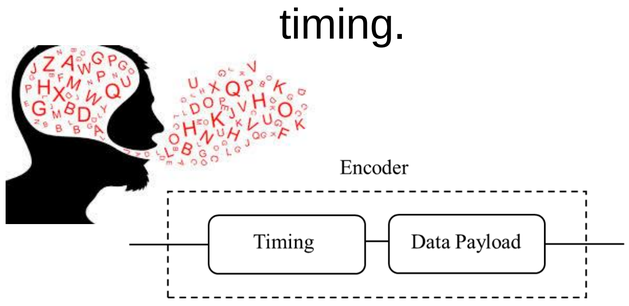
Communication and security in cyber-physical systems

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

Timing information

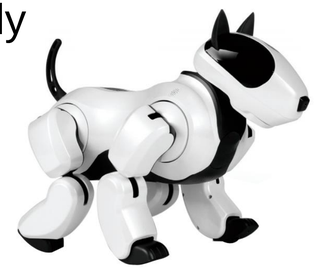
In the same way that subsequent pauses in spoken language are used to convey information, it is also possible to transmit information in communication systems not only by message content but also with its timing.



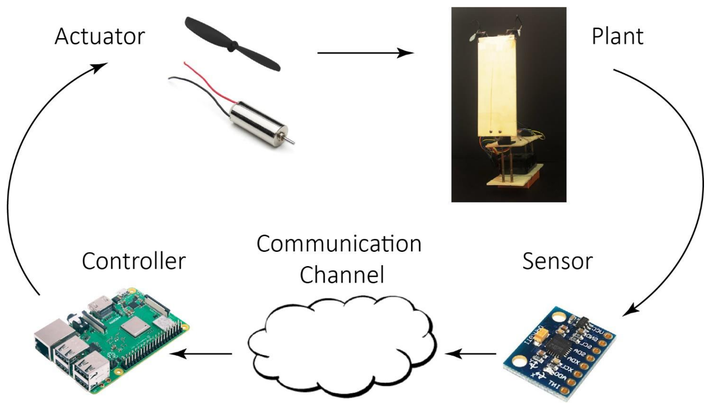
Event-triggered control

In CPS we need to use distributed resources efficiently

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



Experimental Validation



Delay Upperbound = 6ms
Packet Size = 1 bit

Number of Samples = 6541
Number of Triggering = 170

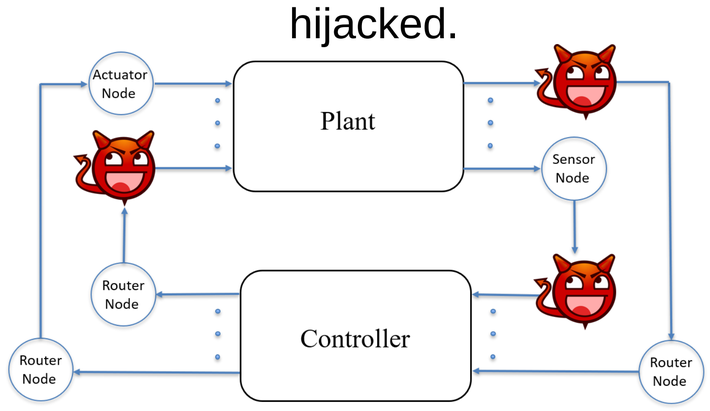
Information Transmission Rate
8.6633 bit/sec

<

Entropy Rate of the System
10.5461 bit/sec

Attacks on CPS

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



MITM attack types

Replay

[redacted] Y. Mo, B. Sinopoli (2009)

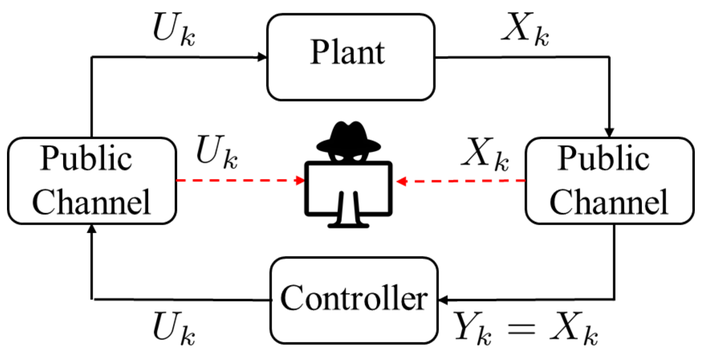
Statistical-duplicate B. Satchidanandan, P. R. Kumar (2017) R. S. Smith (2011)

