WSTS Conference 2024

Physics-Aware Approach for Detecting PTP Clock Servo Attacks

Vuk Lesi | vuk.lesi@intel.com

Contributors: Christopher Gutierrez, Shabbir Ahmed, Marcio Juliato, Manoj Sastry

Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more on the Performance Index site[1].

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

[1] https://edc.intel.com/content/www/us/en/products/performance/benchmarks/overview/

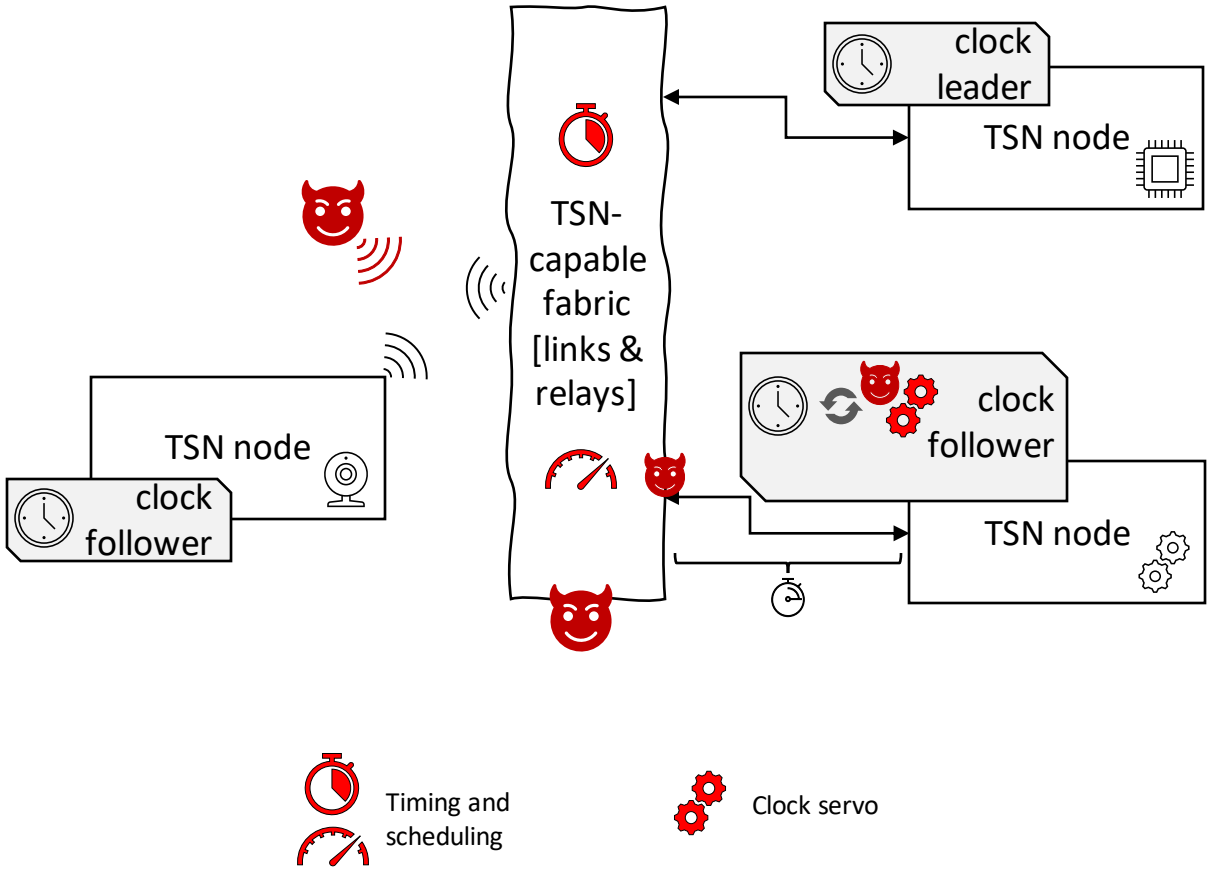
Background

- *Time* synchronization is critical for coordinating sensing, control and actuation in autonomous systems.
- From an adversary's perspective, *time* is an asset that can be compromised.
- Attacks can disrupt real-time functionality impacting safety and plant downtime.
- TSN solutions need to be made resilient.

