THE LEAKY ACTUATOR: A PROVABLY-COVERT CHANNEL IN CYBER PHYSICAL SYSTEMS

Amir Herzberg
amir.herzberg@uconn.edu
University of Connecticut
Storrs, USA

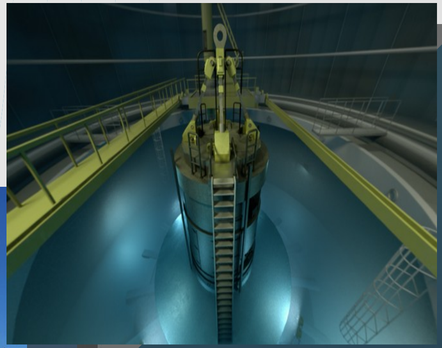
<u>Yehonatan Kfir</u>
yehonatank@gmail.com
Bar-Ilan University
Ramat-Gan, Israel

ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC), 2019

INTRODUCTION

- **Cyber Physical Systems (CPS)** - Smart systems that include networks of physical and computational components, all aimed to governed a physical process.
- **Examples**: Nuclear Plants, Power Generations, Water Plant, Transportations.






- Critical for our life
- Built from large number of devices:

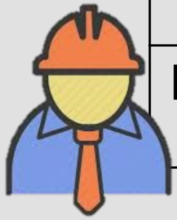
  Sensors, Actuators, Controllers…



INTRODUCTION

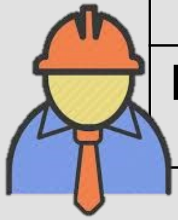
- Devices are chosen based on **sufficient specification** and **lowest cost**.

	Device A	Device B
Specification	High Quality	Sufficient Quality
Price	Expensive	Cheap



INTRODUCTION

- Devices are chosen based on **sufficient specification** and **lowest cost**.

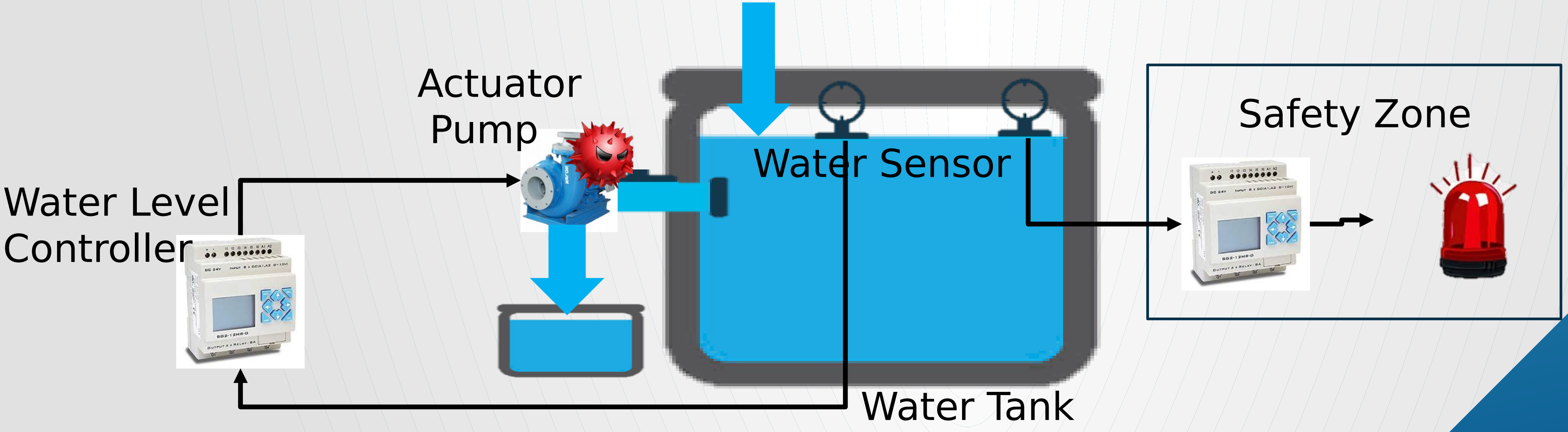


	Device A 	Device B 	Malicious 
Specification	High Quality	Sufficient Quality	Sufficient Quality
Price	Expensive	Cheap	Very Cheap

- **Supply Chain Attack:** Attacker can offer a malicious device with sufficient quality.
- **Attacker Goal:** To cause damage, by deploying its own malicious device.

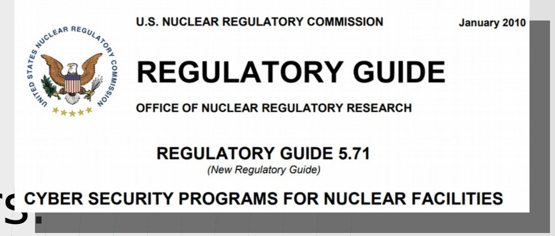
ATTACKER CHALLENGE - 1

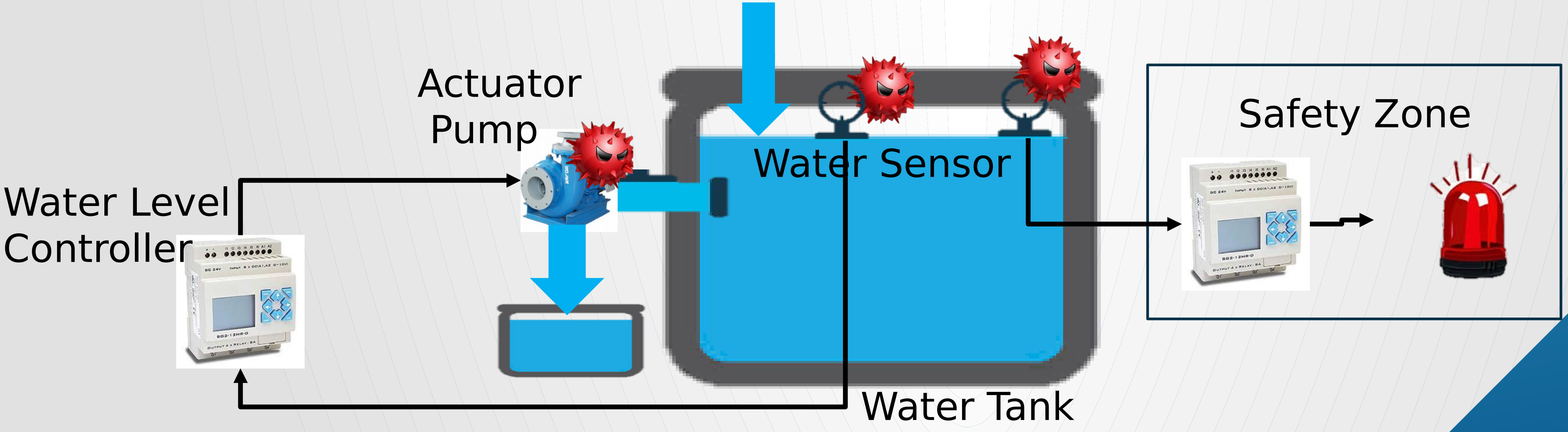
- In order to cause damage, **multiple devices should co-operate**.



