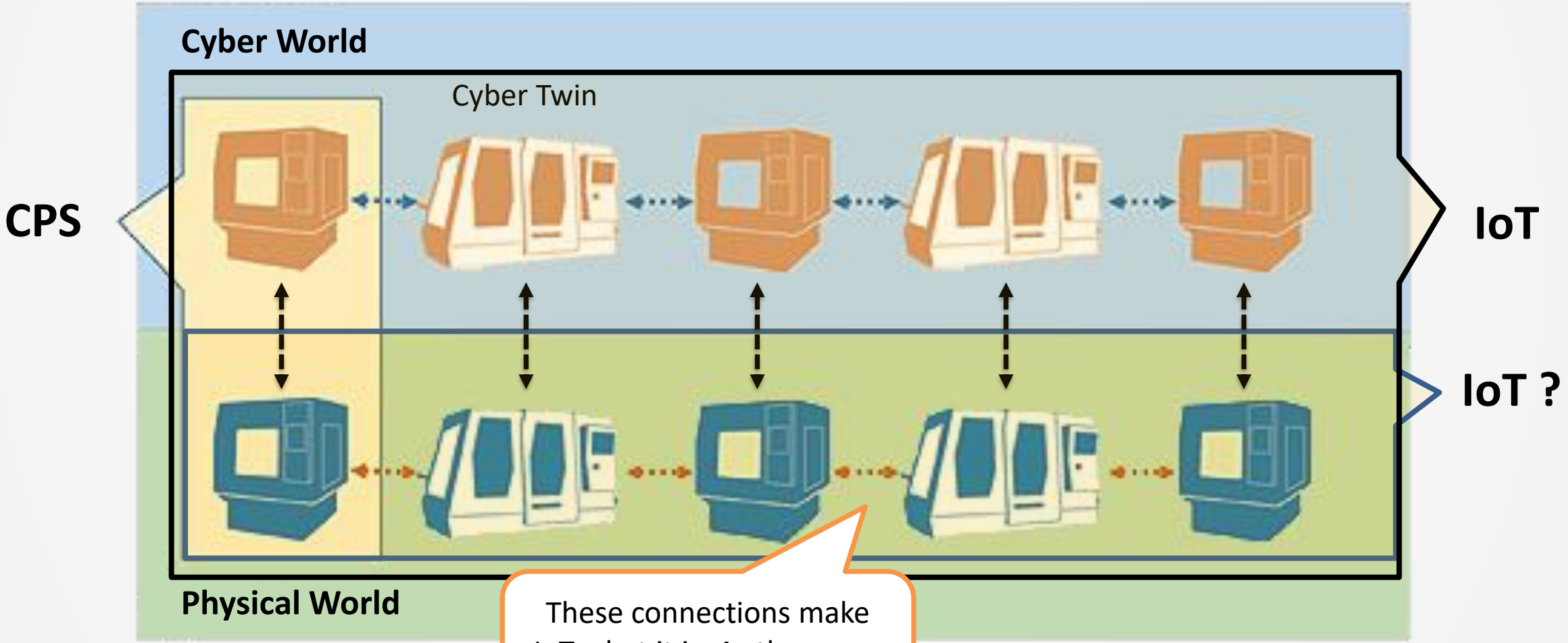
General Detection and Compensation Strategies

Sayad Haghighi

PhD, SMIEEE, Head of the IT Department & Assistant Professor
University of Tehran

Email
sayad@ut.ac.ir

CPS vs IoT

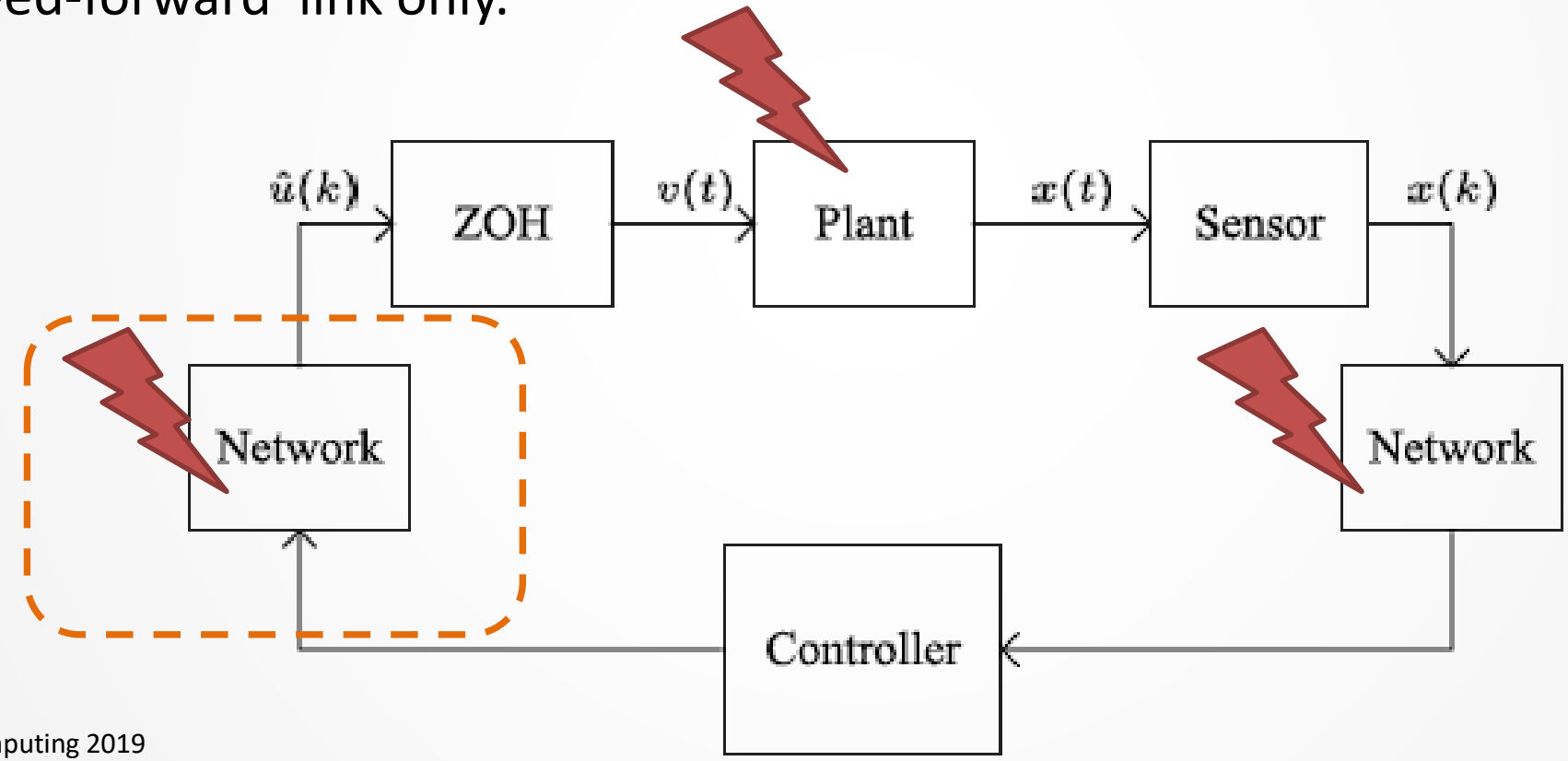

Cyber World
Cyber Twin
CPS
IoT
IoT ?
Physical World
These connections make IoT what it is. As the name says, it's an internet.

Agenda

1. Cyber Physical System & Networked Control Systems
2. Adversarial Model & Covert Attacks
3. 1st Example: Covert Attack on DC Motor
4. 2nd Example: Covert Attack on Cruise Control
5. 3rd Example: DoS Attack on Rotary Gantry

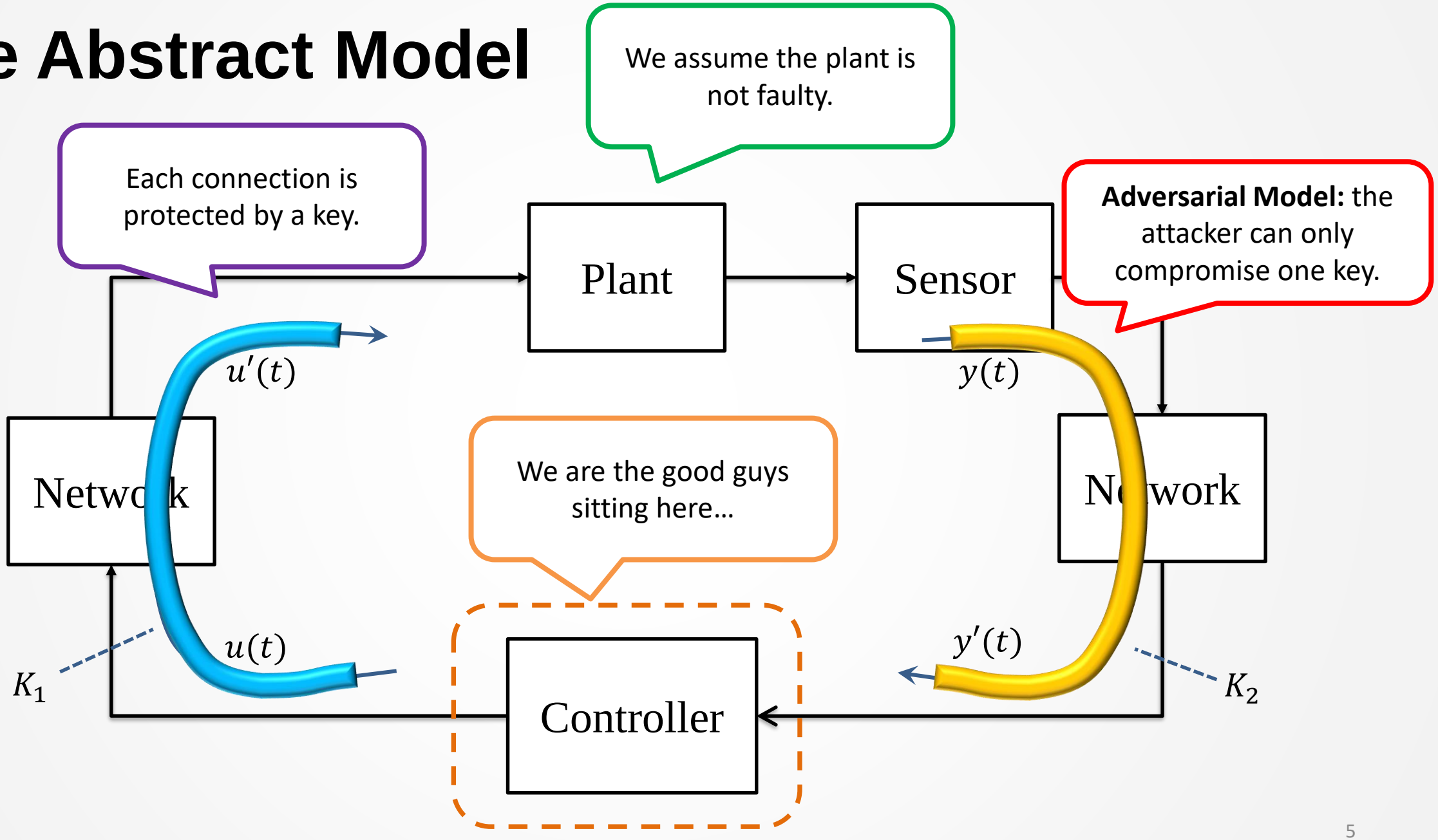
Cyber Physical System Security Model

We are creating a model to detect, characterize, and react to attacks in **networked control systems**. In the 1st example, we are focusing on the feed-forward link only.

