Establishing Cryptographically Secure Communication Channels Between Batteryless and Battery-powered IoT Devices

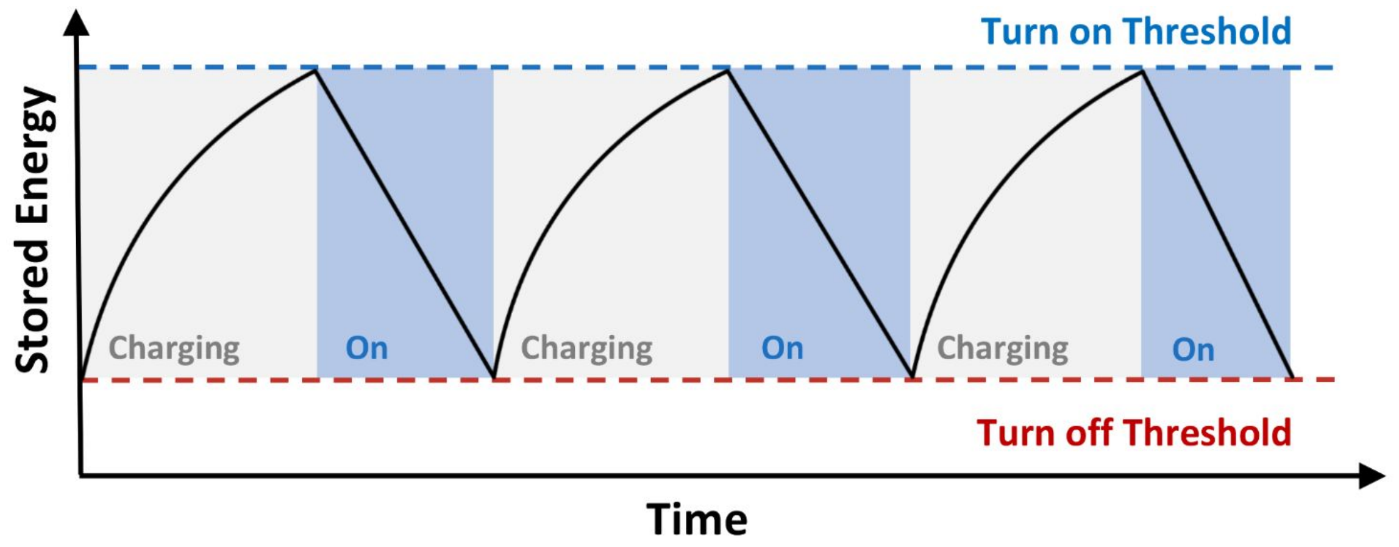
Hui Zhuang, Computer Science
Mentor: Muslum Ozgur Ozmen, Assistant Professor
School of Computing and Augmented Intelligence

Introduction

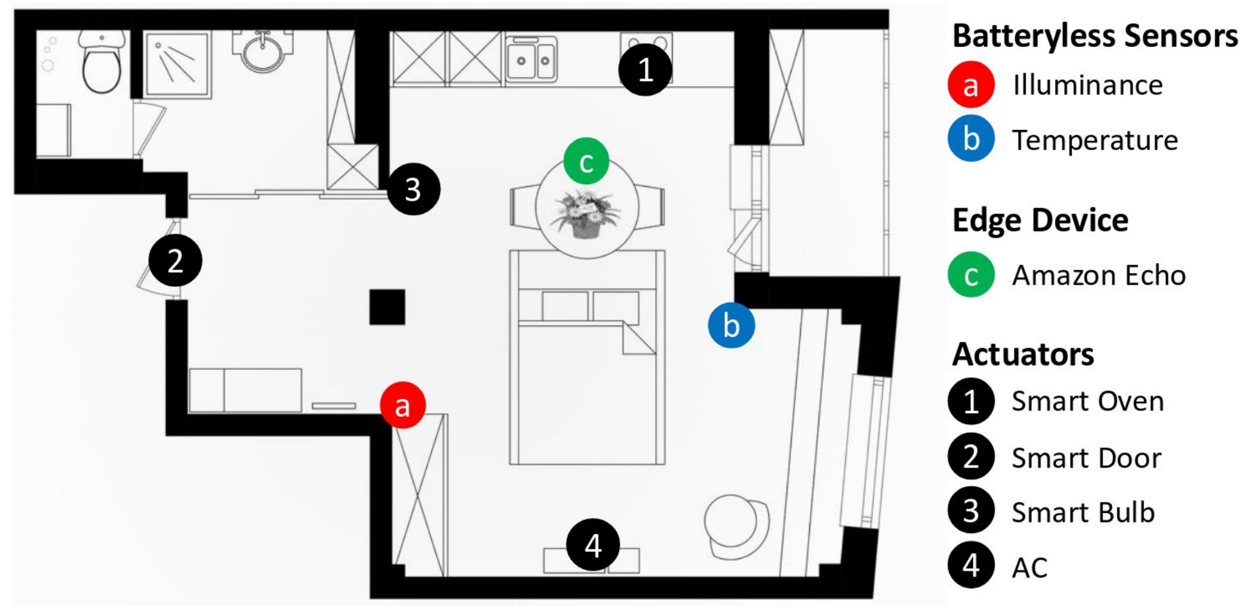
This research project aims to address the issue of maintaining the confidentiality and integrity of messages exchanged between batteryless and battery-powered IoT devices.