ATTACKER CHALLENGE - 1

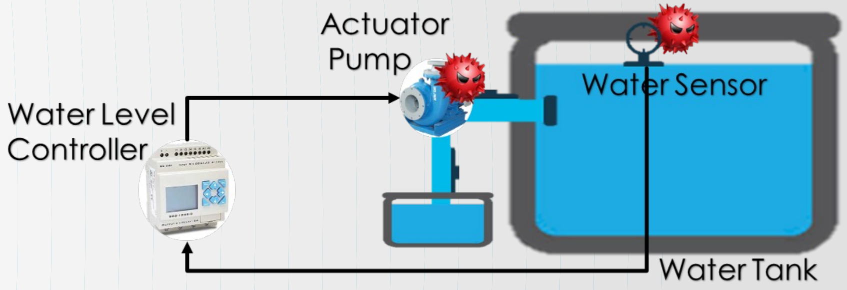
- In order to cause damage, **multiple devices should co-operate**.
- Regulation today requires **isolation inside the CPS**
- There is no **direct communication between** sensor and actuators.





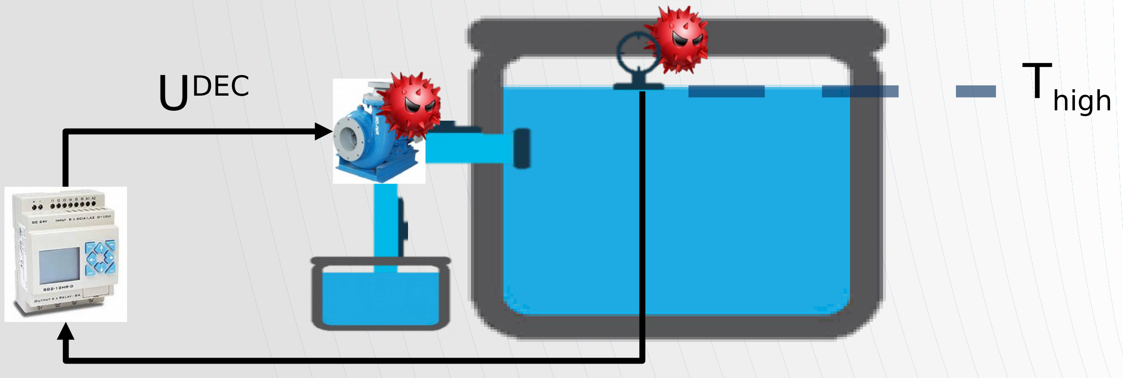
ATTACKER CHALLENGE

How to communicate **between** malicious devices?



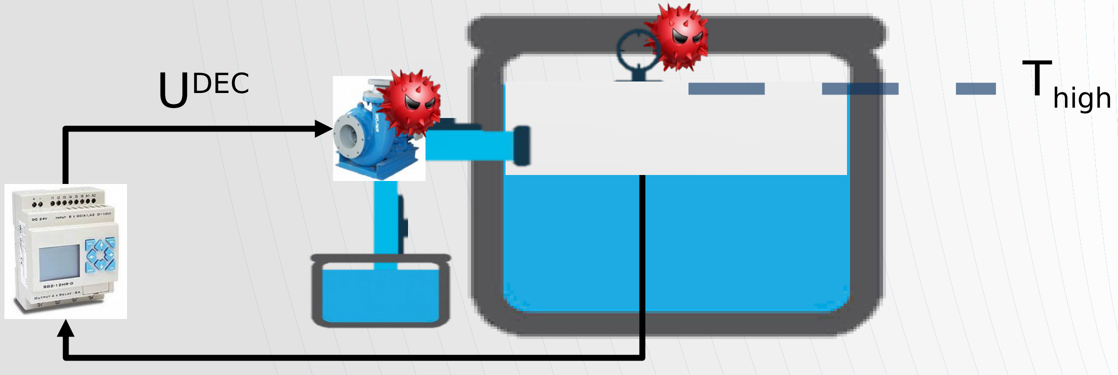
FEEDBACK CONTROL LOOP

- Feedback control loops are the main method used to stabilize physical values in CPS.
- Threshold-controller
  - Actuator with two possible commands to increase / decrease the physical value: U^{INC} / U^{DEC}
  - Two thresholds: T_{high}, T_{low}
- When the sensor measurements reach T_{high} / T_{low} , the controller changes its output to decrease / increase the signal.



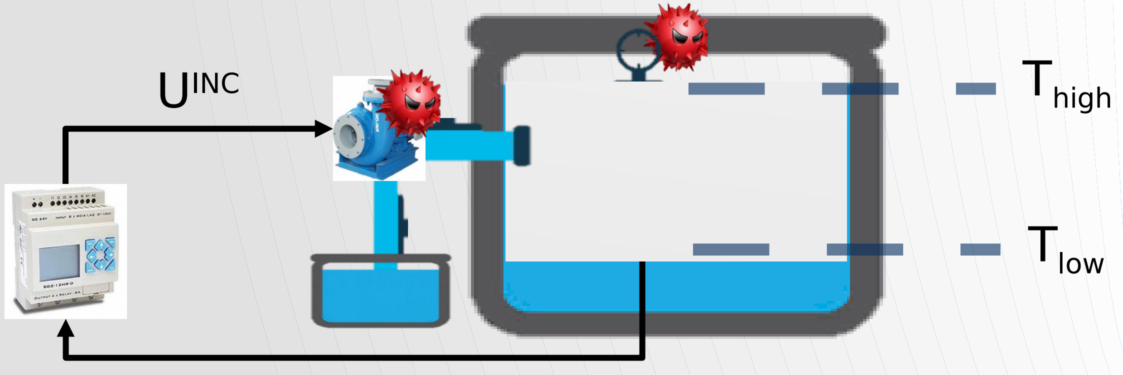
FEEDBACK CONTROL LOOP

- Feedback control loops are the main method used to stabilize physical values in CPS.
- Threshold-controller
  - Actuator with two possible commands to increase / decrease the physical value: U^{INC} / U^{DEC}
  - Two thresholds: T_{high}, T_{low}
- When the sensor measurements reach T_{high} / T_{low} , the controller changes its output to decrease / increase the signal.