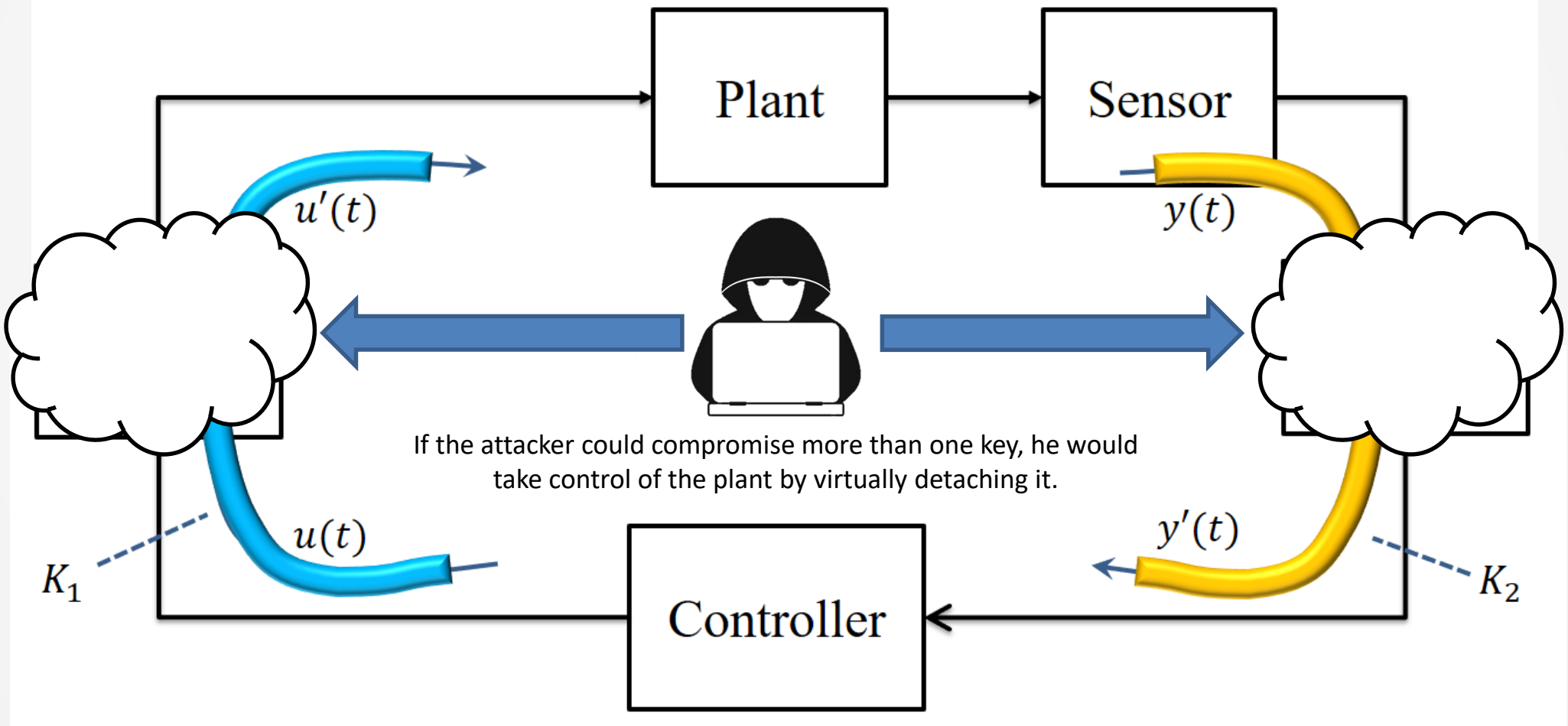


1x in IEEE ICIT'19
1x Elsevier Supercomputing 2019
1x IEEE Transactions on Industrial Informatics, 2019
1x under review in IEEE Transactions on Intelligent Transportation Systems, 2020
1x under development