Outline

- Threat analysis
- Physics-based approach to clock servo monitoring
- Experimental research testbed
- Attack detectability results
- Summary & Next Steps

TSN Attacks



Two Main Entry Points

1. Platform attacks

Local clock control can be modified

2. Protocol attacks

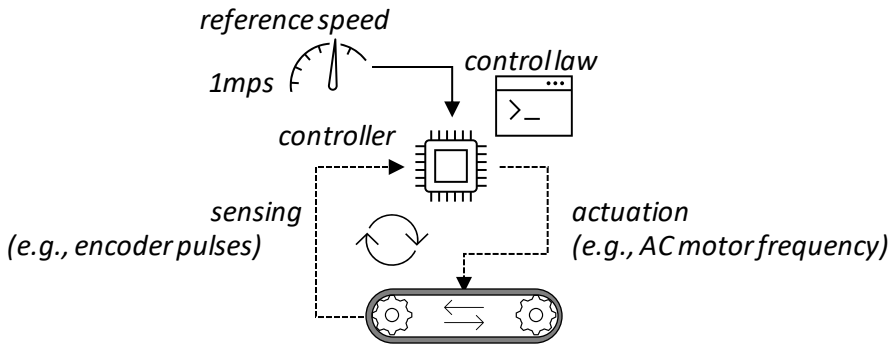
Timestamps can be modified in-flight from leader to follower

EXAMPLE CVE-2021-3570: A missing length check in ptp4l when forwarding PTP messages between ports could allow a potential remote code execution

Physics of Time Synchronization

Conveyor speed control example

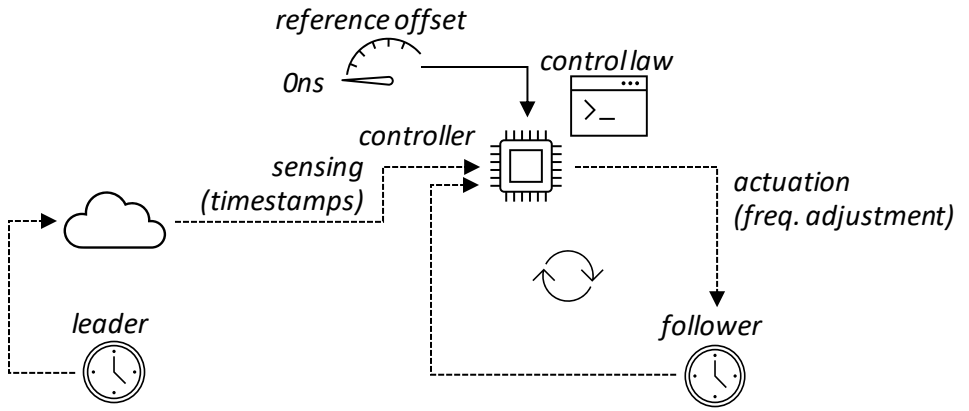
Goal: maintain error between reference and actual speed as close to 0 as possible



- Speed control is a closed-loop control system
- Great because we can use physics to put bounds on expected behavior