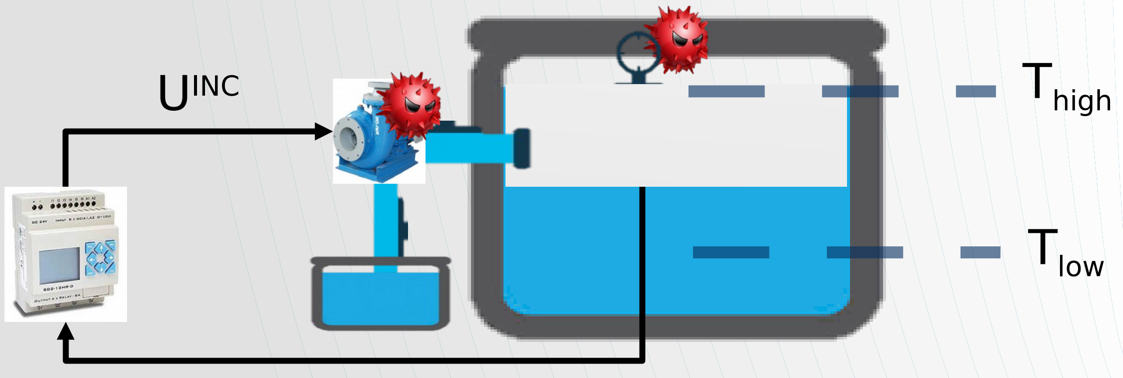
FEEDBACK CONTROL LOOP

- Feedback control loops are the main method used to stabilize physical values in CPS.
- Threshold-controller
  - Actuator with two possible commands to increase / decrease the physical value: U^{INC} / U^{DEC}
  - Two thresholds: T_{high}, T_{low}
- When the sensor measurements reach T_{high} / T_{low} , the controller changes its output to decrease / increase the signal.



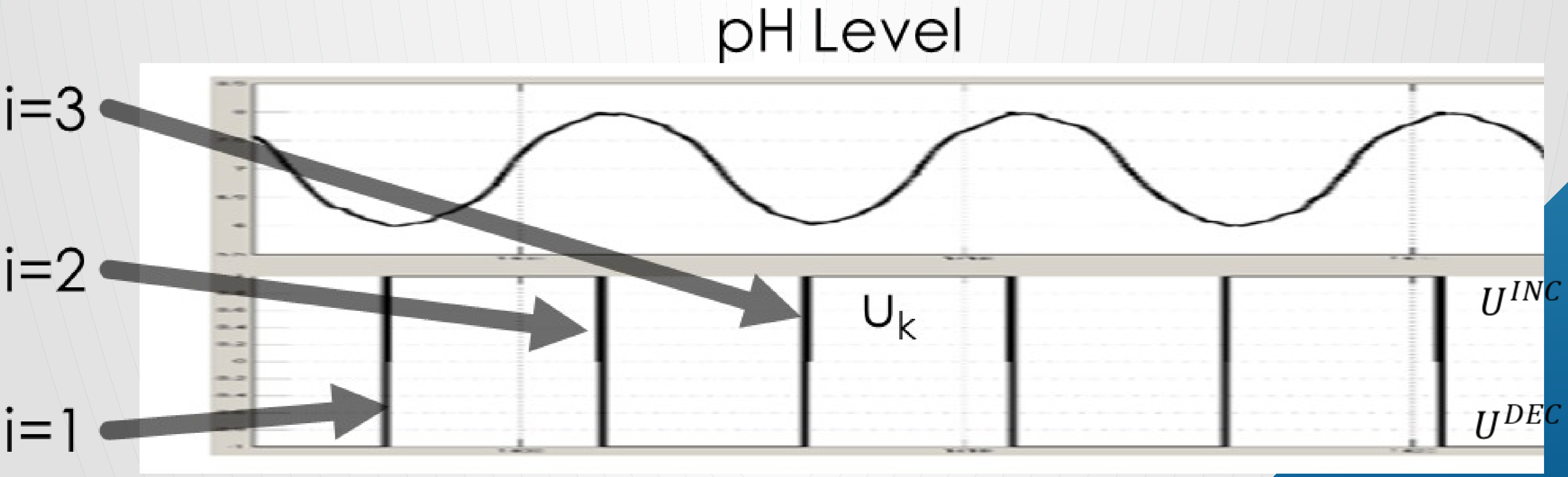
FEEDBACK CONTROL LOOP

- Feedback control loops are the main method used to stabilize physical values in CPS.
- Threshold-controller
  - Actuator with two possible commands to increase / decrease the physical value: U^{INC} / U^{DEC}
  - Two thresholds: T_{high}, T_{low}
- When the sensor measurements reach T_{high} / T_{low} , the controller changes its output to decrease / increase the signal.



FEEDBACK CONTROL LOOP

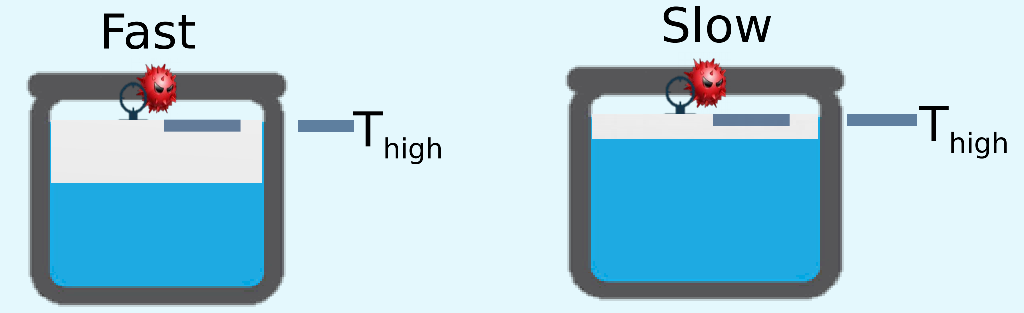
- Widely used in: phase controller, current limiter, pH controllers.
- Periodic Physical Process
  - The process value continuously iterates and pass the thresholds: T_{high}, T_{low}
  - The actuator's input, changes between U^{INC} and U^{DEC} periodically.
  - We denote the i^{th} *transition of the actuator's output by i.*



LEAKY-ACTUATOR COMMUNICATION METHOD

- Upon receiving a command $u_k \in \{U^{INC}, U^{DEC}\}$, the **actuator** changes its output state v_k, **with some random delay.**
- Actuator's **delay influences the process**, which is monitored by the sensor.
- Attacker will use the delay for signaling:
  - Fast / Slow response times, can signal bits 0/1.