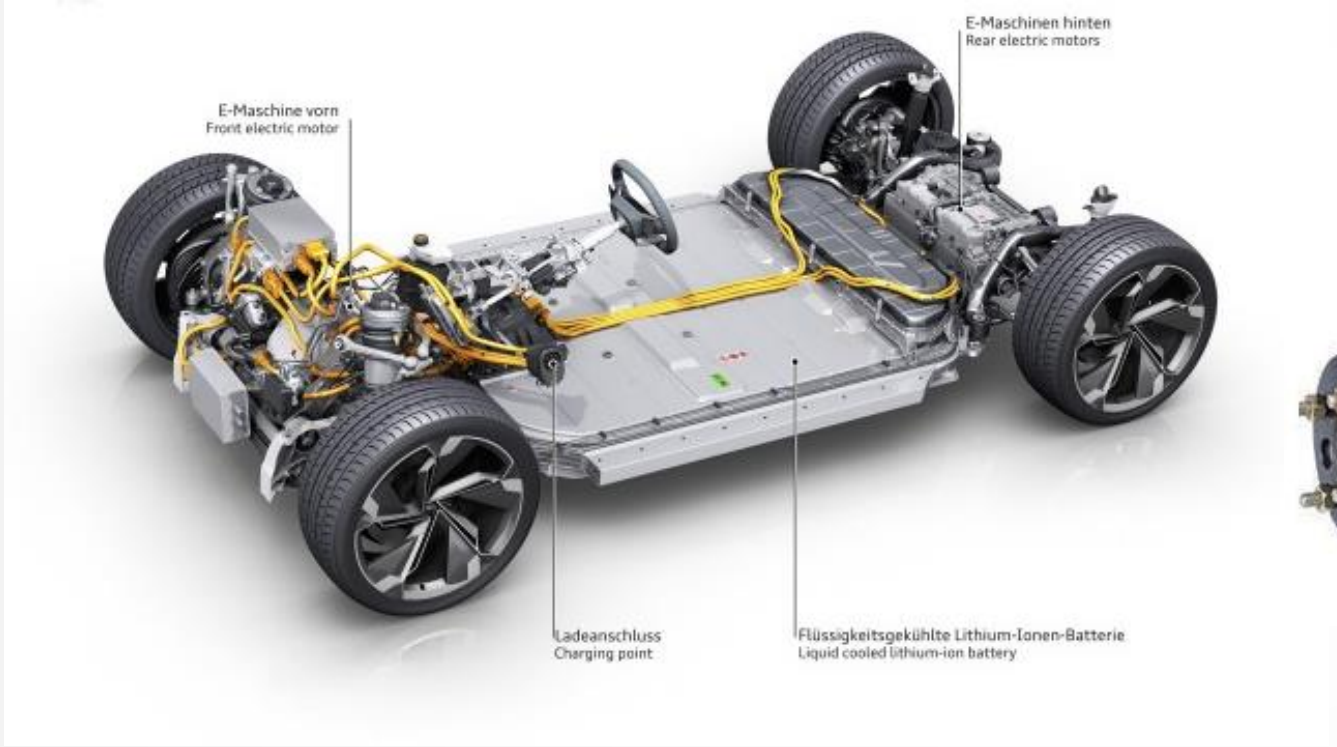
The Abstract Model



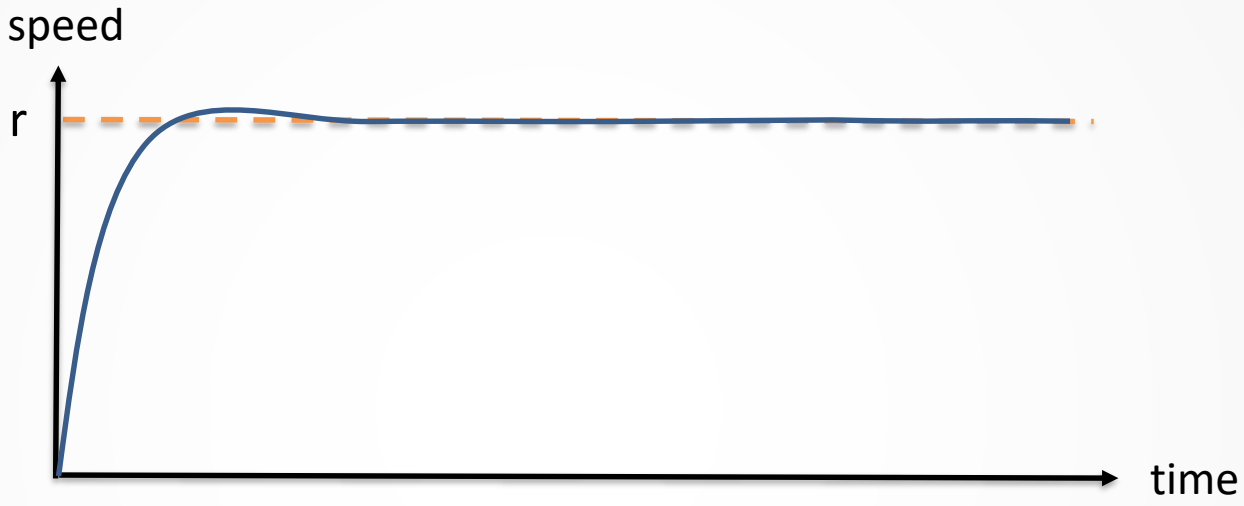
Regarding the Adversarial Model

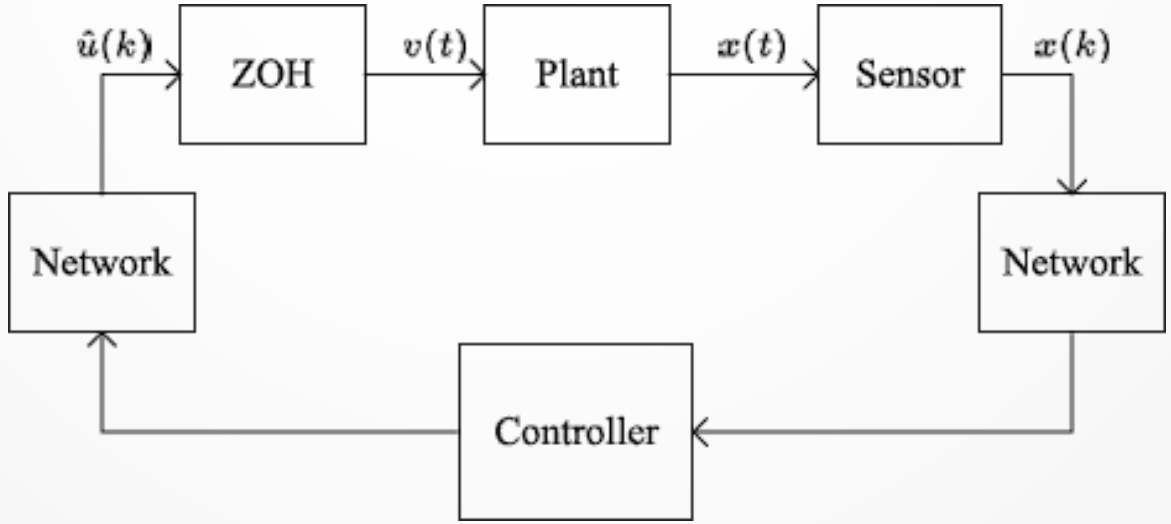


Plant Example : DC Motor

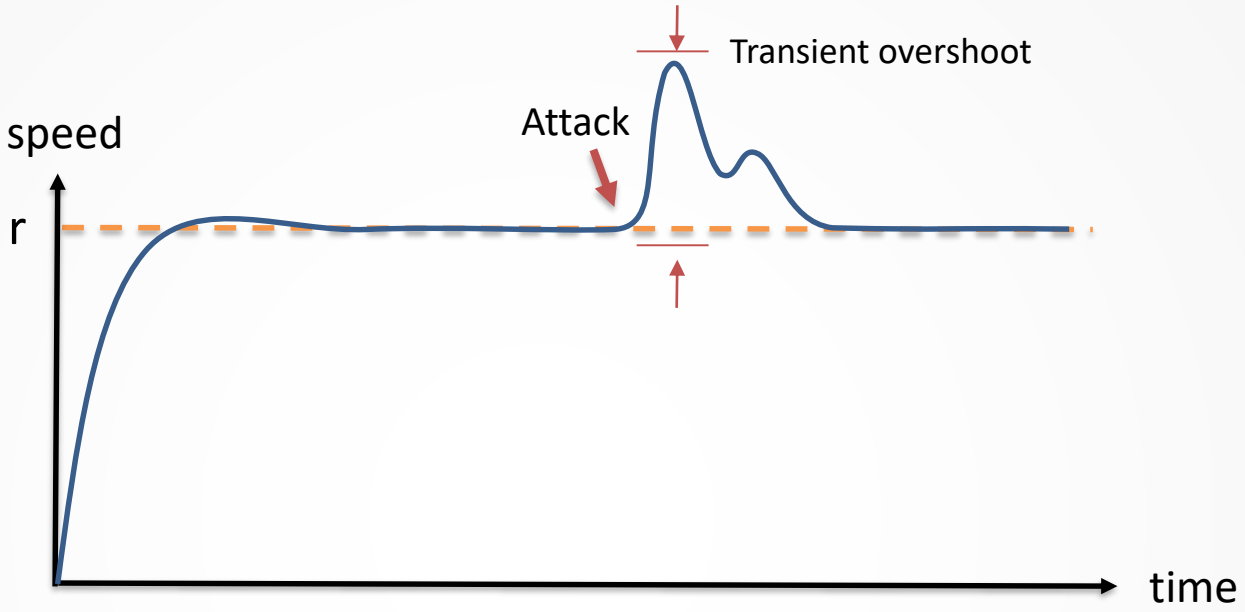


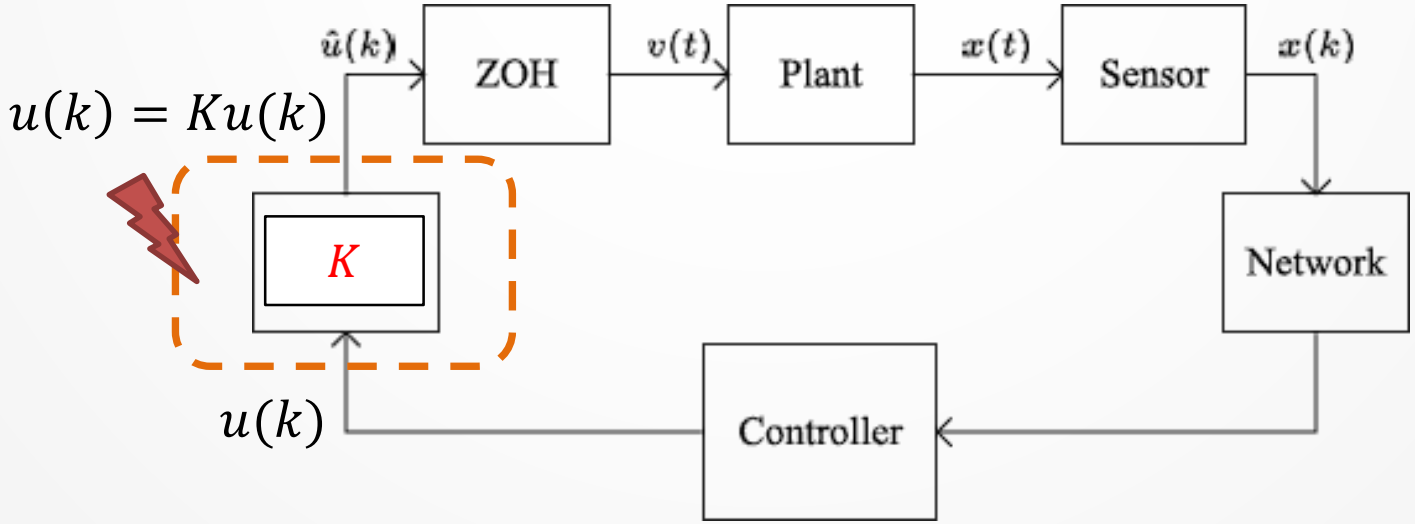
Normal Operation of the Plant



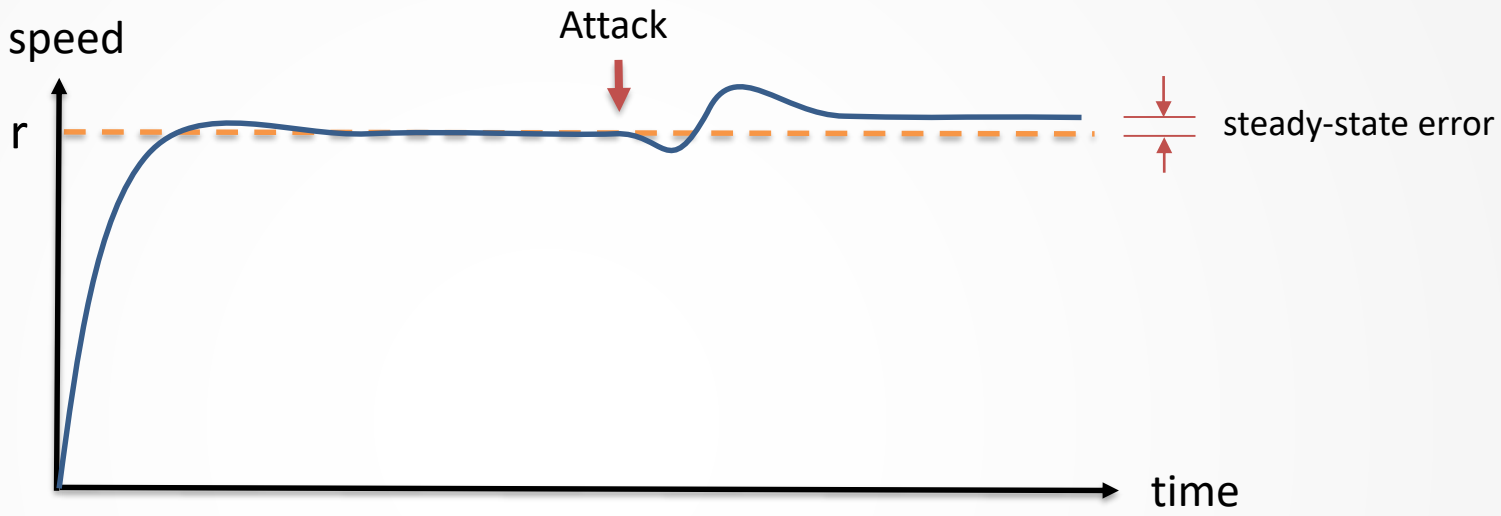


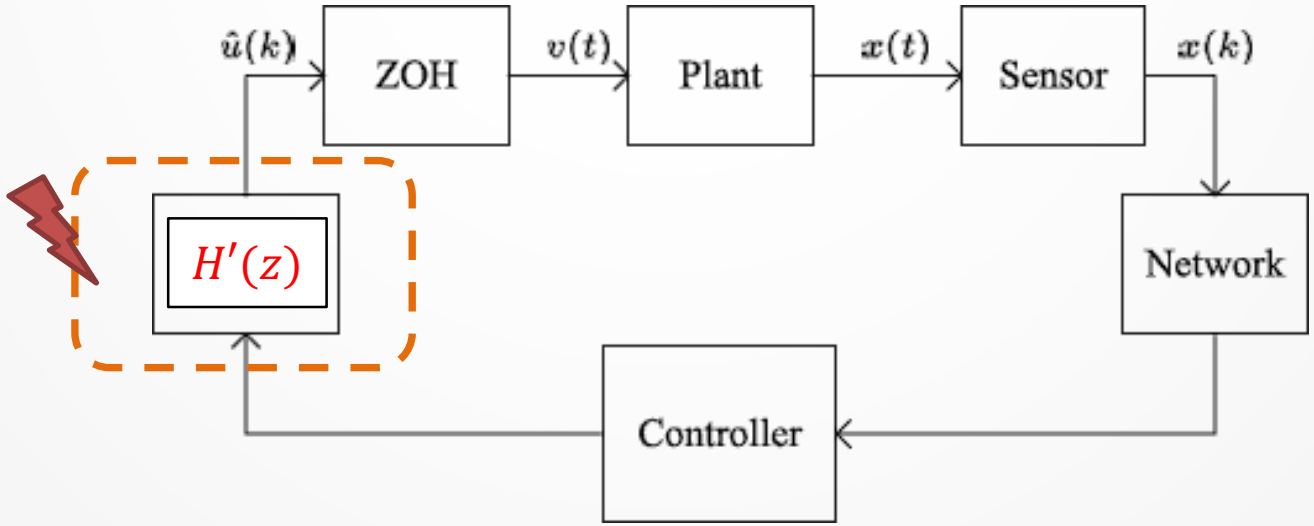
Covert Service Degradation Attacks (#1)





Covert Service Degradation Attacks (#2)





A General Approach for IDS Construction

- An Identifier learns the plant in the initial safe period.
  - Alternatively, we can use the plant model.

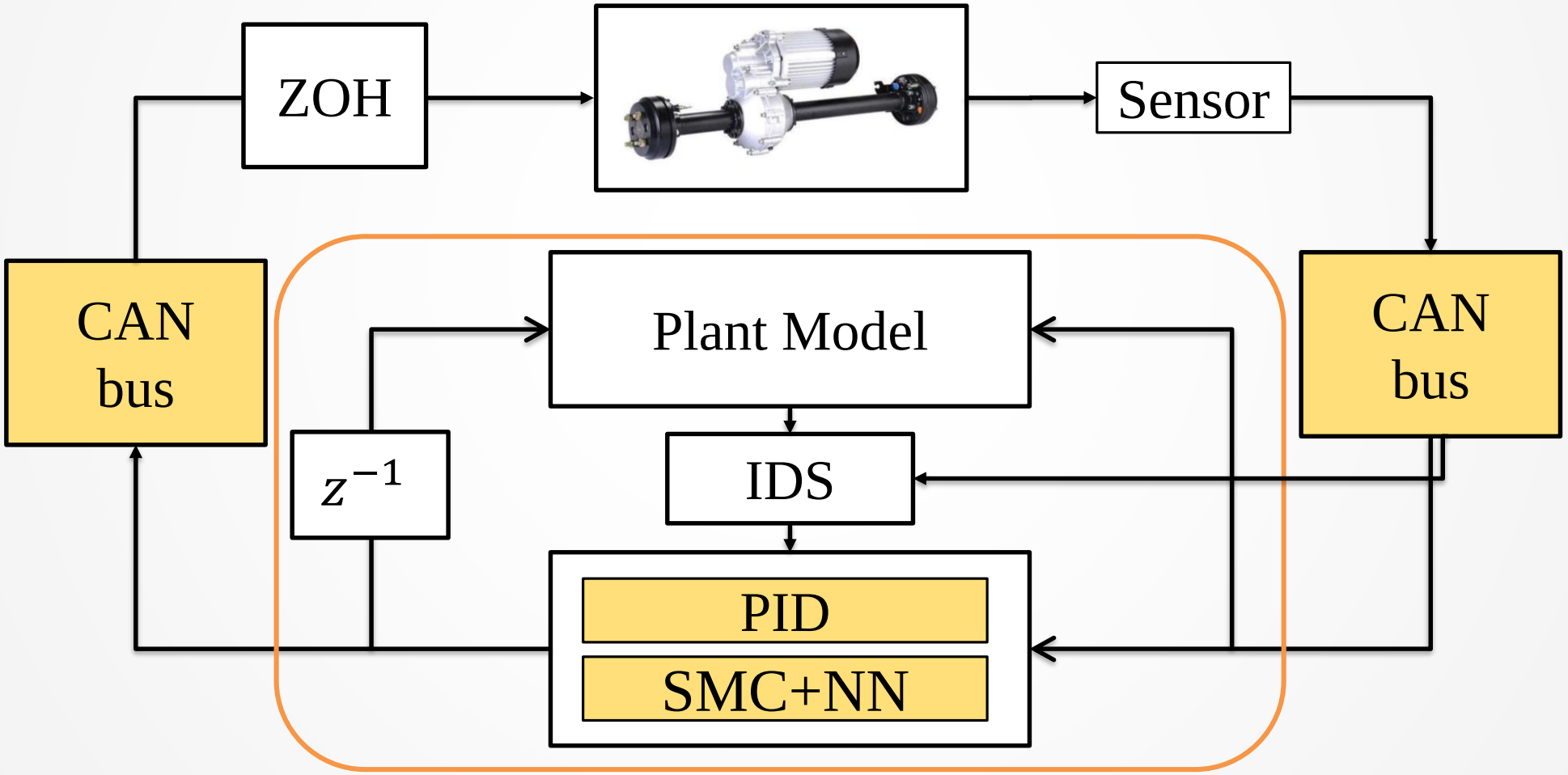
- Then, the learning finishes and it starts estimating the output (y) with each issued input (u).

- Intrusion is detected when the model output significantly deviates from the system output.

