Collaborative Research: CPS: Medium: Sensor Attack Detection and Recovery in Cyber-Physical Systems

Insup Lee[1], Oleg Sokolsky[1] and Fanxin Kong[2]

University of Pennsylvania[1] and University of Notre Dame[2]

https://sites.google.com/seas.upenn.edu/cpsrecovery/

Abstract: Cyber-Physical Systems (CPS) are vulnerable to sensor attacks such as spoofing and data injection. This project aims to improve CPS safety, resilience and capability of maintaining normal functionalities by stateful detection and recovery. Our main contributions include using both model-based and learning-based approaches to (1) detect and diagnose the attack, and (2) recover the CPS to predefined target states, using a specific recovery controller.

Challenges

1. How to detect and diagnose useful information about the attacker, such as the attack start time?
2. How to recover the system back to safety within a deadline with guarantee?

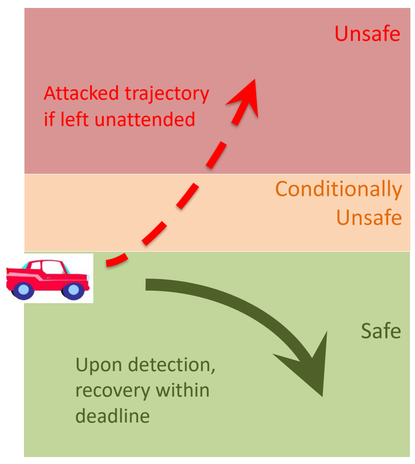


Figure 1: Effects of our framework

Scientific Impacts

1. Enhanced CPS detection and diagnosis abilities against sensor attacks.
2. Improved CPS resilience against sensor attacks by a recovery controller.

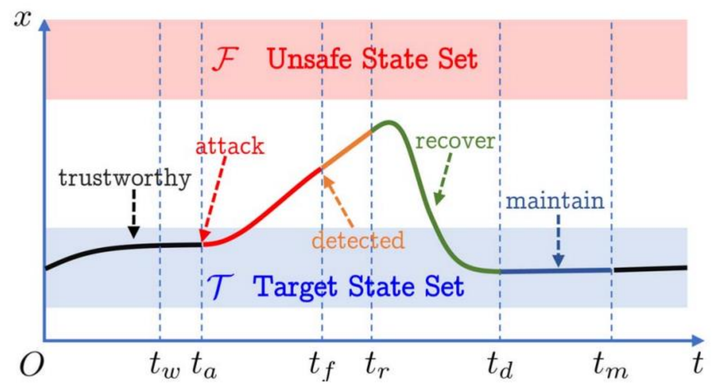
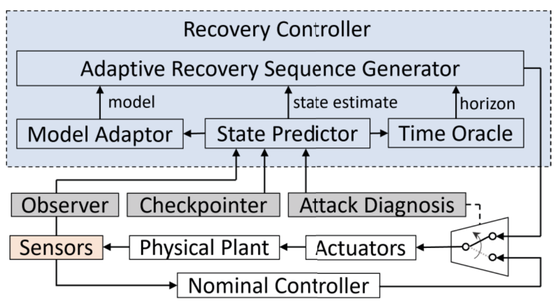


Figure 2: Recovery phases in time

Approach 1: Model-based



$$J = (\boldsymbol{x}_N - \boldsymbol{x}^*)^T \mathbf{Q}_N (\boldsymbol{x}_N - \boldsymbol{x}^*) + \sum_{}^{N-1} (\boldsymbol{x}_k - \boldsymbol{x}^*)^T \mathbf{Q} (\boldsymbol{x}_k - \boldsymbol{x}^*) + \boldsymbol{u}_k^T \mathbf{R} \boldsymbol{u}_k$$

$$\boldsymbol{x}_0 \in X_0 = \boldsymbol{x}_0 \oplus I_0 \quad \text{from state predictor}$$

$$\boldsymbol{x}_{i+1} = \mathbf{A}\boldsymbol{x}_i + \mathbf{B}\boldsymbol{u}_i + \boldsymbol{c} \quad \forall i$$

$$\boldsymbol{u}_i \in \mathcal{U} \quad \forall i$$

$$\boldsymbol{x}_i \cap (\mathcal{F} \oplus \mathbf{A}^i I_0) = \emptyset \quad \forall i \in [0, M]$$

$$\boldsymbol{x}_i \in \mathcal{T} \ominus \mathbf{A}^i I_0 \quad \forall i \in [D, M]$$

Figure 3: MPC-based recovery controller in complex dynamics [1]

With a trustworthy model of system dynamics (plant), we can first checkpoint the states, and roll forward from the last uncompromised state to do LP/LQR/MPC-based recovery control.

Approach 2: Learning-based

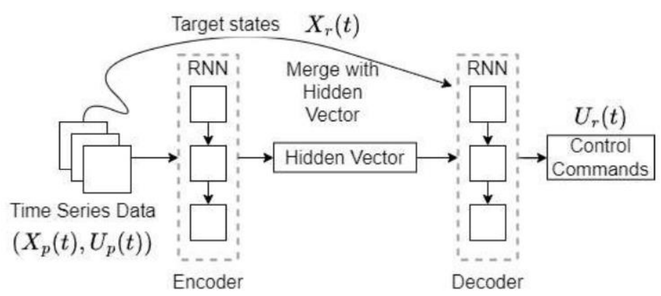


Figure 4: Seq2Seq recovery controller [2]

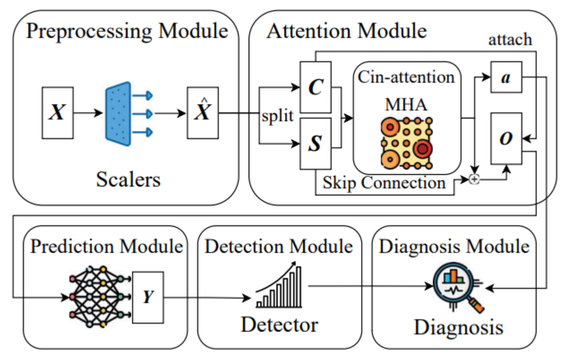


Figure 5: Attention-based sensor attack diagnosis [3]

When the plant model exhibits errors in state estimation, we use Seq2Seq models to reduce these errors.