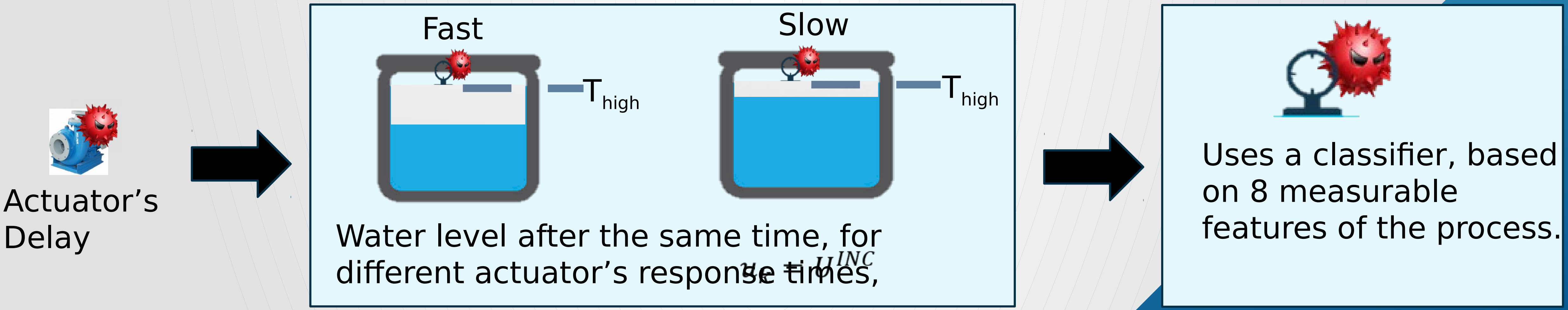
Actuator's Delay



Water level after the same time, for $u_k = U^{INC}$ different actuator's response times,

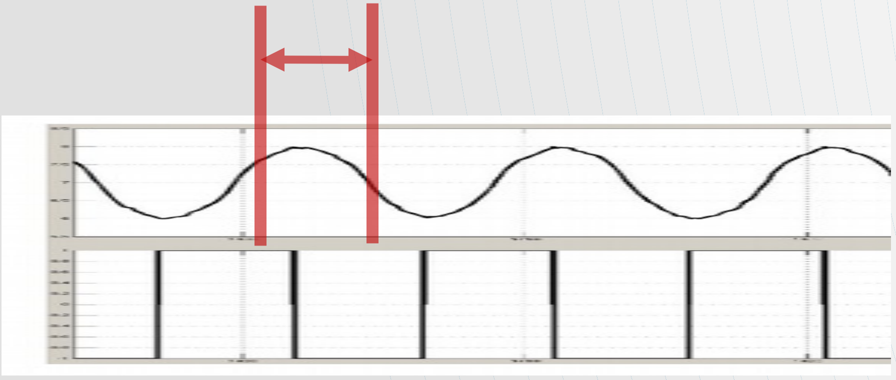
LEAKY-ACTUATOR COMMUNICATION METHOD

- Upon receiving a command $u_k \in \{U^{INC}, U^{DEC}\}$, the **actuator** changes its output state v_k, **with some random delay.**
- Actuator's **delay influences the process**, which is monitored by the sensor.
- Attacker will use the delay for signaling:
  - Fast / Slow response times, can signal bits 0/1.



THE RECEIVER

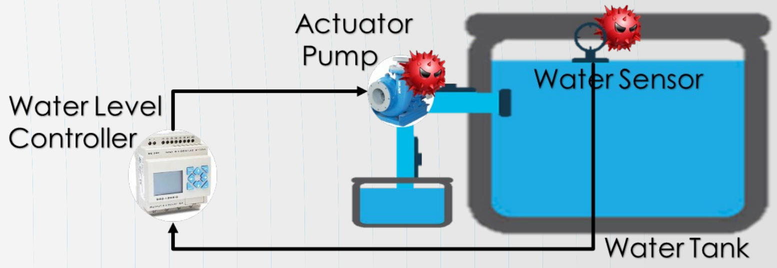
- The receiver measures a set of physical properties of the physical value z_k.
- Properties calculated over a set of $\{z_k\}$:
  - Starting at the first z_k that pass one of the thresholds T_{high}, T_{low}.
  - Ends on the next threshold.



Property	Description
Last Threshold Passed	The last threshold passed by the physical process. The values of this feature can be T_{high} or T_{low}.
Set Size	The number of samples in the set of z_k.
Max z	The maximal value of z_k in the set.
Min z	The minimal value of z_k in the set.
Linear Approximation Coefficients	The linear approximation of z_k in the set. Formally, there are three coefficients in this feature. Two coefficients $A_{1,0}, A_{1,1}$ represent the approximated function $A_{1,1} \cdot x + A_{1,0}$ of the values z_k, and a third coefficient err_1 represents the least-mean-square error of the approximated function.
2^{nd}-order Polynomial Approximation Coefficients	The second order approximation of z_k in the set. Formally, there are four coefficients in this feature. Three coefficients $A_{2,0}, A_{2,1}, A_{2,2}$ represent the approximated function $A_{2,2} \cdot x^2 + A_{2,1} \cdot x + A_{2,0}$ of the values z_k, and a fourth coefficient err_2 represents the least-mean-square error of the approximated function.

Table 1: Features used by the covert receiver classifier

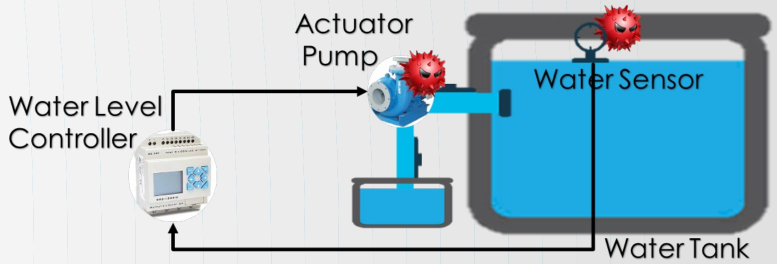
ATTACKER CHALLENGES



- How to communicate **between** malicious devices?

