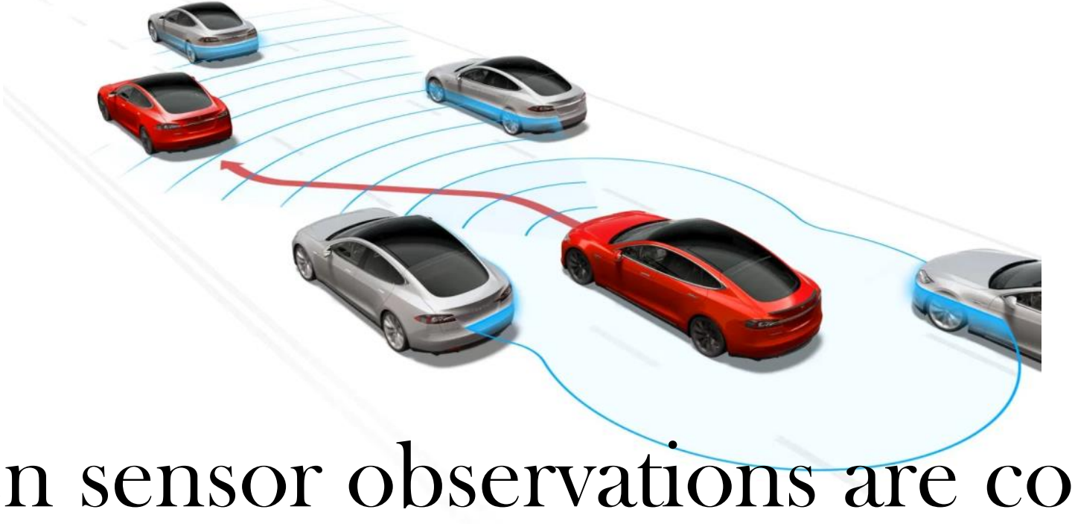
Communication and security in cyber-physical systems

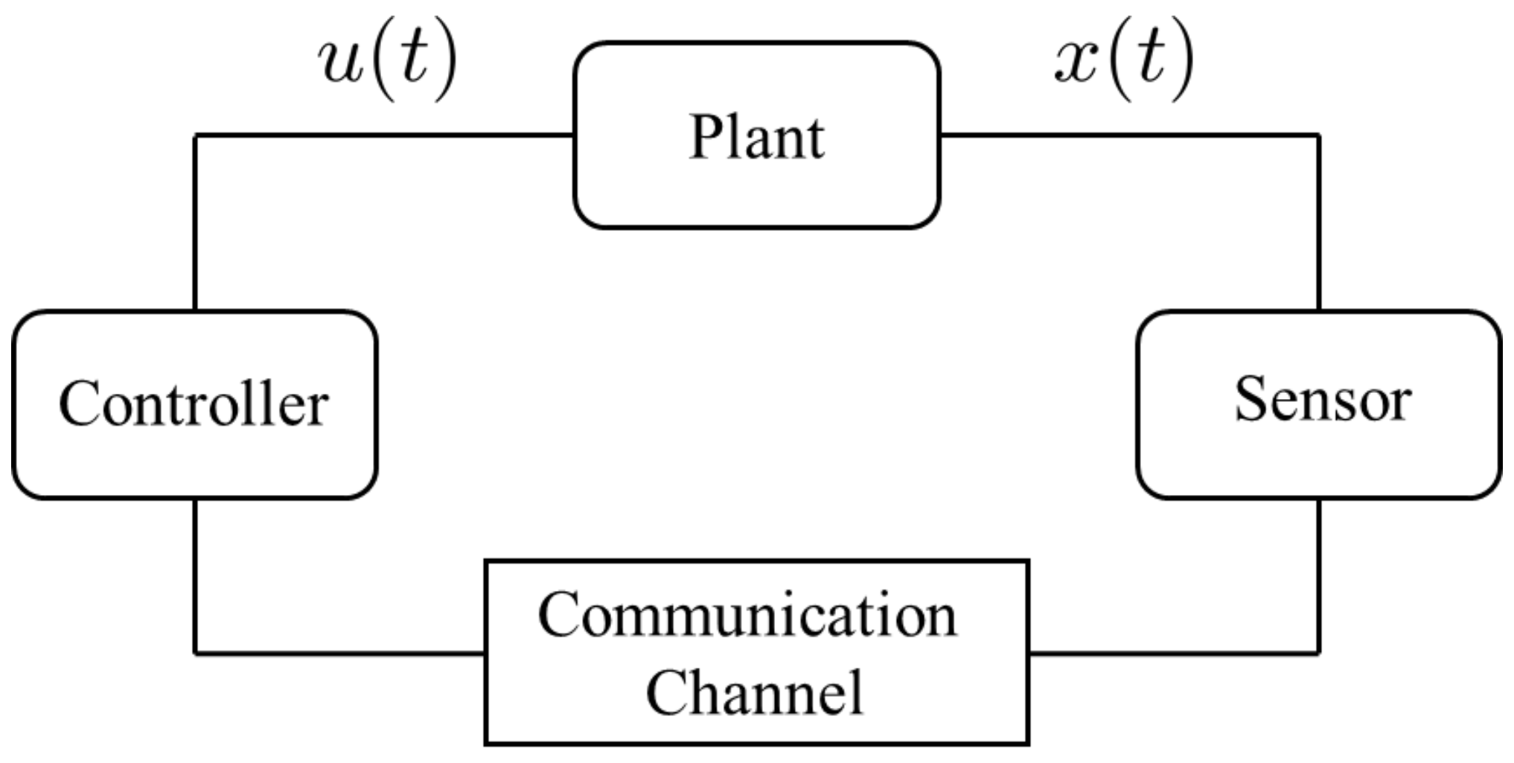
PI: Massimo Franceschetti, University of California San Diego
Co-PI: Jorge Cortés, University of California San Diego