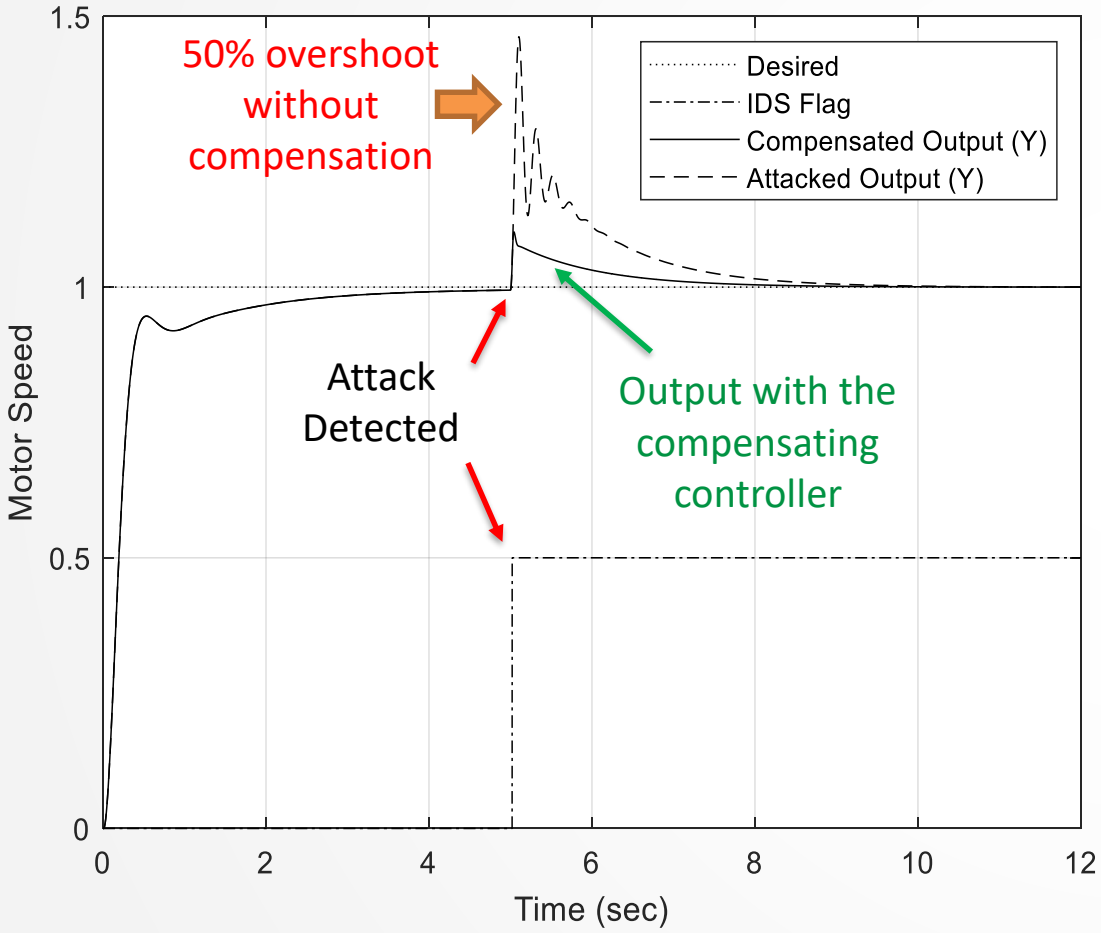
Compensation in Forward-link Attacks

- In covert SD attacks, the attacker has identified the plant and the controller:
  - In the first attempt, we tried to compensate FW-link attacks.
  - A model-free compensating robust controller replaces the identified controller upon IDS alarm.
    - The attacker hasn't learnt the 2nd controller.

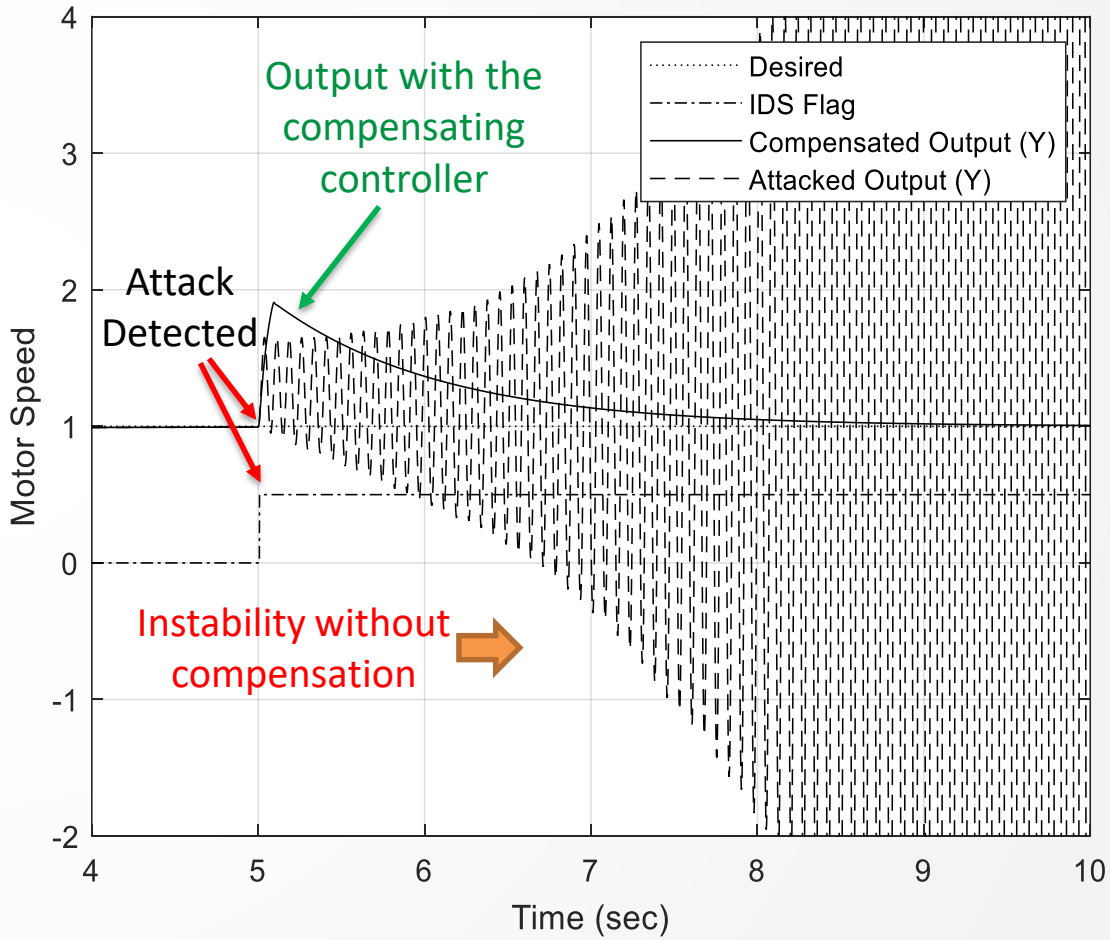
The Simulation Model



Detection & Compensation Results

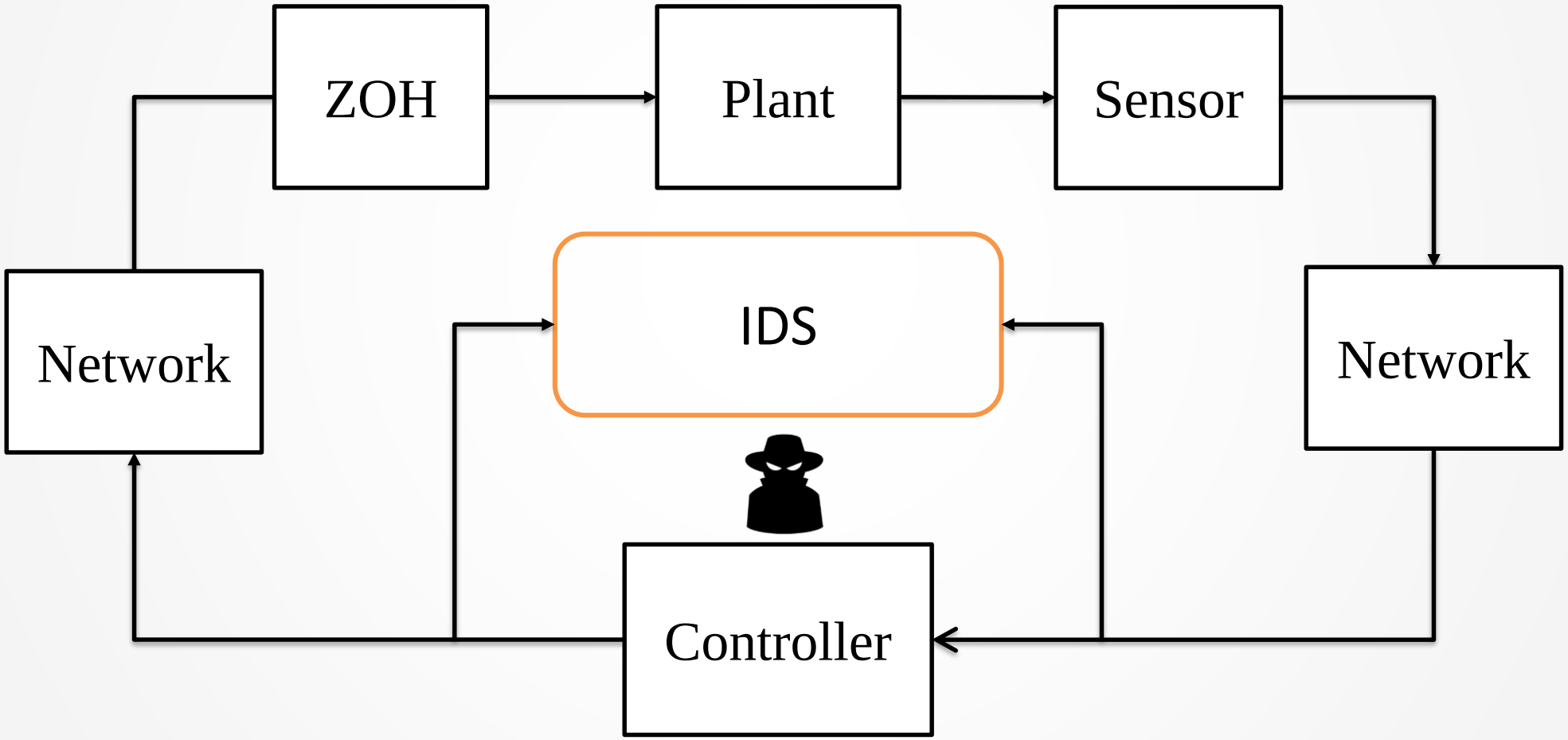


SD attack Type 2, K=15



SD attack Type 2, K=120

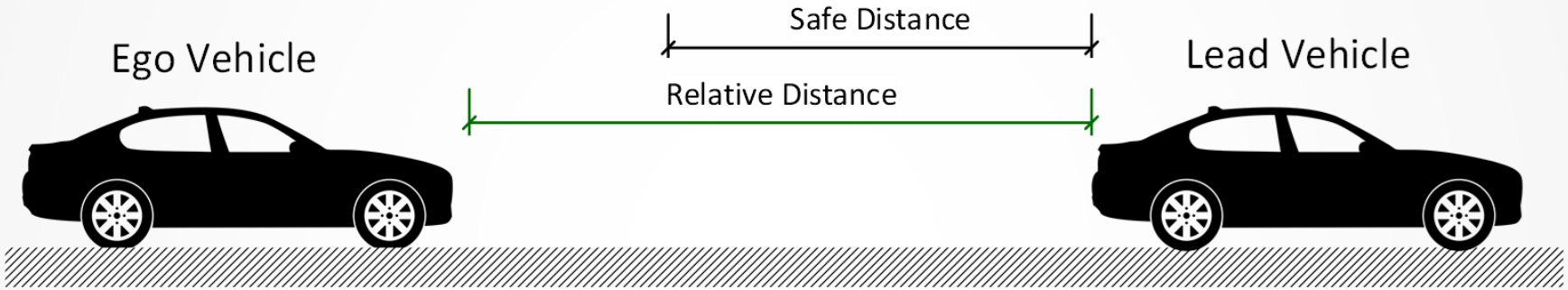
Okay, what if the controller itself is attacked?



Adaptive Cruise Control

Control Objective:

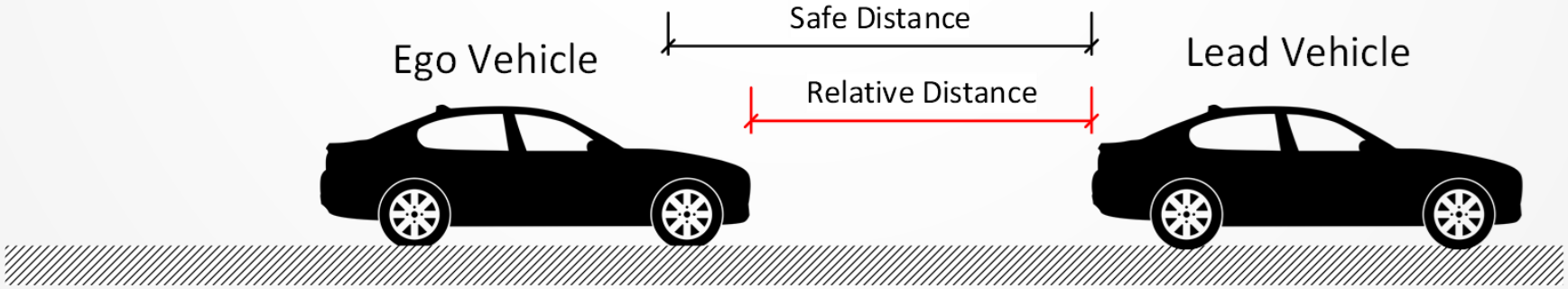
$V_{ego}=V_{cruise}$



The relative distance is greater than the safe distance.