Experimental Results

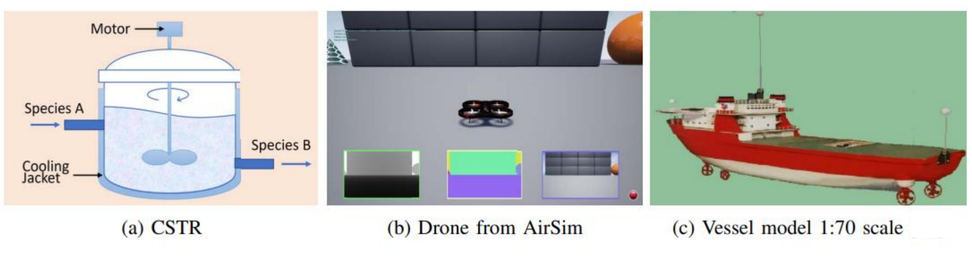


Figure 6: High-fidelity simulators that our methods have tested on [1].

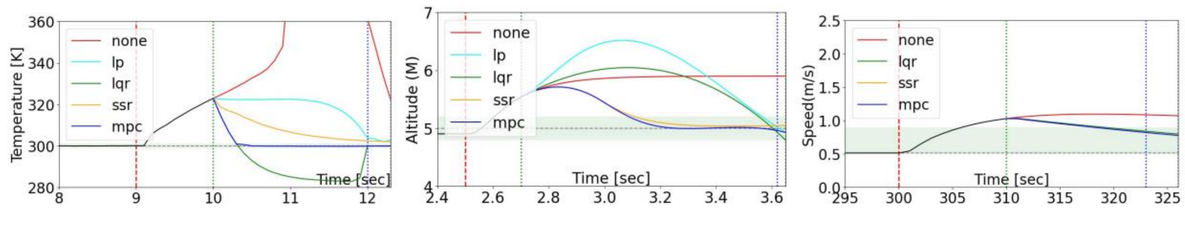


Figure 7: Performance of our recovery method (MPC) compared to state-of-the-art on the three simulators [1]

References and additional papers

[1] Zhang, Lin, et al. "Real-Time Data-Predictive Attack-Recovery for Complex Cyber-Physical Systems." 2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS). IEEE, 2023.
[2] Liu, Mengyu, et al. "Learn-to-respond: Sequence-predictive recovery from sensor attacks in cyber-physical systems." 2023 IEEE Real-Time Systems Symposium (RTSS). IEEE, 2023.
[3] Wang, Zifan, et al. "Catch you if pay attention: Temporal sensor attack diagnosis using attention mechanisms for cyber-physical systems." 2023 IEEE Real-Time Systems Symposium (RTSS). IEEE, 2023.
[4] Zhang, Lin, Zifan Wang, and Fanxin Kong. "Optimal Checkpointing Strategy for Real-time Systems with Both Logical and Timing Correctness." ACM Transactions on Embedded Computing Systems (2023).
[5] Akowuah, Francis, Kenneth Fletcher, and Fanxin Kong. "Variable Window and Deadline-Aware Sensor Attack Detector for Automotive CPS." *2023 IEEE 26th International Symposium on Real-Time Distributed Computing (ISORC)*. IEEE, 2023.
[6] Zhang, Lin, Mengyu Liu, and Fanxin Kong. "AI-enabled Real-Time Sensor Attack Detection for Cyber-Physical Systems." *AI Embedded Assurance for Cyber Systems*. Cham: Springer International Publishing, 2023. 91-120.
[7] Liu, Mengyu, et al. "Fail-safe: Securing cyber-physical systems against hidden sensor attacks." 2022 IEEE Real-Time Systems Symposium (RTSS). IEEE, 2022.
[8] Zhang, Lin, et al. "Real-time attack-recovery for cyber-physical systems using linear-quadratic regulator." ACM Transactions on Embedded Computing Systems (TECS) 20.5s (2021): 1-24.

Broader Impact on Society

- Our project considerably contributes to maintaining proper CPS functions, safety and resilience, and therefore safeguards vital sectors in applications such as autonomous vehicles and power grids.

Broader Impact on Education

- Our solution can be actively integrated into courses, teaching students on CPS safety topics, as well as workforce training.

Quantified Potential Impact

- CPS application market is huge, reportedly 86 billion USD in 2022, with an annual growth rate of 7.6%. *
- Our techniques can improve resiliency of CPS applications against sensor attacks.

* Source: Futuremarketinsights. 2022. Cyber-physical Systems Market. https://www.futuremarketinsights.com/reports/cyber-physical-systems-market

Contact:
{lee, sokolsky}@seas.upenn.edu, fkong@nd.edu

Award ID#:
NSF CNS-2143274 and NSF CNS-2333980