Cyber-physical systems (CPS):



When sensor observations are corrupted by noise, subject to delay, and hijacked by attackers, can we still guarantee safe operation of the system?

Networked Control System:



$$\dot{x} = Ax(t) + Bu(t) + w(t)$$

$$|w(t)| \leq M$$

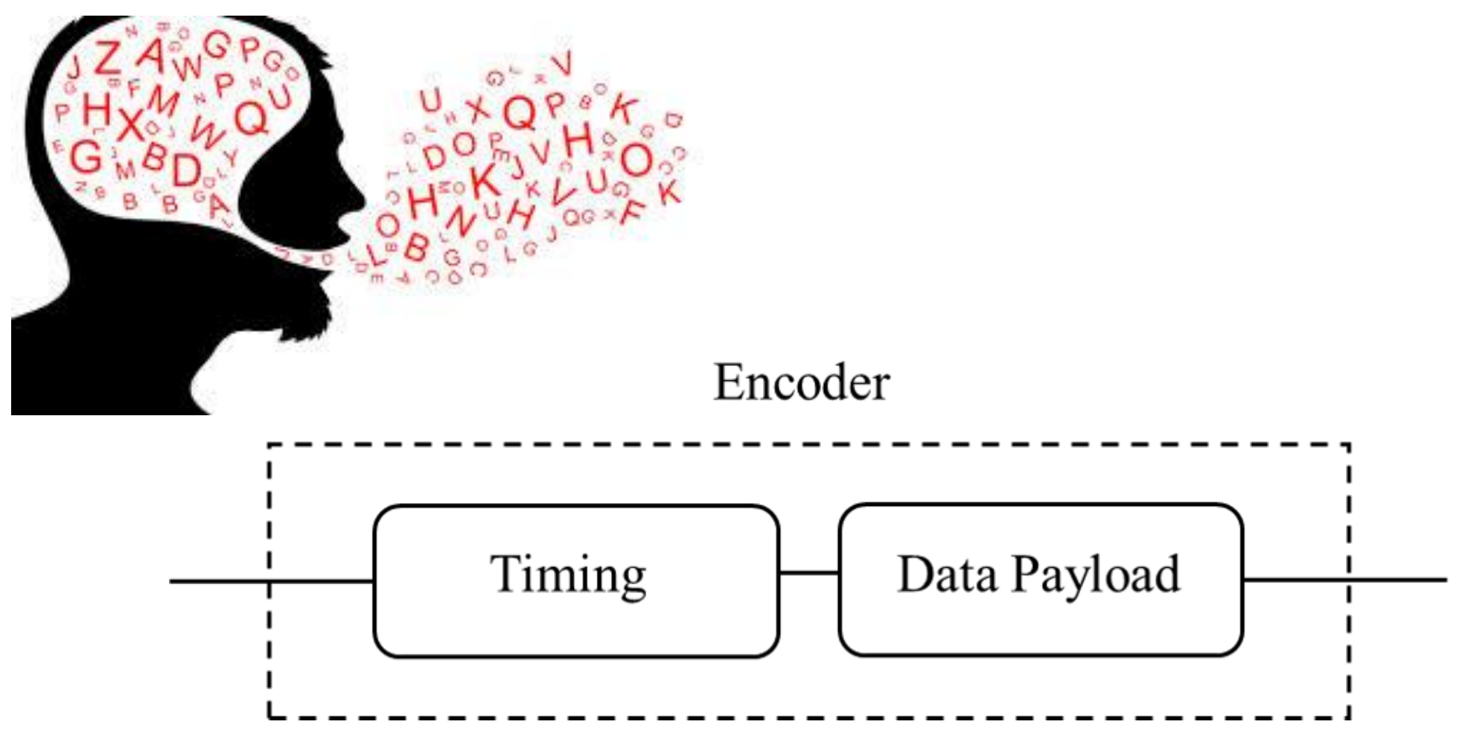
Event-triggered control:

In CPS we need to use distributed resources efficiently

Step 1: --
Step 2: --
Step 3: Bad Dog
Step 4: --
.
.
.

Timing information:

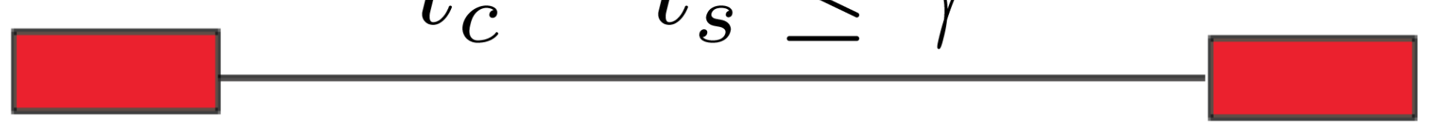
In the same way that subsequent pauses in spoken language are used to convey information, it is also possible to transmit information in communication systems not only by message content but also with its timing.



Transmission with delay:

Packet transmission time t_s
Packet reception time t_c
Delay

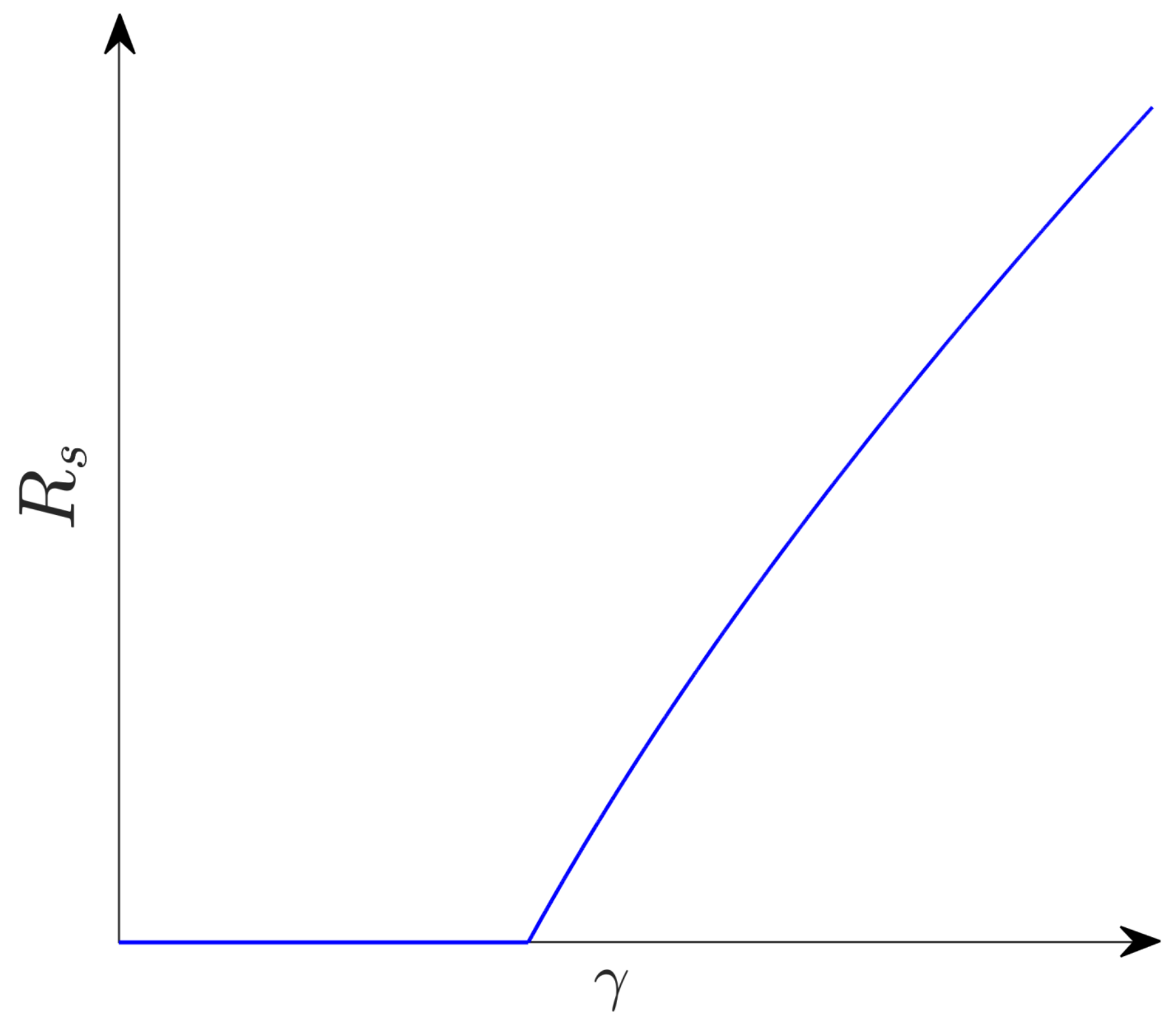