Delay

ATTACKER CHALLENGES

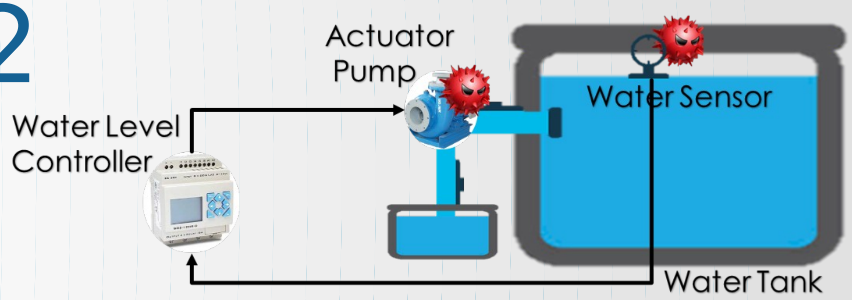


- How to communicate **between** malicious devices?

Delay

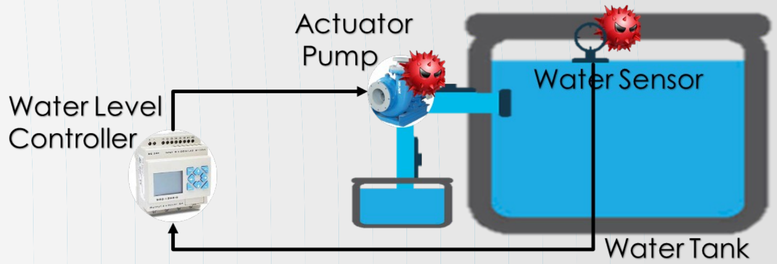
Creates Anomaly in the CPS behavior…

ATTACKER CHALLENGE - 2



- A lot of works on anomalies detections in CPS.
- Communication Network Anomalies
  - Kleinmann, Amit, and Avishai Wool. "Accurate modeling of the siemens s7 scada protocol for intrusion detection and digital forensics.“, 2014.
- Physical Anomalies – malicious sensor reporting / malfunctioning actuator
  - Urbina, David I., et al. "Limiting the impact of stealthy attacks on industrial control systems.", 2016.

ATTACKER CHALLENGES



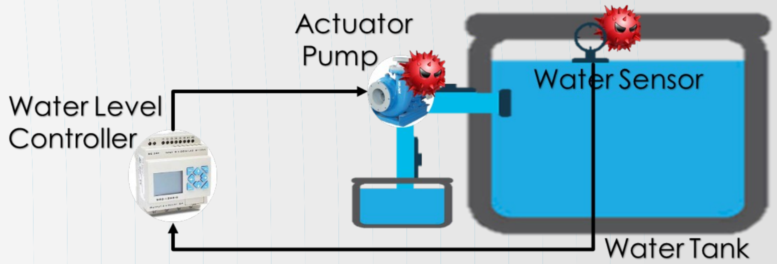
- How to communicate **between** malicious devices?
- **How to avoid detection?**

Delay

Creates Anomaly in the CPS behavior…

Urbina, David I., et al. "Limiting the impact of stealthy attacks on industrial control systems.", 2016.

ATTACKER CHALLENGES



- How to communicate **between** malicious devices?
- **How to avoid detection?**

Covert Channel

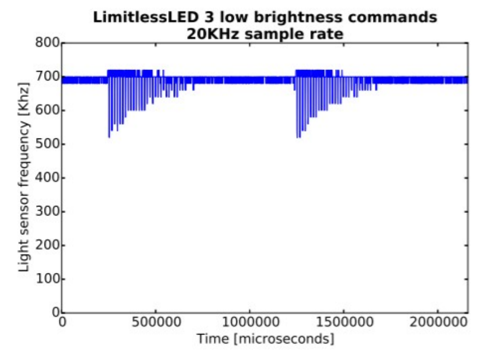
Delay

Creates Anomaly in the CPS behavior…

Urbina, David I., et al. "Limiting the impact of stealthy attacks on industrial control systems.", 2016.

COVERT CHANNELS

- Communication channel are critical for operating malwares.
- “**Covert**” - using some **“<u>unmonitorred</u>”** channels
  - Encoding information using light brightness (“Extended functionality attacks on IoT devices: The case of smart lights“, Shamir et. al. 2016)
  - Packet headers (“Embedding Covert Channels into TCP/IP”, Murdoch et. al. , 2005)
  - Acoustic emissions of a motor (“Process-aware covert channels using physical instru-mentation in cyber-physical systems”, Krishnamurthy et. al. 2018)
  - And more…
- Monitoring the “**<u>unmonitorred</u>**” property, reveals the communication channel.



(a) Low brightness - 3 commands

Eyal Ronen and Adi Shamir. Extended functionality attacks on IoT devices: The case of smart lights. In2016 IEEE European Symposium on Security and Privacy(EuroS&P), pages 3–12. IEEE, 2016

PROVABLE COVERT CHANNELS

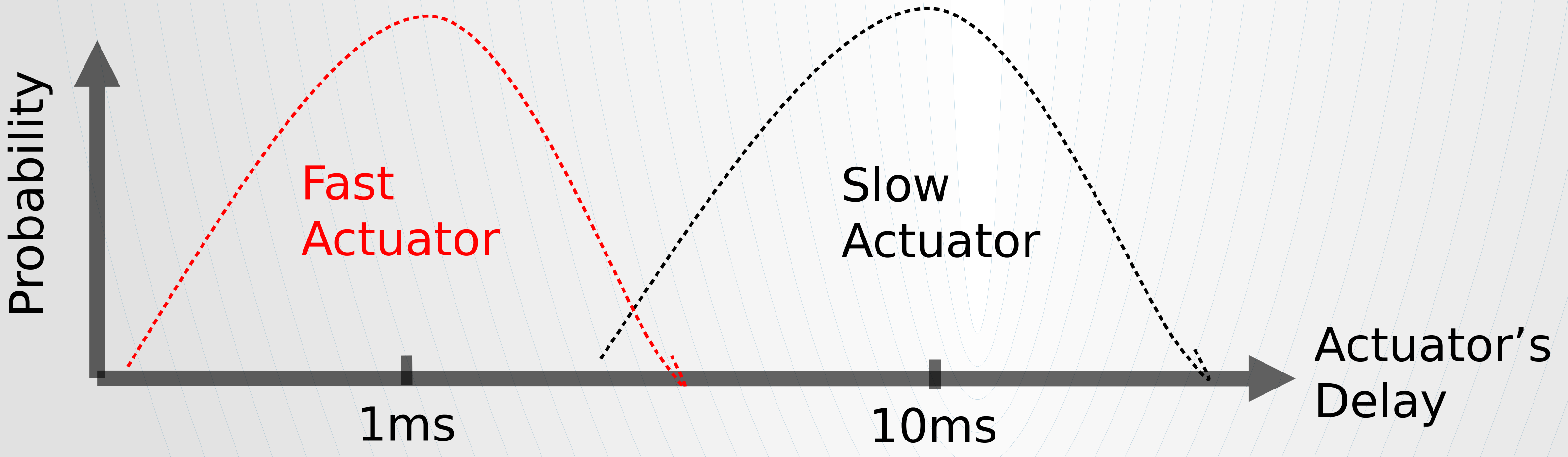
- “**Provable-Covert**” –
  - No secret property
  - Proving that it is impossible to detect the channel (under well defined assumptions)