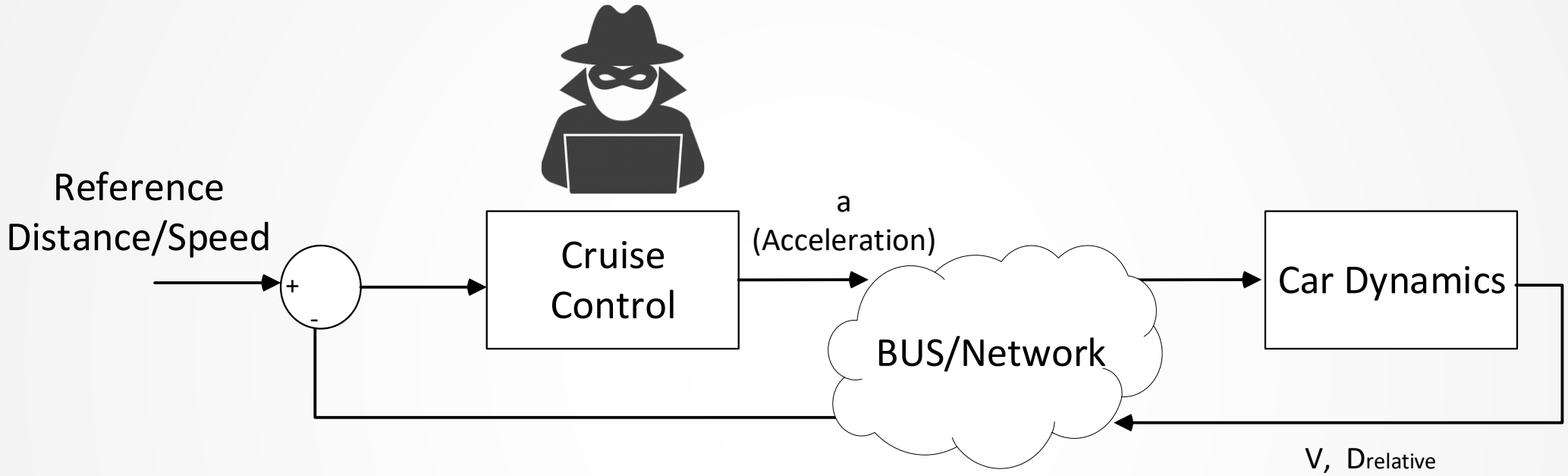
Control Objective:

$D_{relative}=D_{safe}$



The relative distance is smaller than the safe distance.

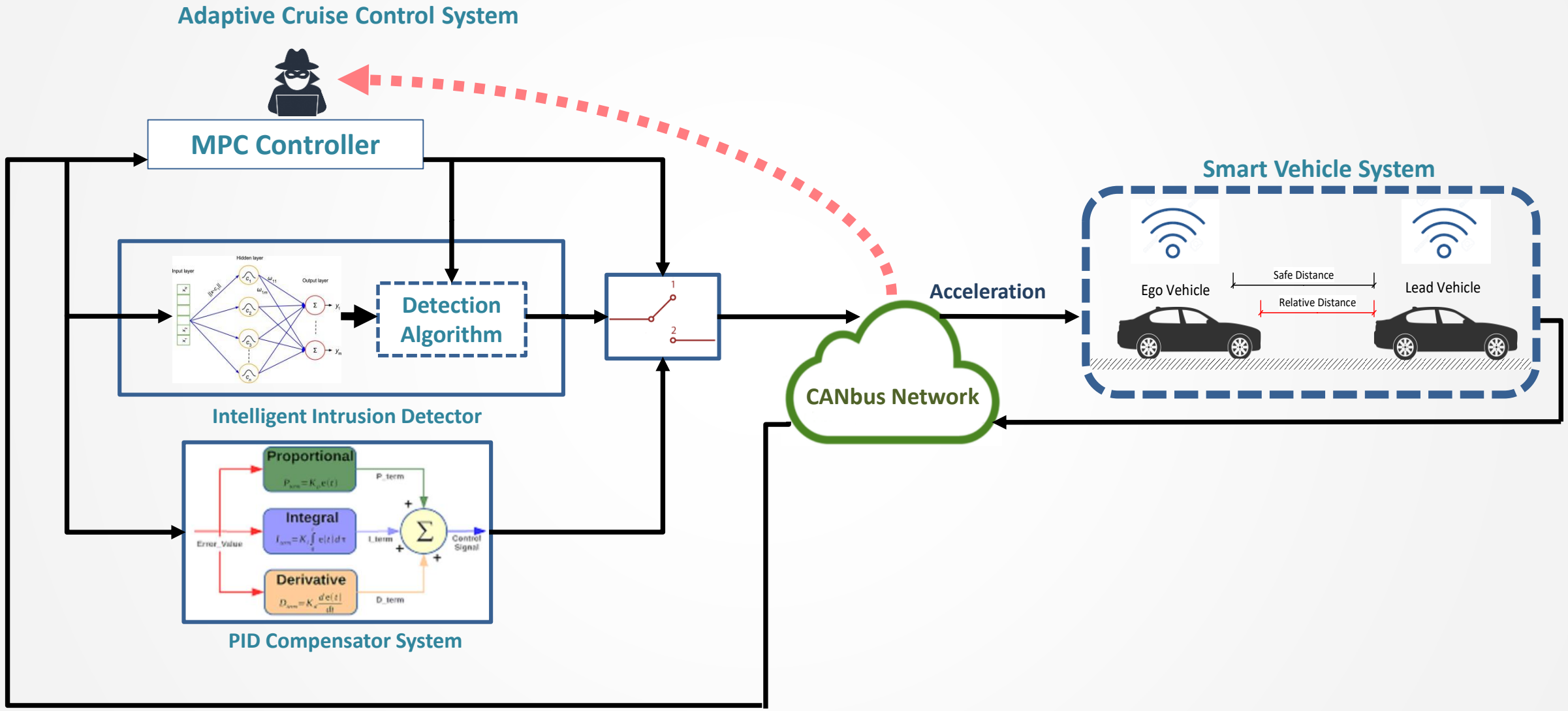
Covert Attack Scenarios



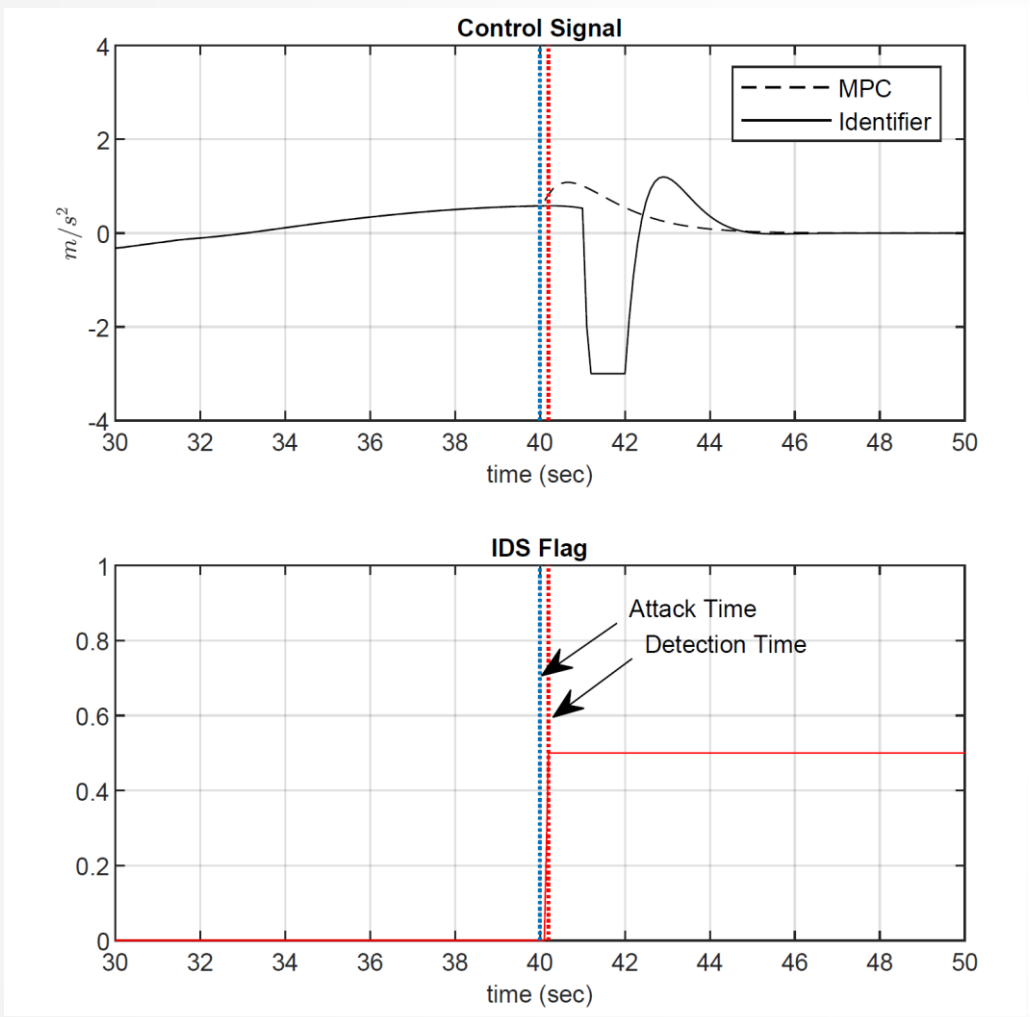
Type 1: Temporally reducing the relative distance to lower than the safe distance, perhaps at a desired time.

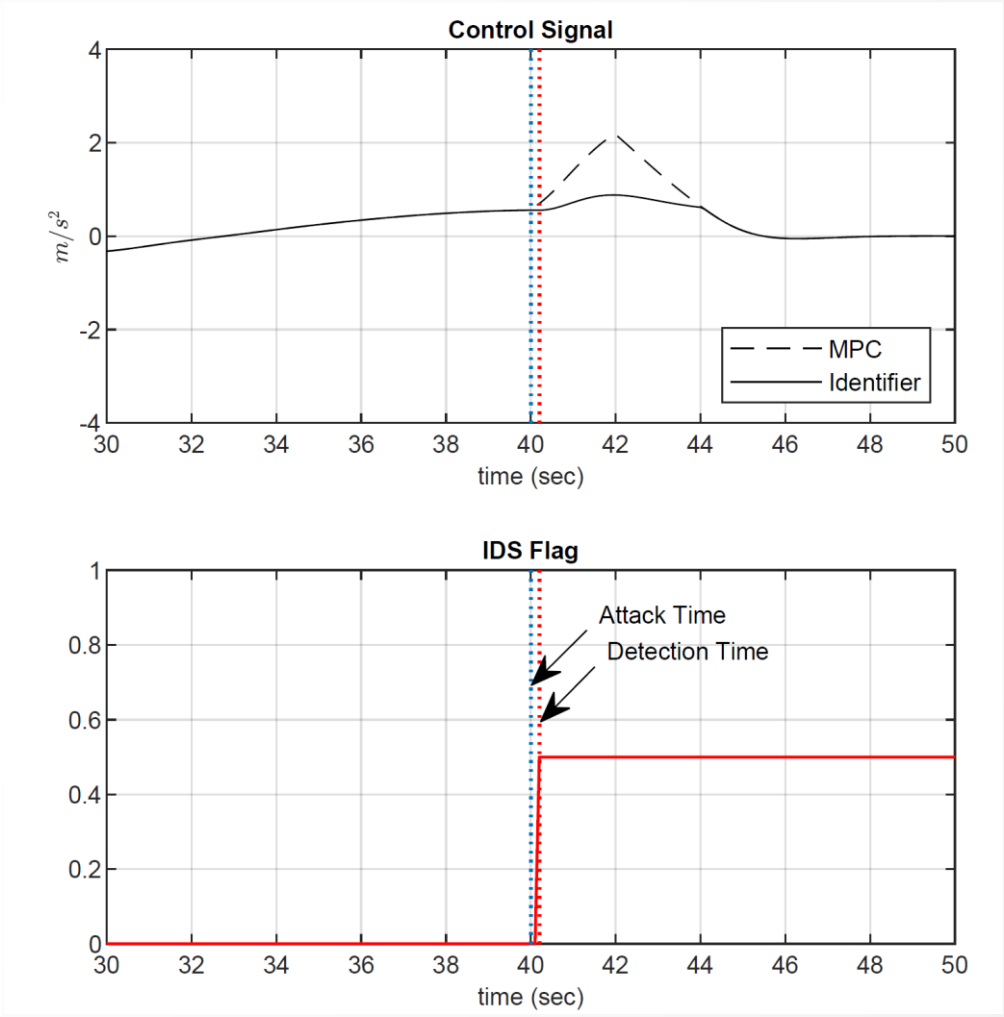
Type 2: Reducing the relative distance to permanently stay slightly lower than the safe distance.