$$X_{k+1} = aX_k + U_k + W_k$$

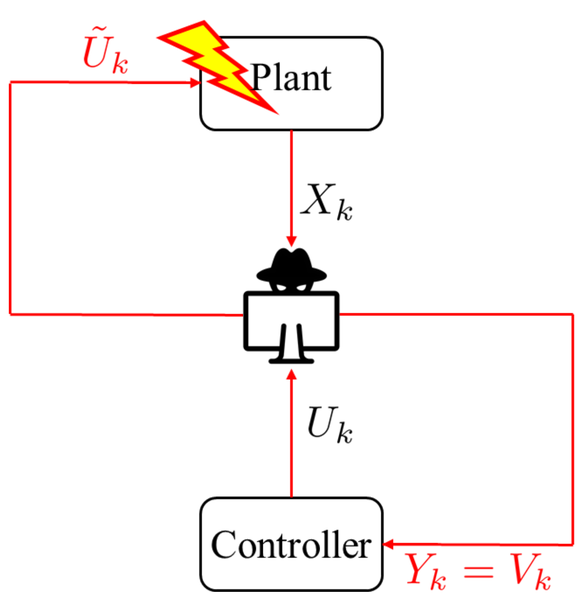
Learning-based M. J. Khojasteh, A. Khina, M. Franceschetti, T. Javidi (2019)

$$X_{k+1} = aX_k + U_k + W_k$$

Learning phase



Hijacking phase

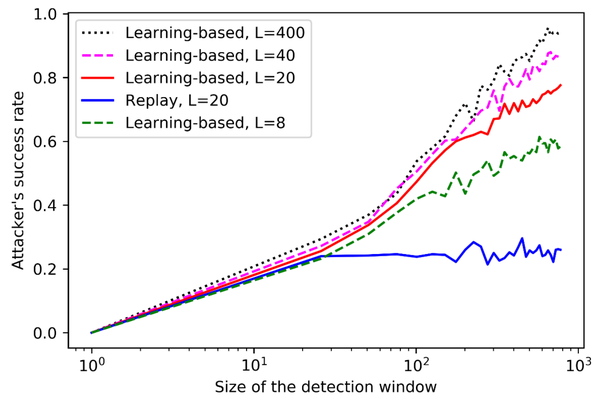


lower bound

Least-square learning algorithm

$$\hat{A} = \frac{\sum_{k=1}^{L-1}(X_{k+1} - U_k)X_k}{\sum_{k=1}^{L-1} X_k^2}$$

$$\lim_{T\to\infty} P_{dec}^a \geq 1 - \frac{2}{(1+\delta\beta)^{L/2}}$$



The deception probability, upper bound

Assume the open-loop gain of the plant is a random variable

$$A \sim \text{Unif.}[-R, R]$$

whose distribution is known to the attacker, and whose realization is known to the controller. Then letting

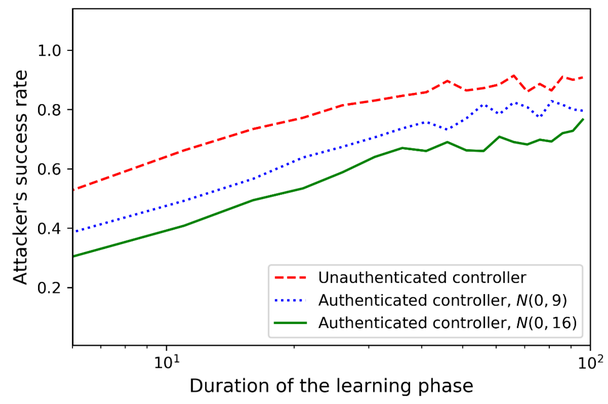
$$Z_1^k = (X_1^k, U_1^k)$$

we have

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

Privacy-enhancing signal

$$U_k = \bar{U}_k + \Gamma_k$$



2019 NSF Cyber-Physical Systems Principal Investigators' Meeting
November 21-22, 2019 | Crystal City, Virginia

Award ID#: 1446891