$$t_c - t_s \leq \gamma$$



$b_s(t)$: number of bits in packets transmitted up to time t

Information transmission rate

$$R_s = \limsup_{t\to\infty} \frac{b_s(t)}{t}$$



Attacks on CPS:

Computer virus Stuxnet a 'game changer,' DHS official tells Senate

The New York Times
Israeli Test on Worm Called Crucial in Iran Nuclear Delay

Stuxnet Returns, Striking Iran with New Variant

"Stuxnet has changed the way we view the security threat"

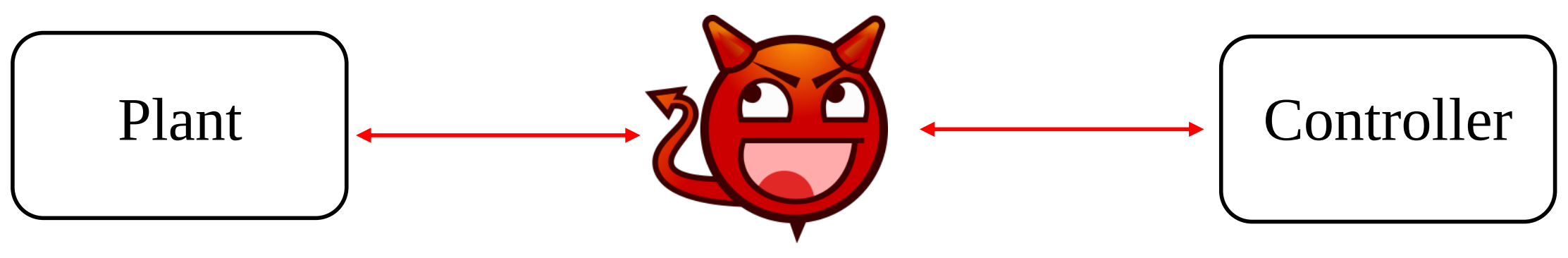
Symantec.