Attack Detection & Compensation of Malicious Attacks on ACC

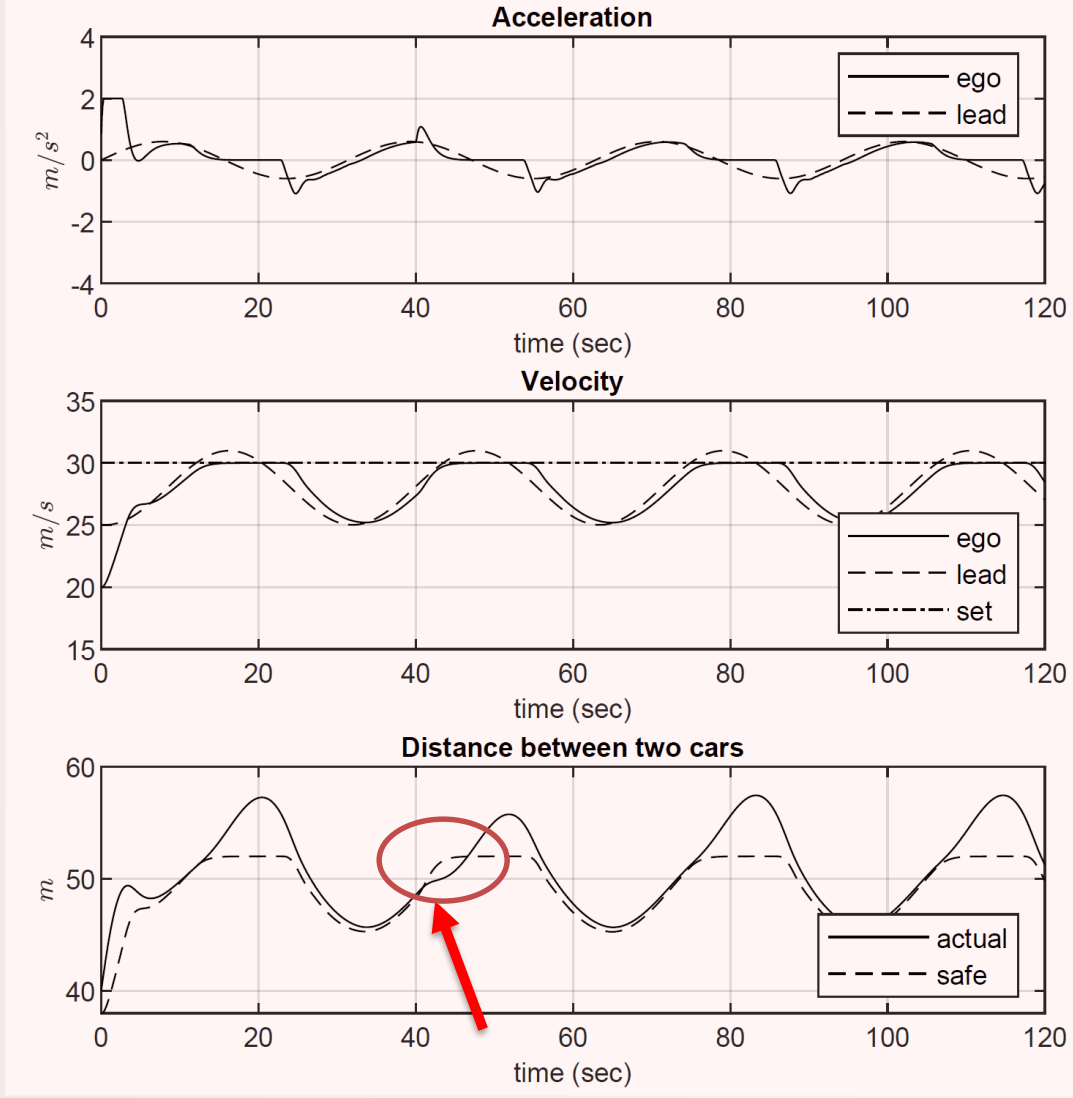


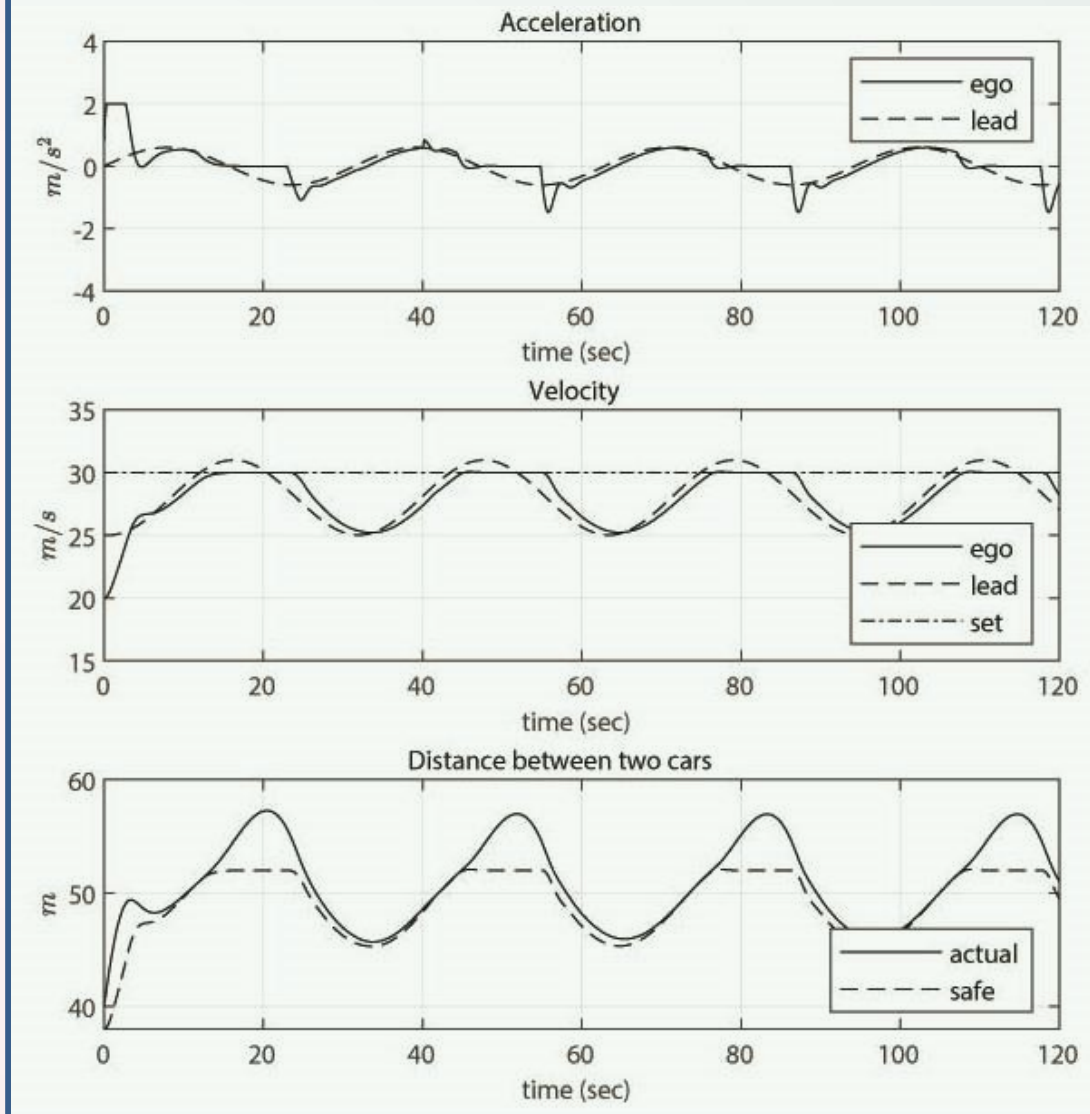
Attack Detection of Covert Attacks (Type 1 & 2) on ACC