$\Pr(D($  $) = Mal.) \approx \Pr(D($  $) = Mal.)$

- Provable channels were presented in the past, for IP networks:
  - Liu, Yali, et al. "Robust and undetectable steganographic timing channels for iid traffic.", 2010.
- **How to (provably) avoid detection?**

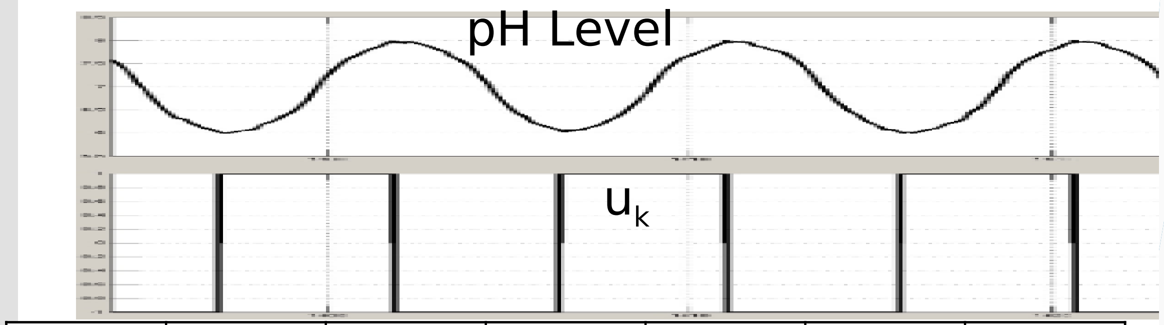
LEAKY-ACTUATOR COVERT CHANNEL

- The provably-covert channel is based on **two basic observations** about actuators:
  - The **response time is random,** derived from some (known) distribution.
  - There are different **benign** types of actuators in the market:
    - Low response time (‘fast / high quality actuators’)
    - Long response time (‘slow actuators’).

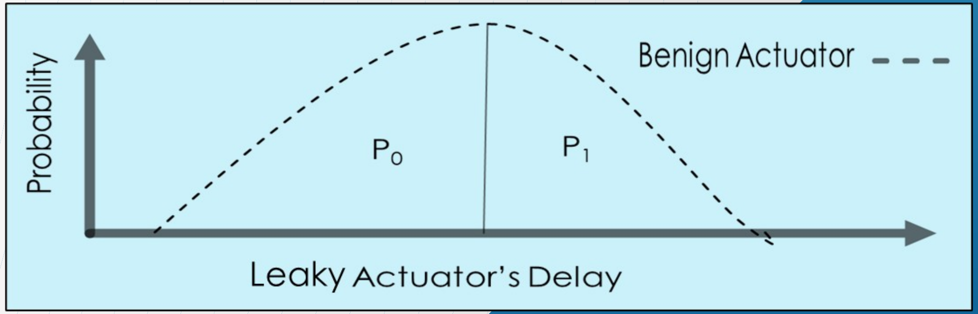


LEAKY-ACTUATOR COVERT CHANNEL

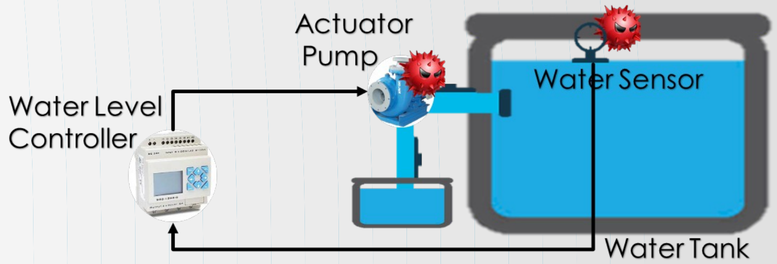
- Leaky-actuator is using an internal fast actuator.
- It adds a **pseudo-random delay**, from two possible delay distributions: P_0 and P_1
- For transmitting bit b_i, the leaky actuator choses the added delay distribution to be P_{b_i}
- In **random** choice of b_i , the delay distribution of the leaky actuator will be identical to benign actuator.



i	1	2	3	4	5	6
	0	0	1	0	1	1
$\mathbf{P_{b_i}}$	P_0	P_0	P_1	P_0	P_1	P_1



ATTACKER CHALLENGES



- How to communicate **between** malicious devices?
- **How to avoid detection?**

