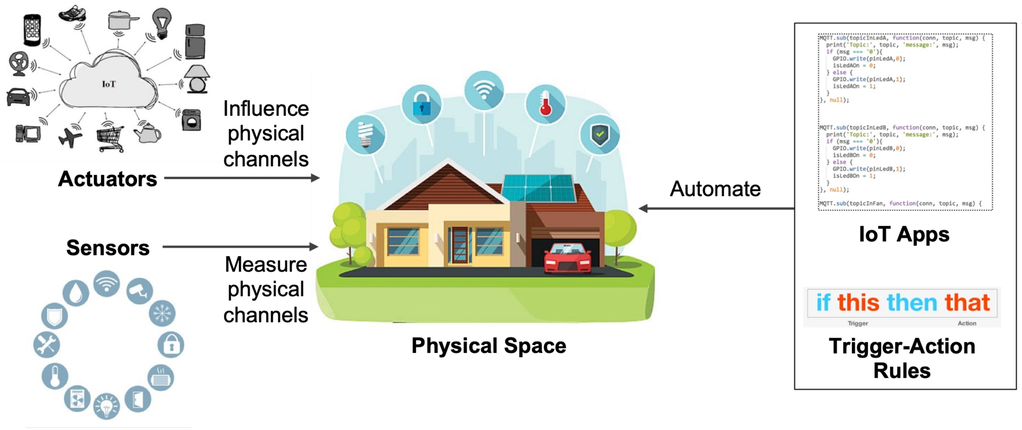
Discovering IoT Physical Channel Vulnerabilities

Muslum Ozgur Ozmen†, Xuansong Li‡, Andrew Chu*, Z. Berkay Celik†, Bardh Hoxha¶, Xiangyu Zhang†

†Purdue University, ‡Nanjing University Science and Technology, *University of Chicago, ¶Toyota Research Institute North America

Introduction

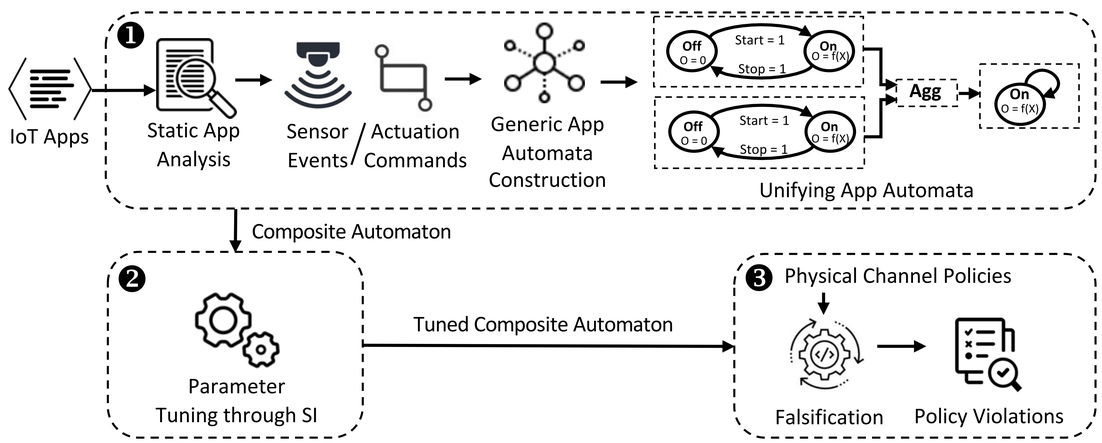


Motivation

When an actuation command is invoked, it influences a set of physical channels measured by sensors. The command then interacts with apps subscribed to those sensor events, invoking other commands. An adversary can exploit such physical interactions to indirectly control devices and cause unsafe states.