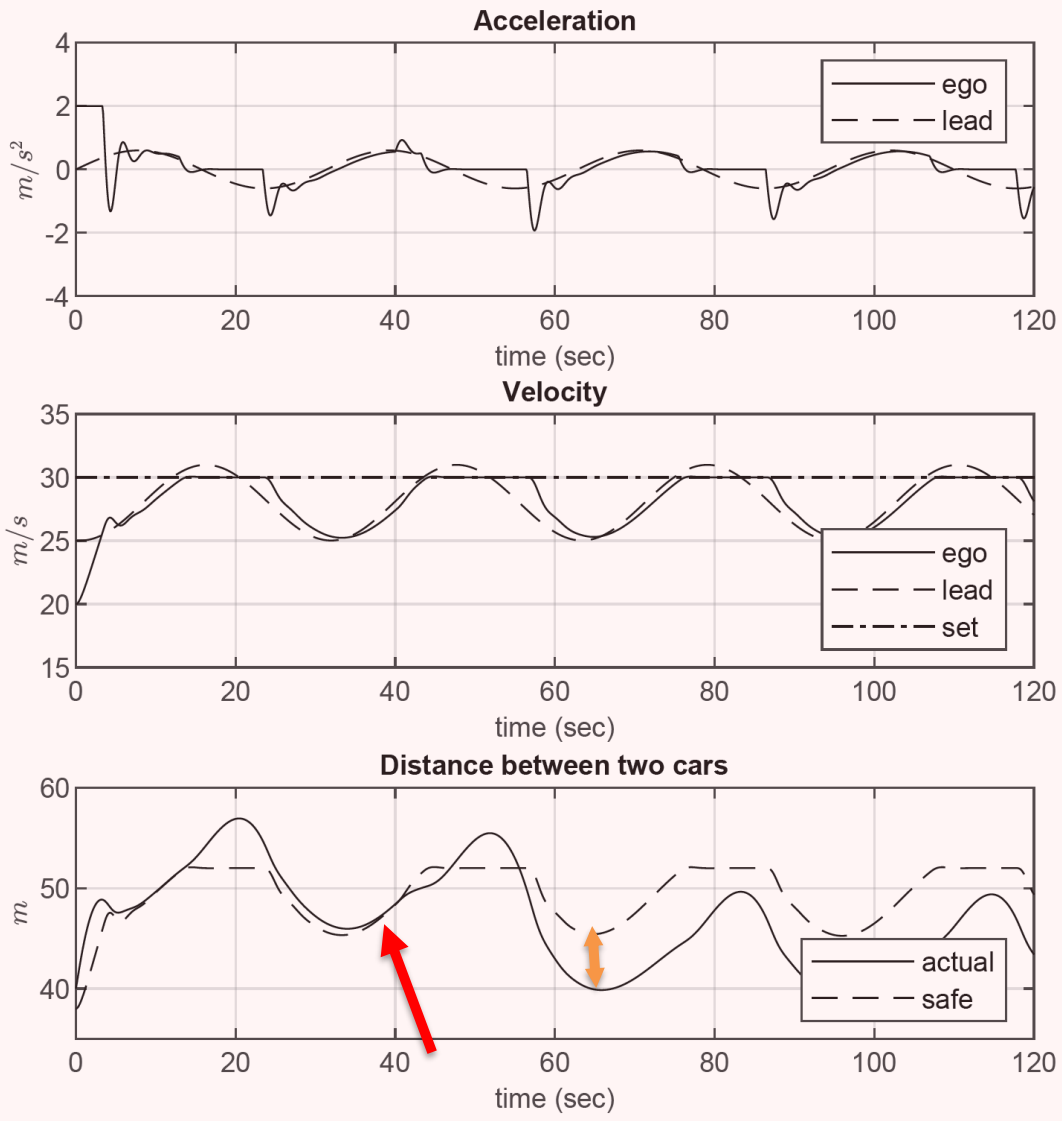


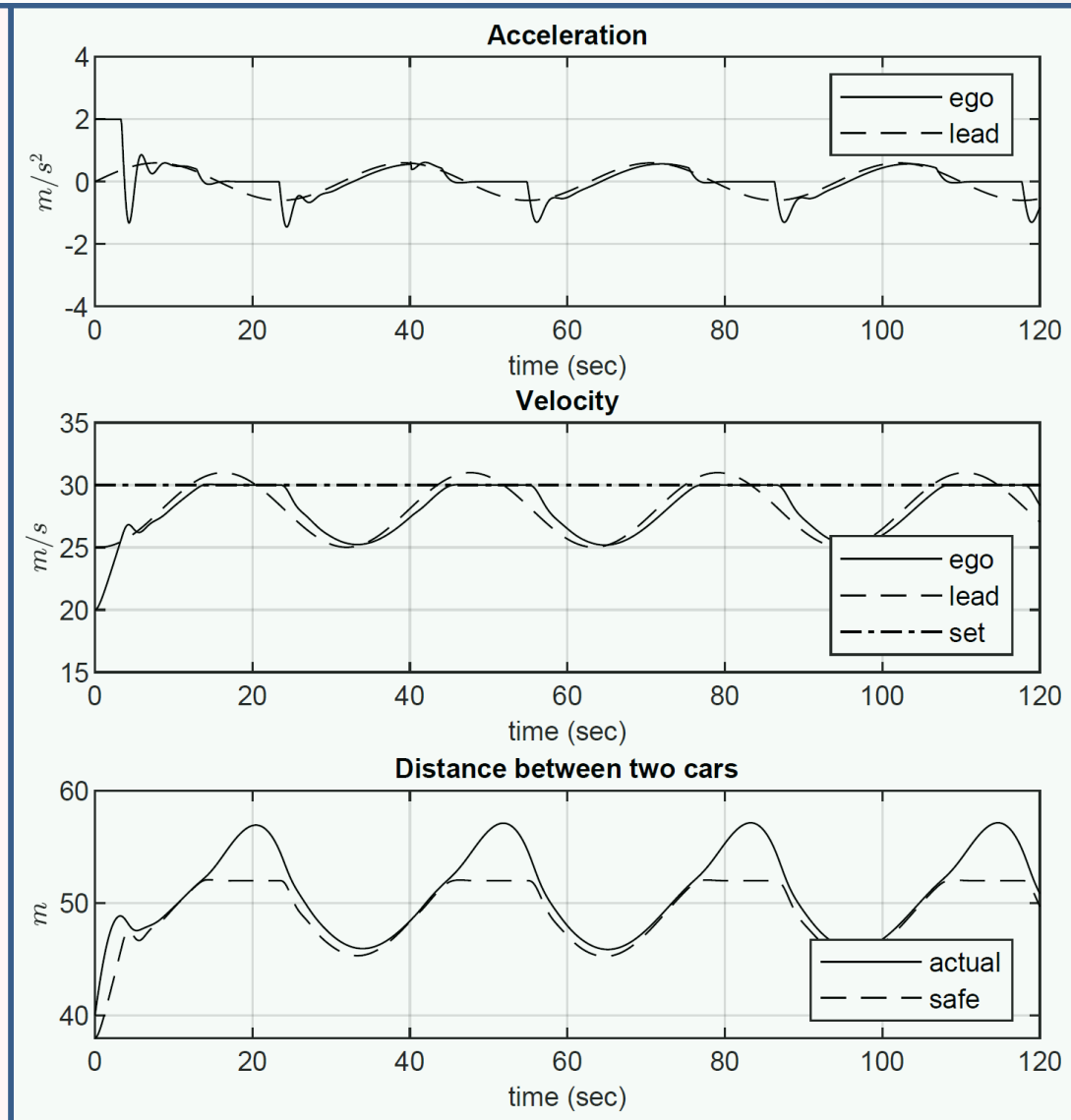
Attack Compensation of (Type 1) Covert Attack on ACC





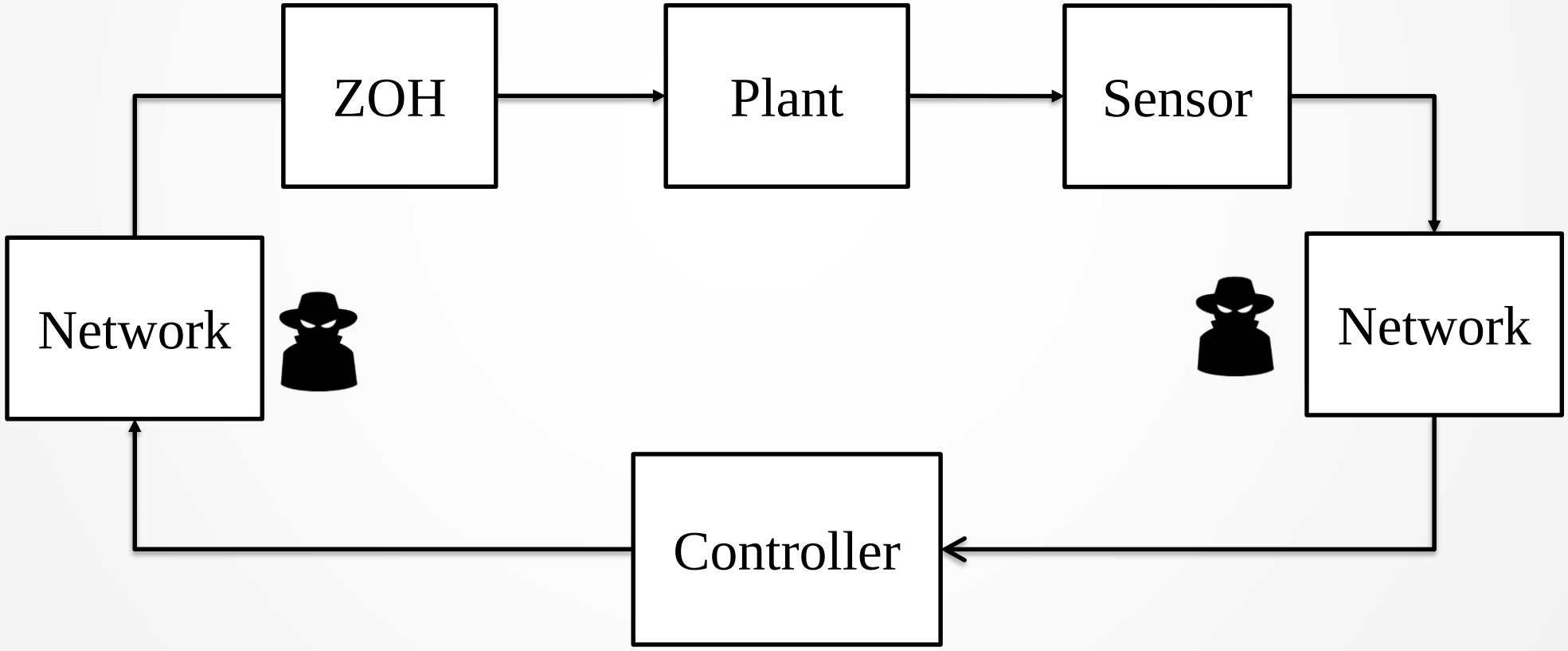
Attack Compensation of (Type 2) Covert Attack on ACC



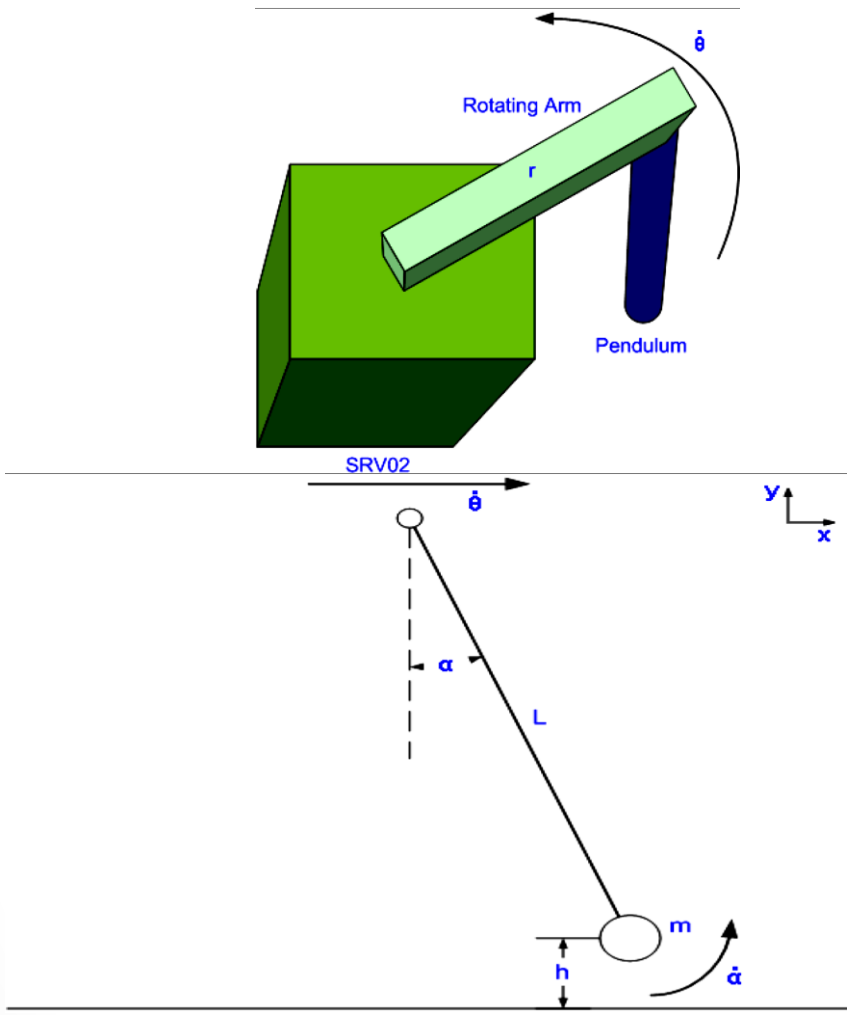


DoS Attack in the Network Links

- Sometimes the attacker cannot compromise the keys. But can create a DoS attack that prevents control and sensor packets to be delivered.
- We are working on DoS-resilient controllers too.