WIRED The US Tried to Stuxnet North Korea's Nuclear Program

The man in the middle:

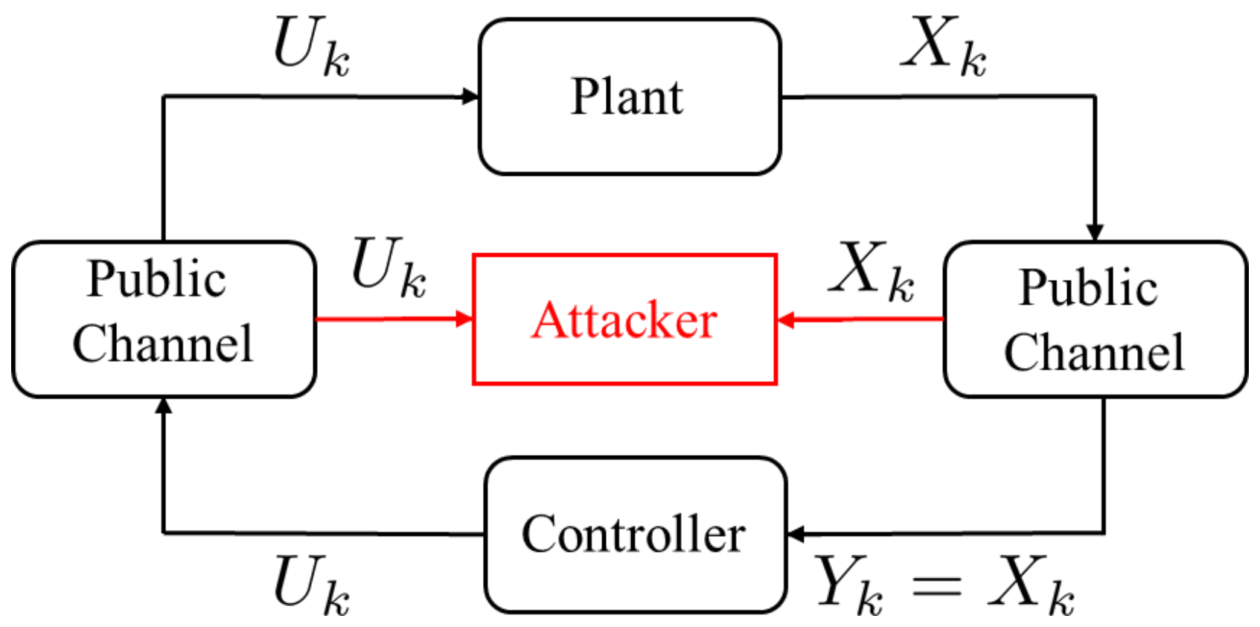
In network control systems, sensor observations and control signals can be hijacked.