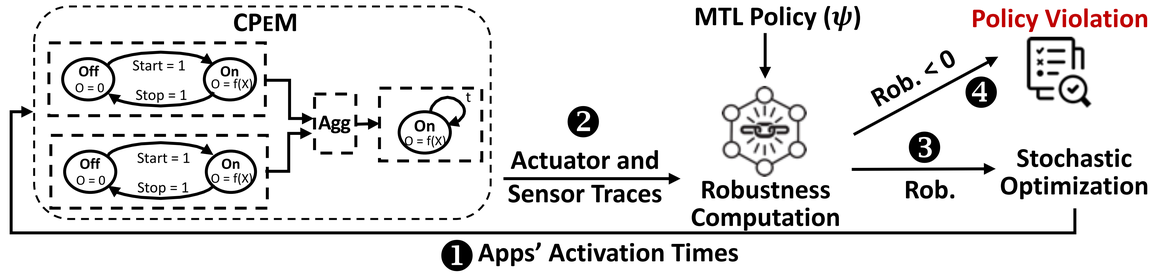
IoTSeer Overview

IoTSeer builds the joint physical behavior of IoT apps in hybrid automata and validates a set of security policies to discover physical interaction vulnerabilities.



❶ Translate sensor events and actuator commands of each app into a physical execution model (PeM) and unify PeMs to express composite physical execution of apps (CPeM).
❷ Collect device traces to define CPeM's execution parameters to maximize its fidelity.
❸ Validate if IoT apps conform to physical channel policies through falsification.

Optimization-guided Falsification

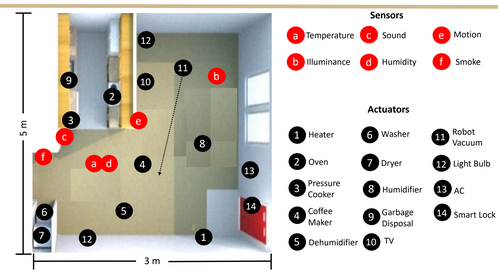


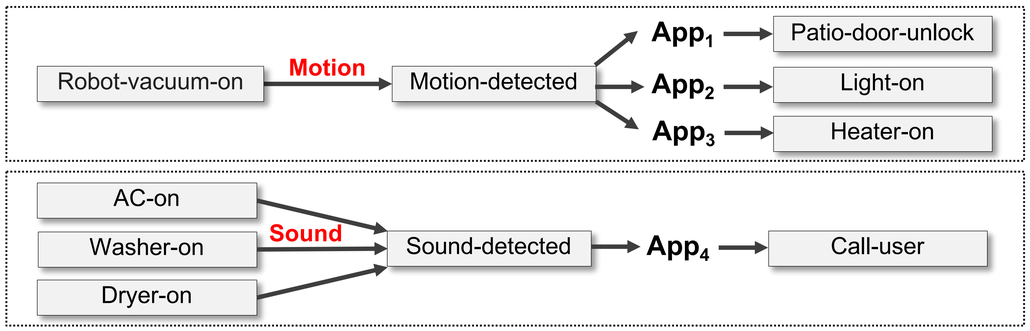
❶ Sample apps' activation times.
❷ Execute the CPeM and record actuator and sensor traces.
❸ Compute a robustness value that quantifies how close an MTL formula is to a policy violation and sample another input with the objective of minimizing the robustness.
❹ Terminate when the policy is violated, or a user-defined max number of iterations is met.

Evaluation Results

To evaluate IoTSeer, we deployed 6 sensors and 14 actuators in a real smart home.
We installed 39 apps from popular IoT platforms.

IoTSeer identified **16 unique policy violations** among different interacting apps, and we confirmed in the real home that all are true positives





Conclusions

We introduce IoTSeer, which identifies undesired states due to physical IoT app interactions by

- Translating app source code into its physical behavior
- Composition of interacting apps
- Physical interaction policy validation

Through this effort, we put forth an important step towards achieving the compositional safety and security of an IoT system's physical behavior

References

[1] Muslum Ozgur Ozmen, Xuansong Li, Andrew Chu, Z. Berkay Celik, Bardh Hoxha and Xiangyu Zhang. Discovering IoT Physical Channel Vulnerabilities. ACM Conference on Computer and Communications Security (ACM CCS) 2022.