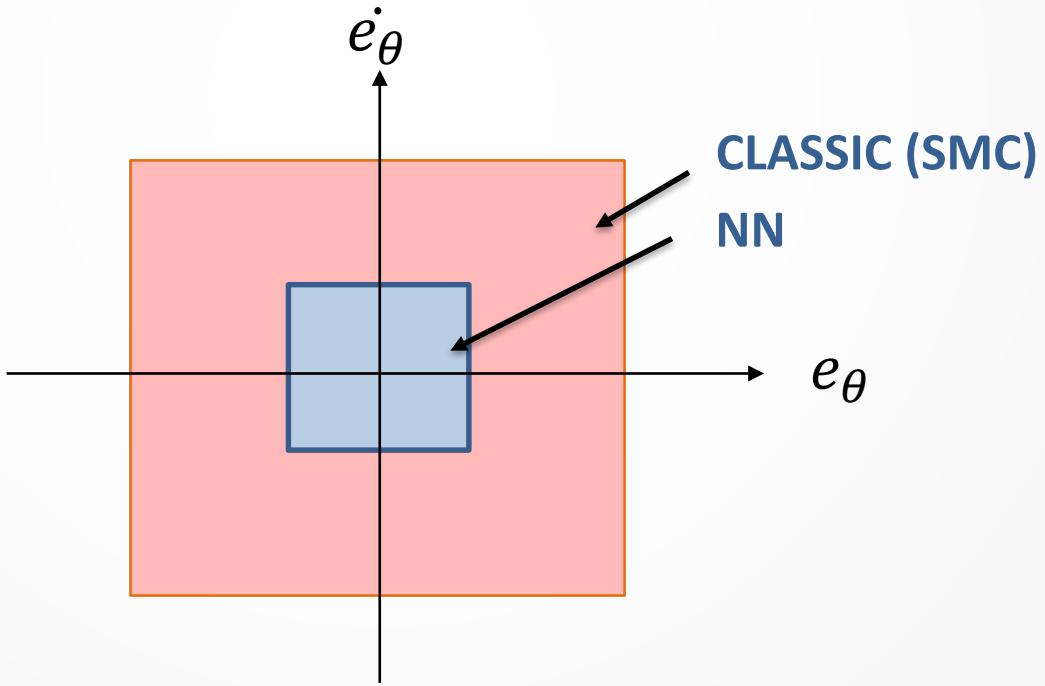
Rotary Gantry Crane Plant



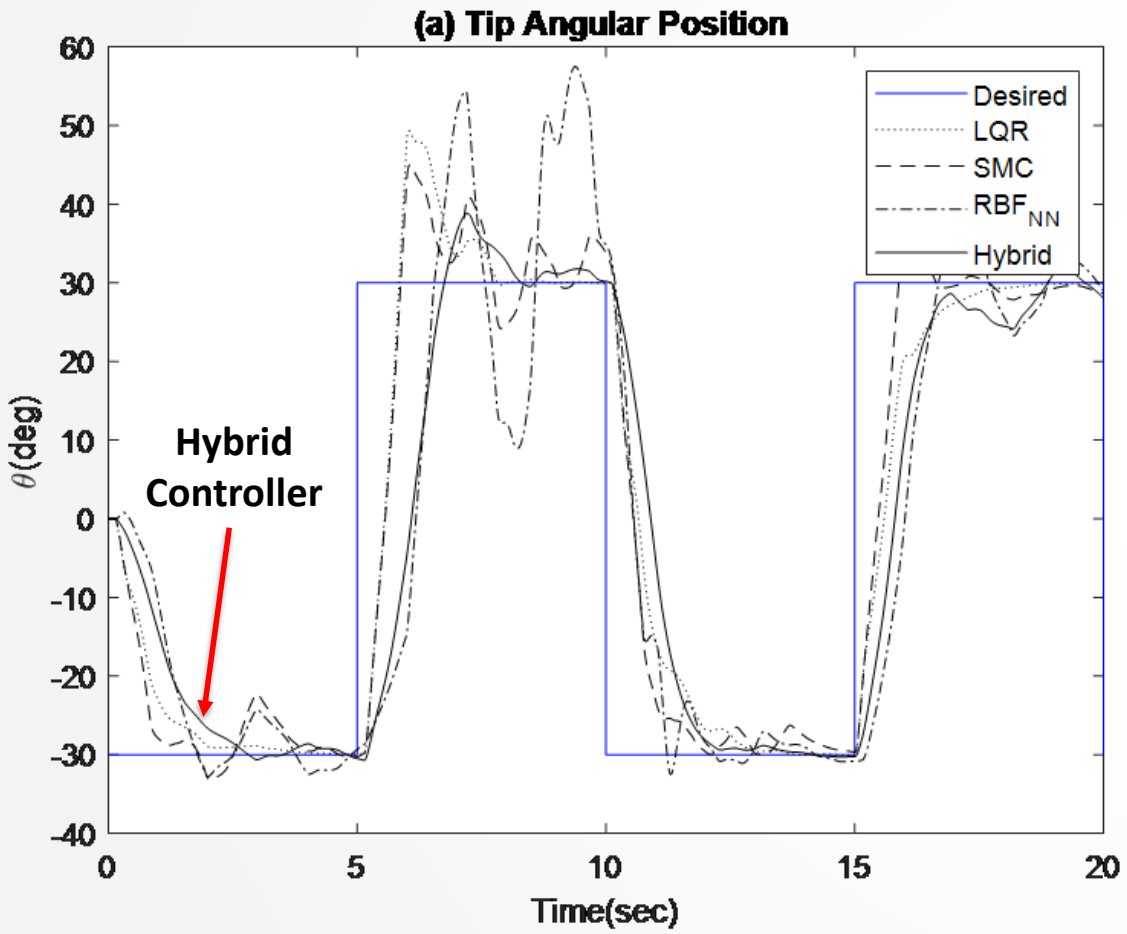
Networked Intelligent-Classic Control System

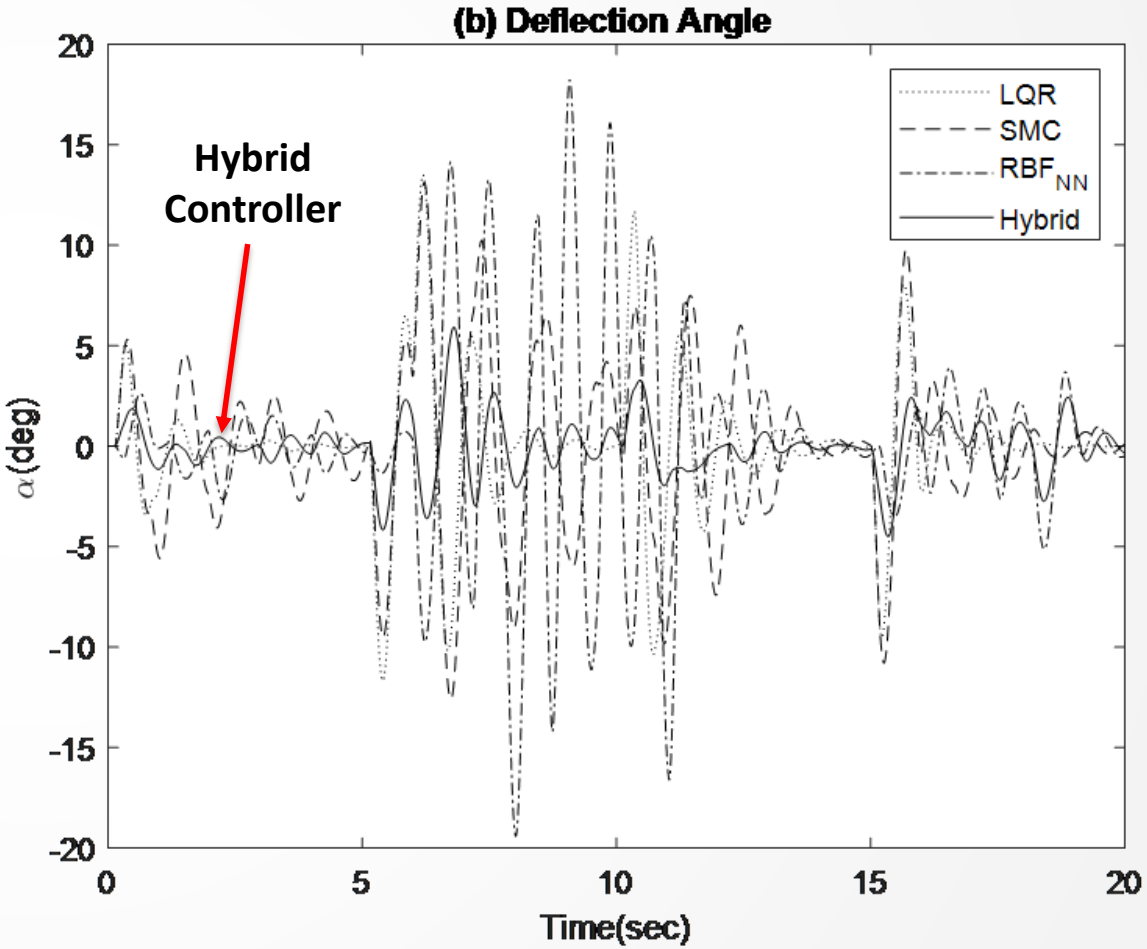
The Soft-Switched Hybrid Controller:

$$u(t)=\lambda_1 u_{①}(t)+\lambda_2 u_{②}(t)$$

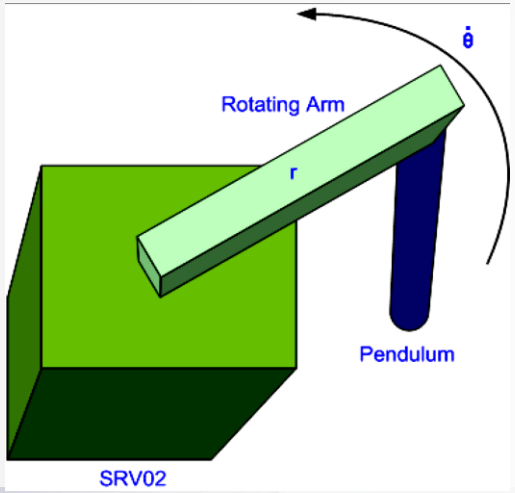


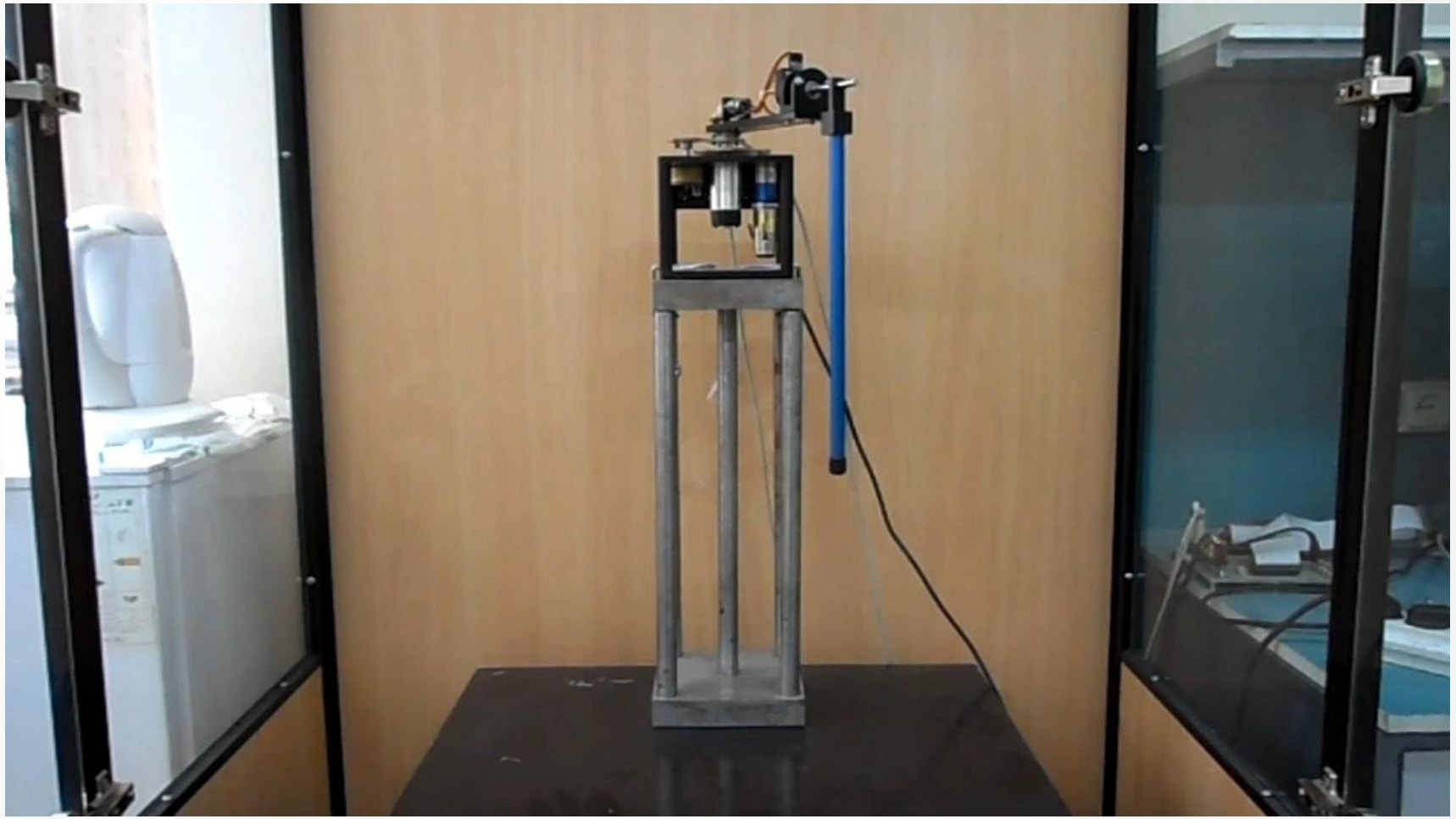
Resistance to DoS (80% loss in FW Link)





Quanser Test Plant





Thank you

Advanced Networking & Security Research Lab

www.ANSLab.org
sayad@ieee.org