A fictitious plant for the controller

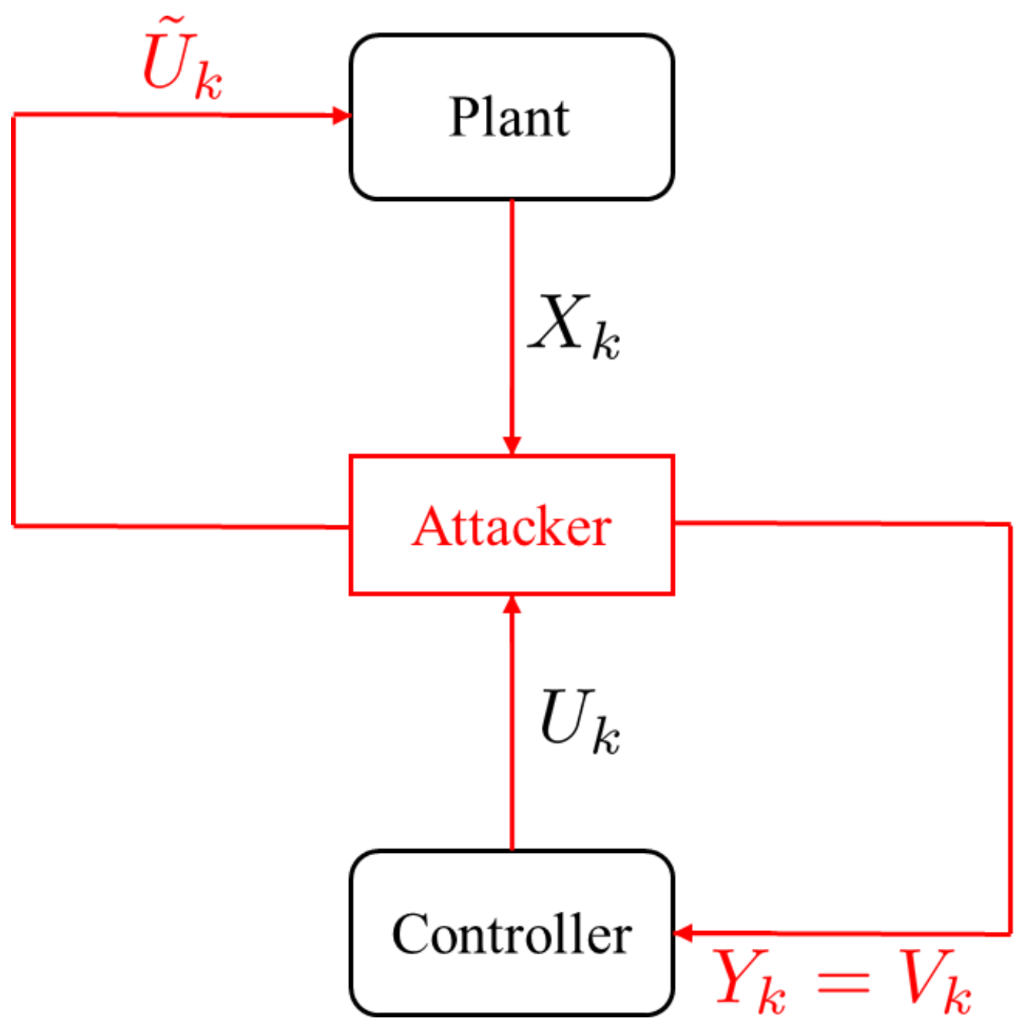


A malicious controller for the plant

Exploration phase:



Exploitation phase:



The deception probability:

If A is distributed uniformly in $[-R, R]$, then letting

$$Z_1^k = (X_1^k, U_1^k),$$

we have

$$\lim_{T\to\infty} P_{dec} \leq \frac{I(A; Z_1^L) + 1}{\log(R/\sqrt{\delta\beta})}.$$

The denominator represents the intrinsic uncertainty of A when this is observed at resolution $\epsilon = \sqrt{\delta\beta}$ corresponding to the entropy of the quantized random variable $H(A_\epsilon)$.

The numerator represents the information revealed about A from the observation of the random variable Z.

In addition, using the least-square learning algorithm, we also provided a lower bound on the deception probability.

References:

M. J. Khojasteh, M. Hedayatpour, J. Cortés, and M. Franceschetti, "Event-triggered stabilization over digital channels of linear systems with disturbances," arXiv preprint arXiv:1805.01969, 2018.

M. J. Khojasteh, A. Khina, M. Franceschetti, and T. Javidi, "Authentication of cyber-physical systems under learning-based attacks," arXiv preprint arXiv: 1809.06023, 2018.

CPS: Synergy: Triggered Control of Cyber Physical Systems with Communication Channels Constraints

Award ID#: 1446891