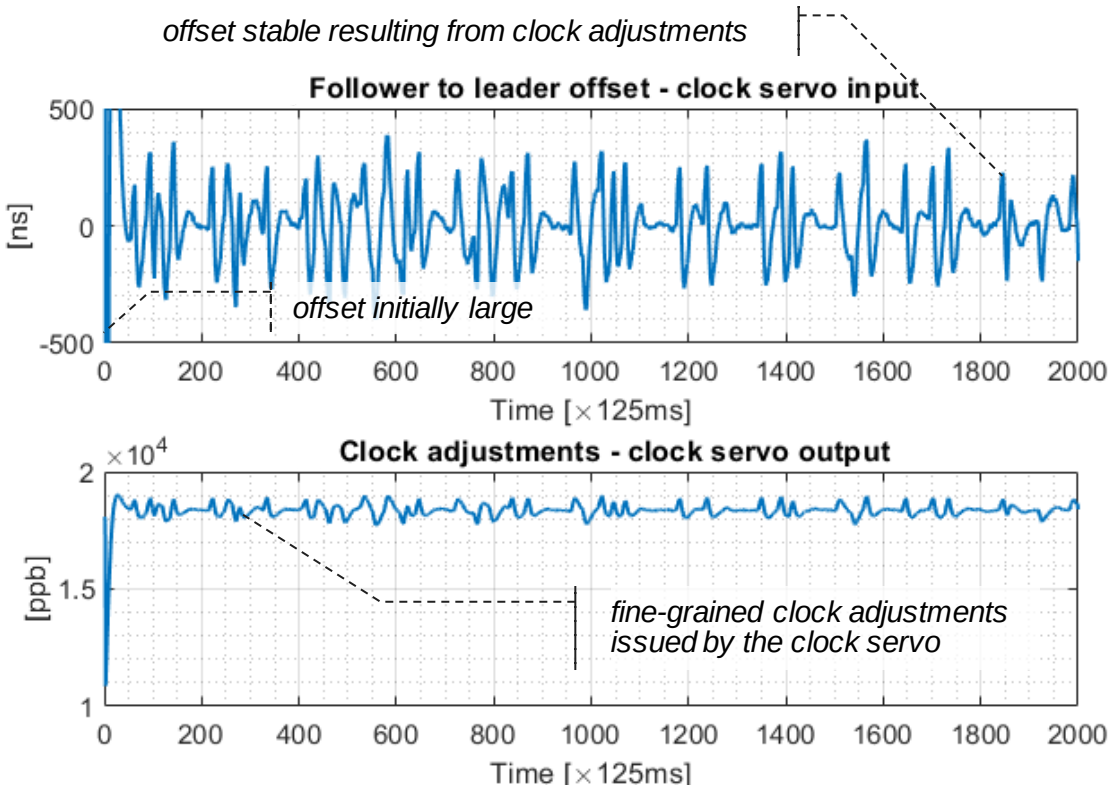
Time sync

Goal: maintain error between two clocks as close to 0 as possible



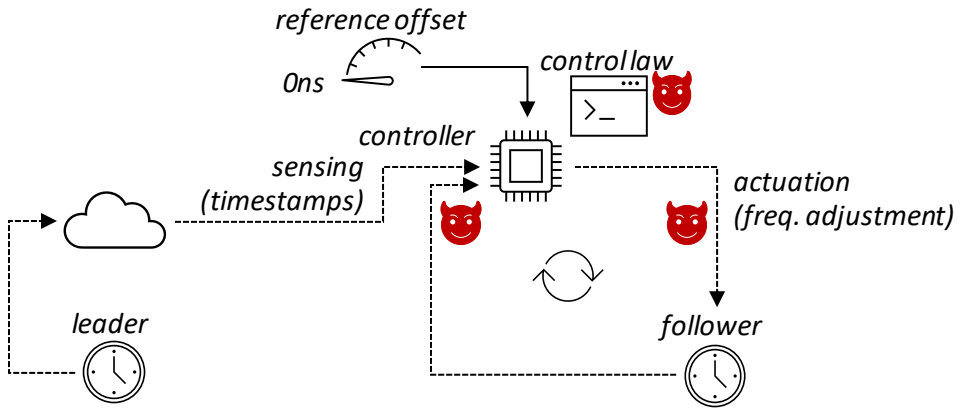
Time sync is a closed-loop control system, too!