Motivation

Batteryless IoT devices are being integrated into IoT and cyber-physical systems (e.g. smart homes, industrial plants) at increasing rates [1]. Thus, these devices need a secure means of communication with other devices in the system.



An example of batteryless device execution.



An illustration of a smart home with batteryless sensors, an edge device, and smart actuators.

Methodology

Based on the inference that devices with like sensing modalities operating in the same environment will have strongly correlated sensor data we can use to derive shared cryptographic keys, we:

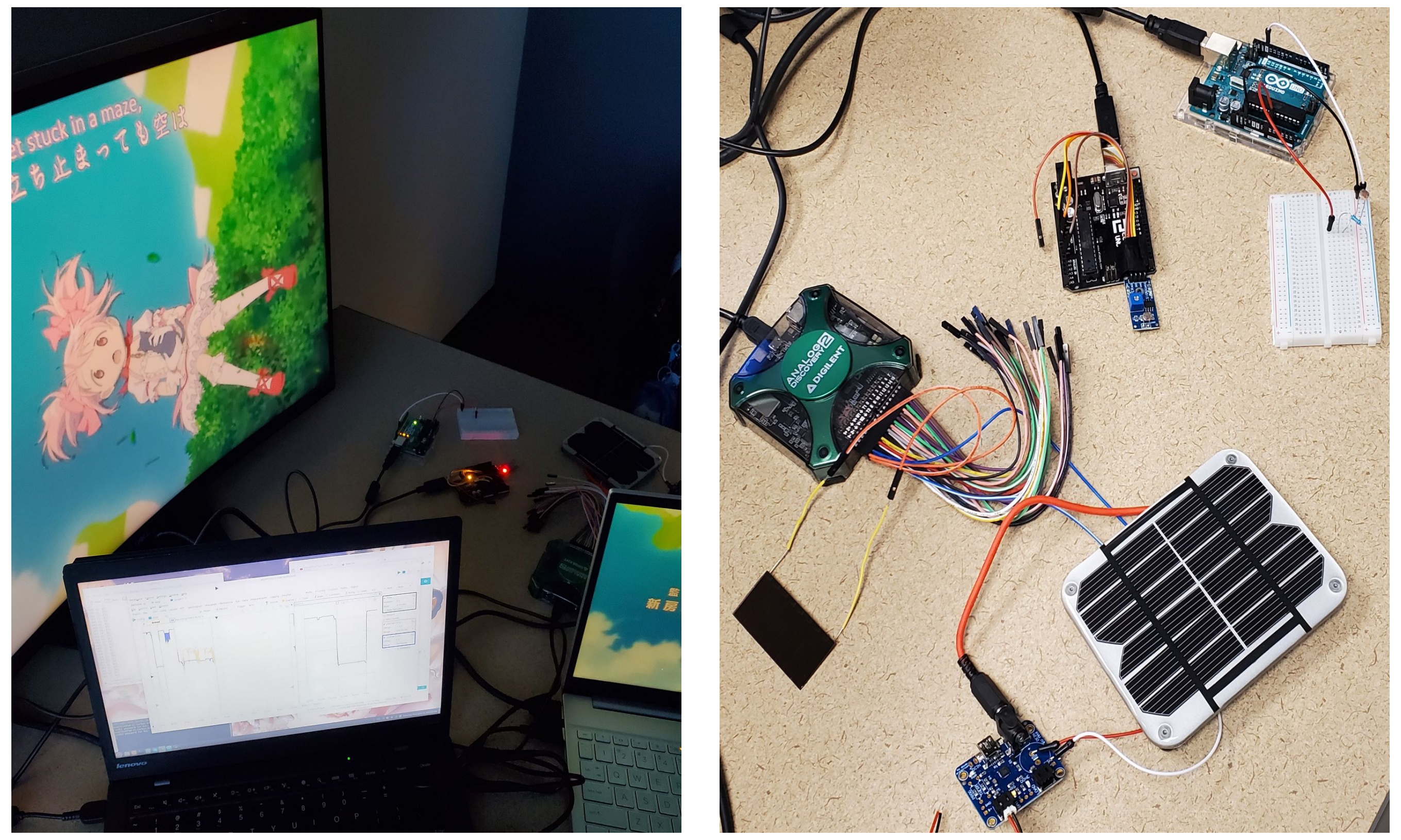
(1) Set up a testbed of two batteryless devices with solar panels and two battery-powered devices with illuminance sensors