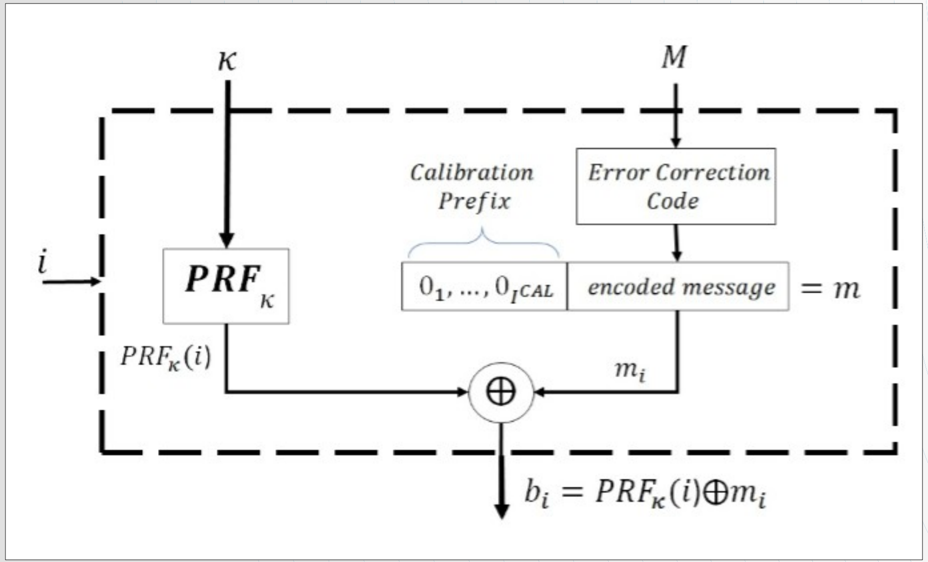
Pseudo-random	Delay

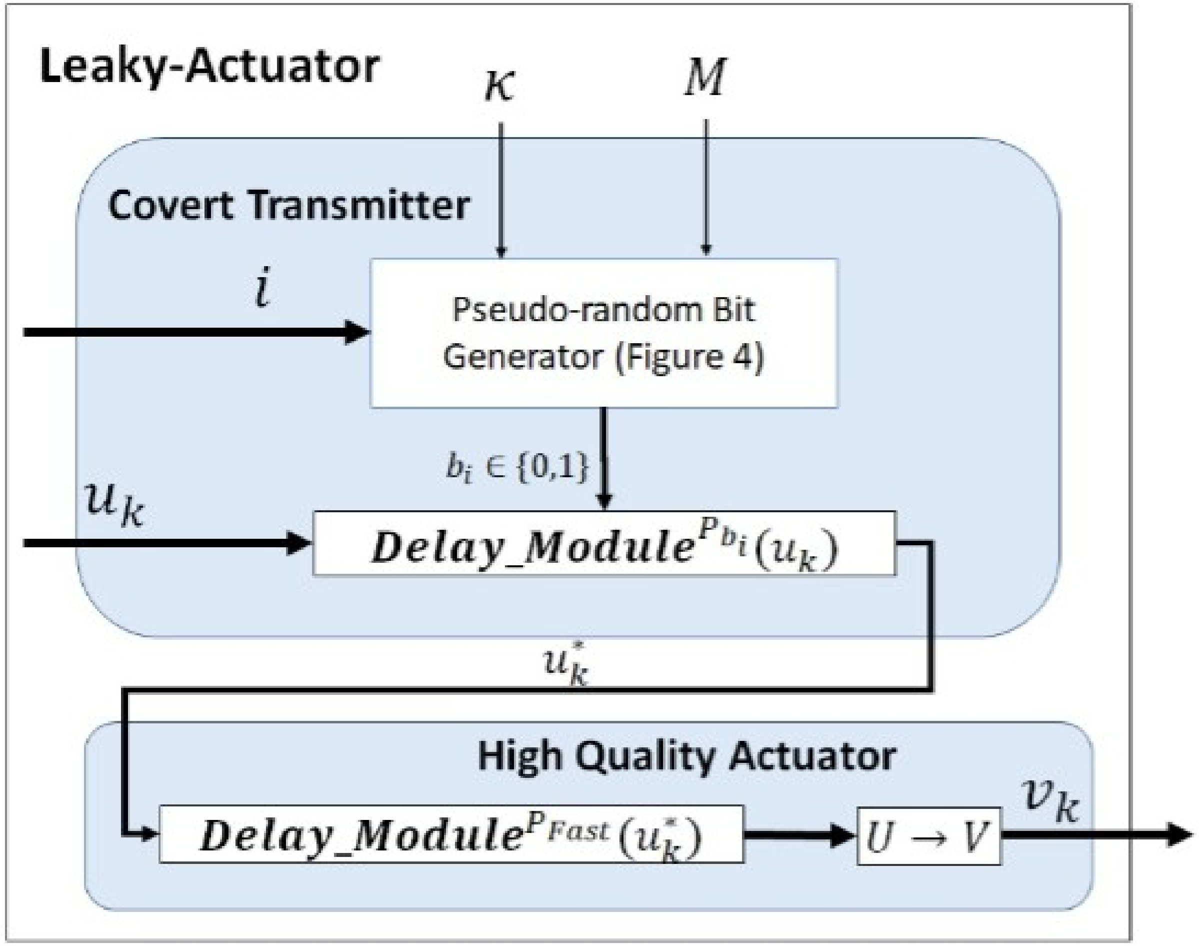
Design	Receiver	Evaluation

THE LEAKY ACTUATOR DESIGN

- Deployed all its devices with a secret key, $\kappa \xleftarrow{\$} \{0,1\}^l$
- M – Message to send
- m – Encoded Message
- i – Transitions counter

Pseudo-random Bit Generator

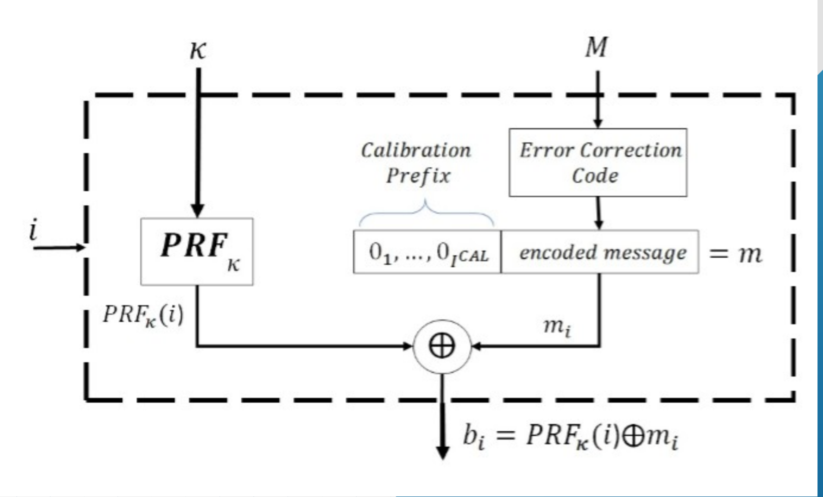




Design | Receiver | Evaluation

THE LEAKY ACTUATOR: BIT GENERATOR

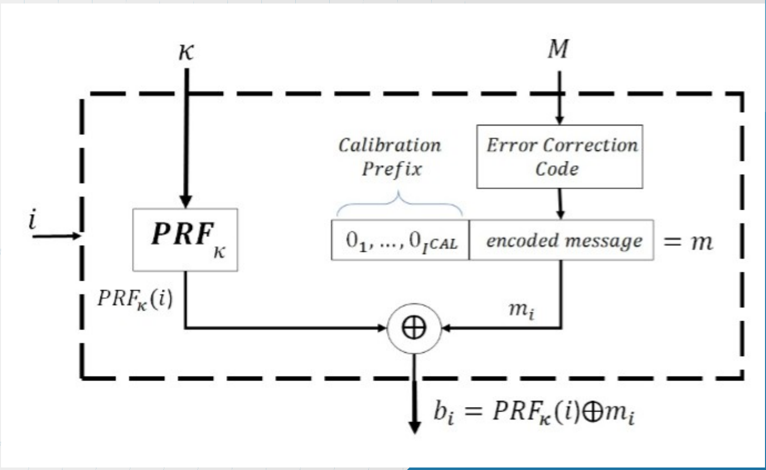
- Pseudo-random Bit Generator
  - **Inputs**: The message M, the key κ and the transition index i .
  - **Output**: b_i - a pseudo-random bit, based on the i^{th} message bit, M_i , and the output of the PRF: $PRF_k(i)$
  - Message M encoded with error-correction code to m.
    - Decreases bit-error-rate.
  - First I^{CAL} bits are all 0 – will be used for calibrating the sensor.
- The Pseudo-random bit generator ensures that the delay is Indistinguishable form random (from PRF property - see paper).