Physics of Time Synchronization



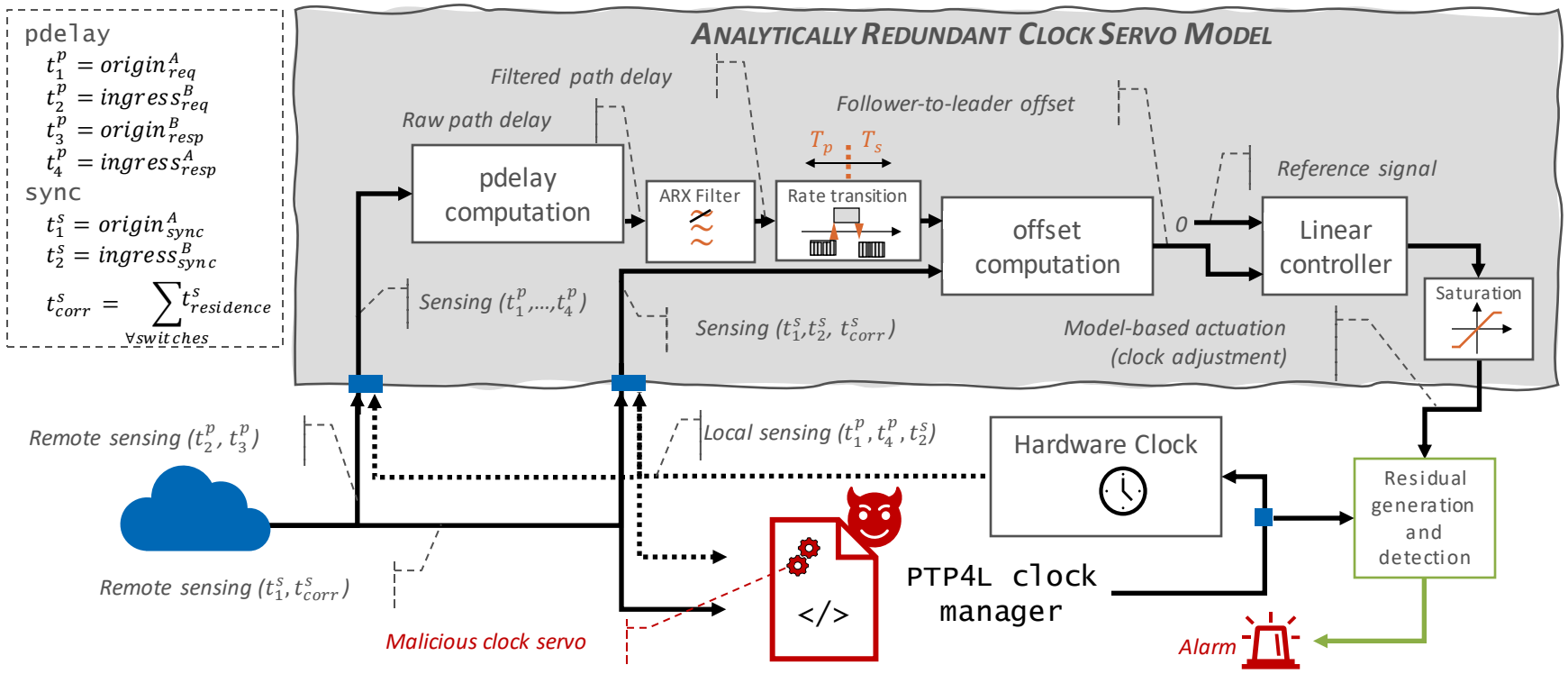
Time sync

Goal: maintain error between two clocks as close to 0 as possible

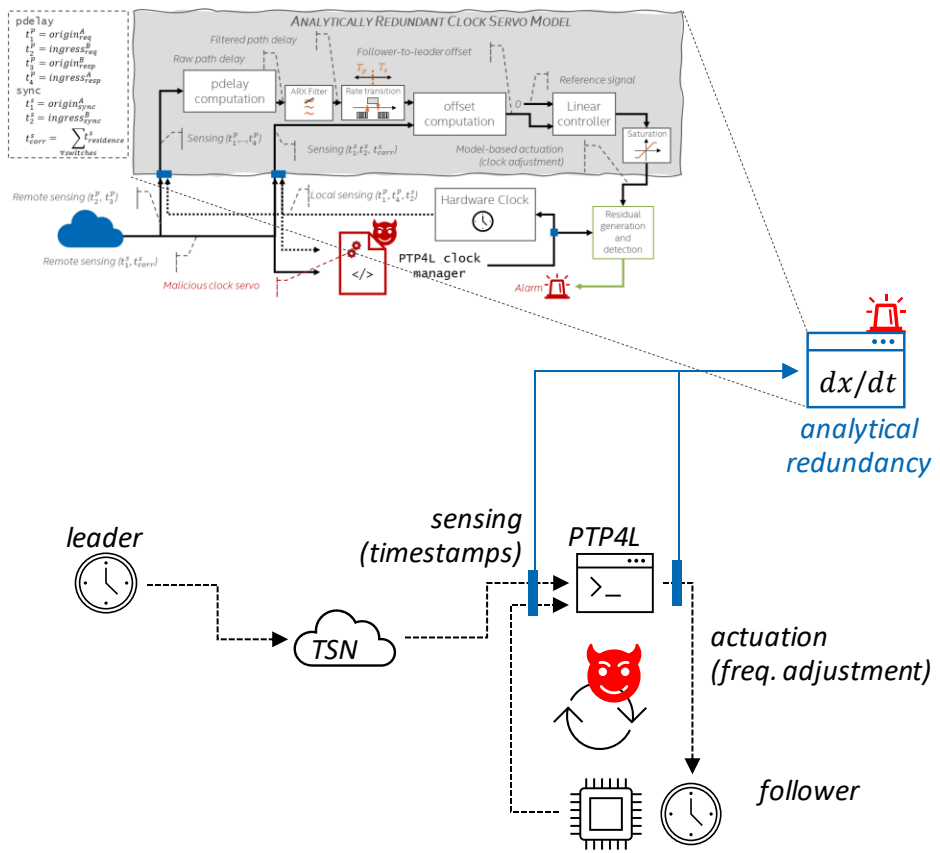


Time sync is a closed-loop control system, too!

Analytically Redundant Clock Servo Model

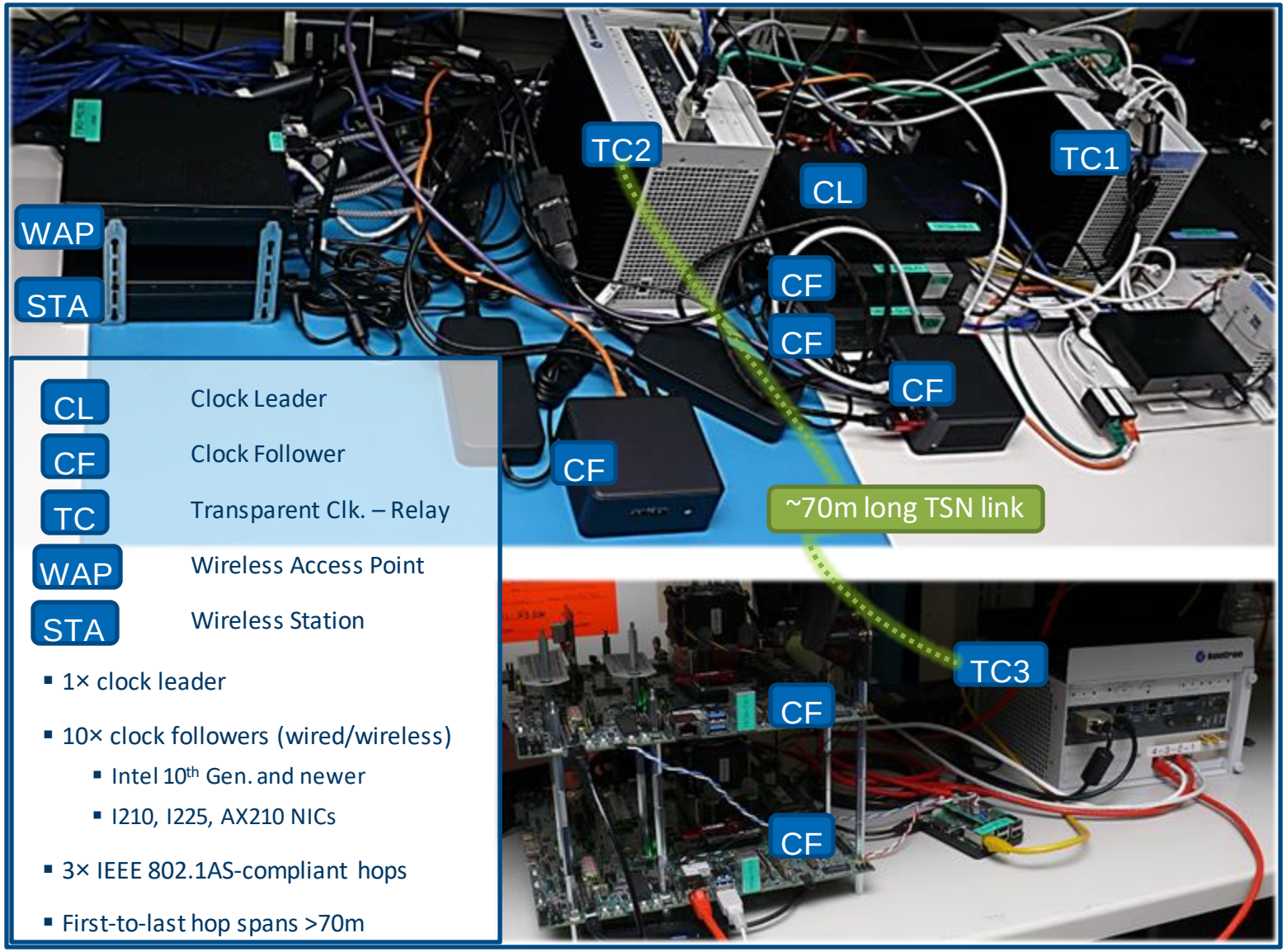


Utilizing the Physics for Security



- From the knowledge of the system structure, we pick a model type and parameter space
- From I/O data, using system identification, we can obtain dynamical models (equations)
- The model is used for monitoring the clock servo output (clock adj.) based on the same input (time offset)
- Heterogeneous redundancy ensures same vulnerabilities are not inherited

TSN Security Testbed

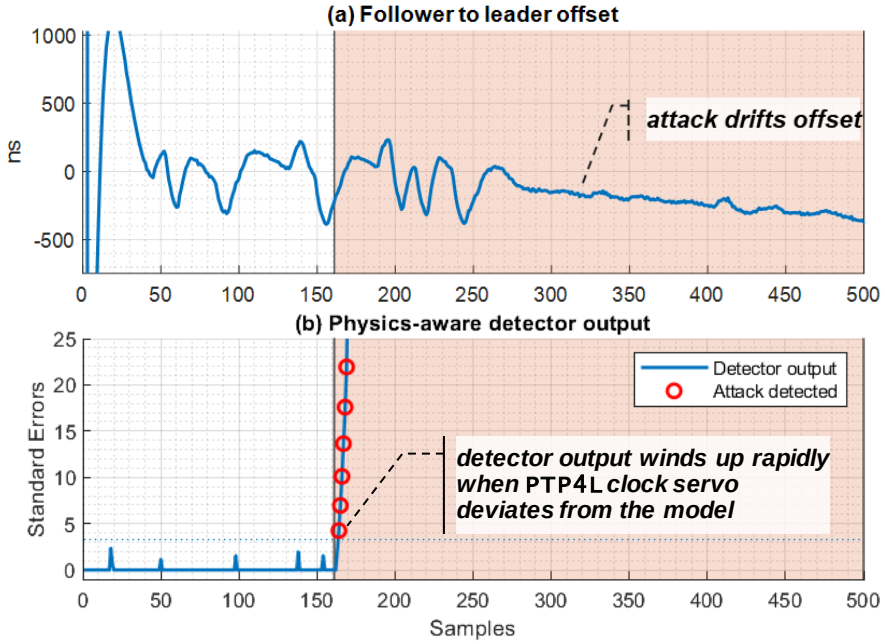


Experimental Results

- Detect attacks targeting PTP4L (Clock Manager)
- Clock manager dynamical behavior compared to physics-aware model
- High accuracy for detecting attacks
  - ~1ns sensing (timestamp modification)
  - ~1ppb actuation (clk. adjustment modification)
  - ~10^{-3} servo parameters (proportional/integral gain)
- Lightweight: exec time ~40ns max. @ Intel 11th Gen. i7
- >100× smaller code base than PTP4L itself

Attack experiment

+1ns/sync bias of time offset



See Disclosures below for workloads and configurations. Results may vary.
Testing performed on 10/31/2022 | OS: Ubuntu 22.04LTS; PTP4L: v3.1.1 custom instrumented | HW: Intel i7-1185GRE reference platform.

Summary & Next Steps

- Time synchronization can be compromised in wired and wireless networks by tampering with clock servos and resulting in safety implications for industrial systems
- Physics behind time sync can be captured in models and used to detect attacks
- Physical models are lightweight, interpretable, and provide heterogenous redundancy
- Demonstrated attacks and validated the approach on a realistic testbed
- Future research to extend physics-based approach to other attacks


intel