$\Pr(D($$) = Mal.) \approx \Pr(D($$) = Mal.)$

THE RECEIVER

- **Synchronization Assumption** (relaxed in the paper): $i^T \equiv i^R$
- **The Goal**: To identify when the delay is derived from P_0 and when from P_1.
  - Detect P_{b_i} --> Conclude b_i --> $m_i^R = b_i \oplus PRF_\kappa(i)$
- **The Challenge:**
  - The delay can not be measured **directly**.
  - The delay has **unknown impact** on the physical process.
- **The Solution**: to use the calibration period to train a classifier.
  - The first I_{CAL} are all 0 --> $m_i = 0$ --> $b_i = 0 \oplus PRF_\kappa(i)$ --> P_{b_i}
  - Different delays present different impact on the physical process.
  - Measure features of the physical process. Label them with the (known) calculated P_{b_i}
  - After calibration period, use the trained classifier to “guess” whether the delay was derived from P_0 or P_1.



EVALUATION

- How good is the receiver in intercepting the leaky-actuator bits?
- **Theoretical:** Channel Capacity.
- **Practical**: Bit-error-rate of our receiver design.

EVALUATION: CHANNEL CAPACITY

- **Channel Capacity** – highest information rate that can be achieved.
- Evaluated two classifiers: **KNN** and Decision Tree (**DT**)
- Different message length $|m|$ and calibrations periods I^{CAL}
- **Results**: About 0.5 bit of information on every transition.

$\lvert m\rvert = 10{,}000$				$\lvert m\rvert = 50{,}000$				$\lvert m\rvert = 100{,}000$			
Classifier	$\frac{I^{CAL}}{\lvert m\rvert}$	p	C	Classifier	$\frac{I^{CAL}}{\lvert m\rvert}$	p	C	Classifier	$\frac{I^{CAL}}{\lvert m\rvert}$	p	C
kNN	0.1%	0.28	0.15	kNN	0.1%	0.12	0.46	kNN	0.1%	0.154	0.38
	0.5%	0.12	0.47		0.5%	0.12	0.46		0.5%	0.13	0.44
	1%	0.12	0.47		1%	0.129	0.45		1%	0.129	0.45
	5%	0.11	0.49		5%	0.11	0.48		5%	0.128	0.45
	10%	0.11	0.49		10%	0.11	0.49		10%	0.128	0.45
DT	0.1%	0.2	0.26	DT	0.1%	0.13	0.43	DT	0.1%	0.154	0.38
	0.5%	0.13	0.44		0.5%	0.11	0.48		0.5%	0.13	0.44
	1%	0.12	0.47		1%	0.11	0.49		1%	0.126	0.45
	5%	0.11	0.49		5%	0.1	0.5		5%	0.126	0.45
	10%	0.11	0.49		10%	0.1	0.5		10%	0.126	0.45

EVALUATION

- **Channel Capacity – 0.5 bit per transition**.
- **Bit-Error-Rate (BER)** – fraction of errors in the bits decoding.
  - **Expansion ECC** – Less than **0.1 bit per transition**.
  - **Reed-Muller ECC** – Better results! ~**0.13 bit per transition**.
- We need better error-correction-codes for this channel [Future Work].

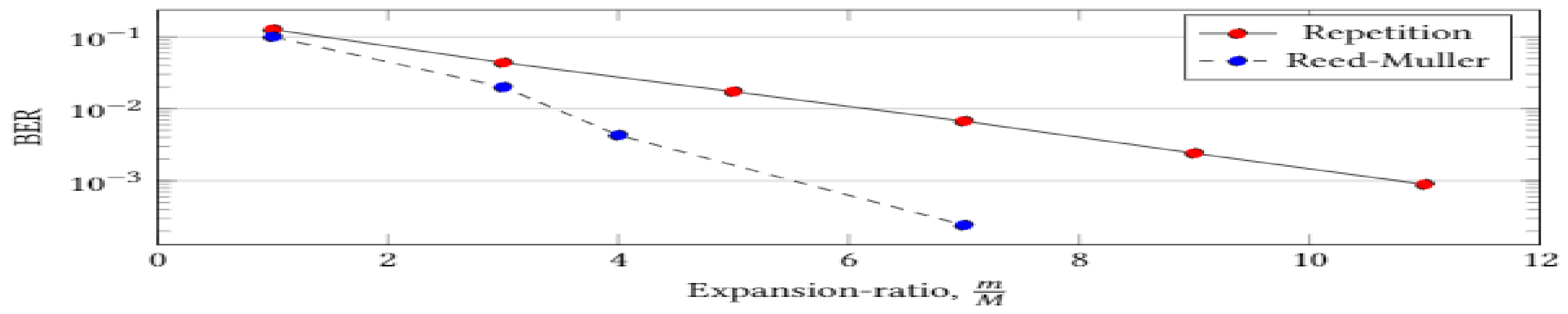


Figure 8: Comparison between repetition code and Reed-Muller codes, for different expansion ratio, with 100,000 bits averaged over 1,000 executions. The calibration period is 1% of the transitions and the classifier is Decision Tree.

SUMMARY AND DISCUSSION

- Choosing devices based on **specification** and **price** enables **provable** covert attacks.
- As for as we know – this is the first **provable** covert channel in CPS.
- Requires to improve defenses:
  - Adding randomness to the channel (e.g. in the controller logic)
  - Purchasing devices from different vendors.
  - Monitoring power consumption of devices.
- In future works:
  - Complimentary channel from the **sensor to the actuator** (“Chatty-Sensor”).
  - Extending the attack to additional control logics and physical processes.

QUESTIONS?