(2) Recorded data from each device over time while varying surrounding light conditions

(3) Ran the NIST Adaptive Proportion Test to detect and discard predictable sections of data

(4) Quantized data in intervals from among the remaining data to use as input to the key exchange protocol

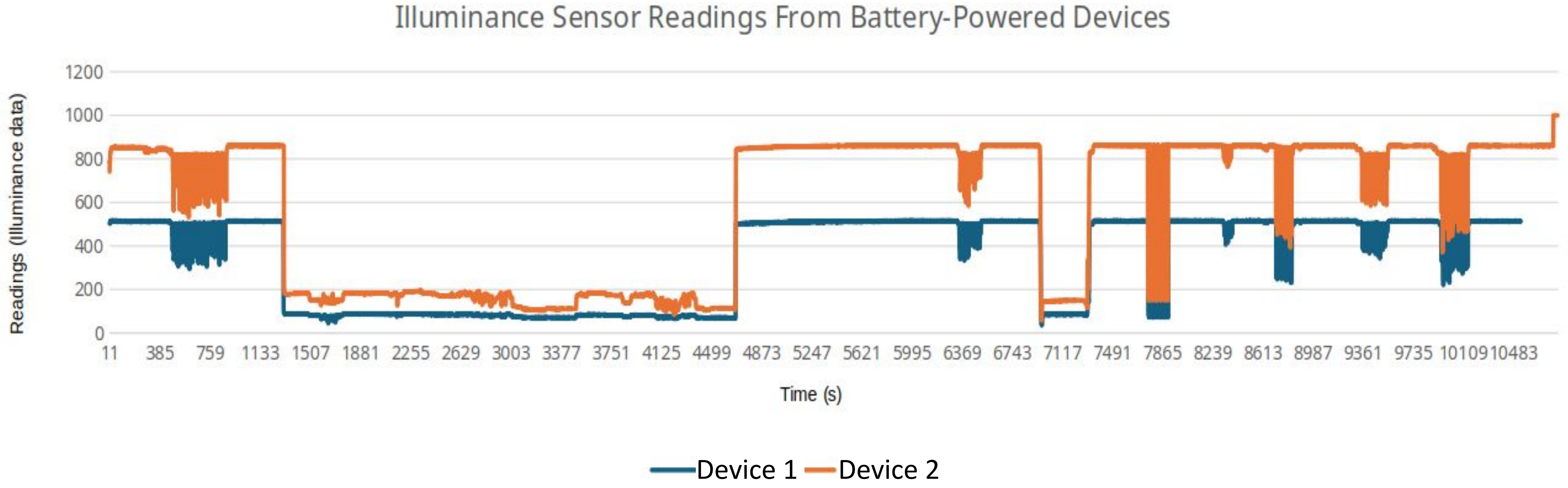
Experimental Setup



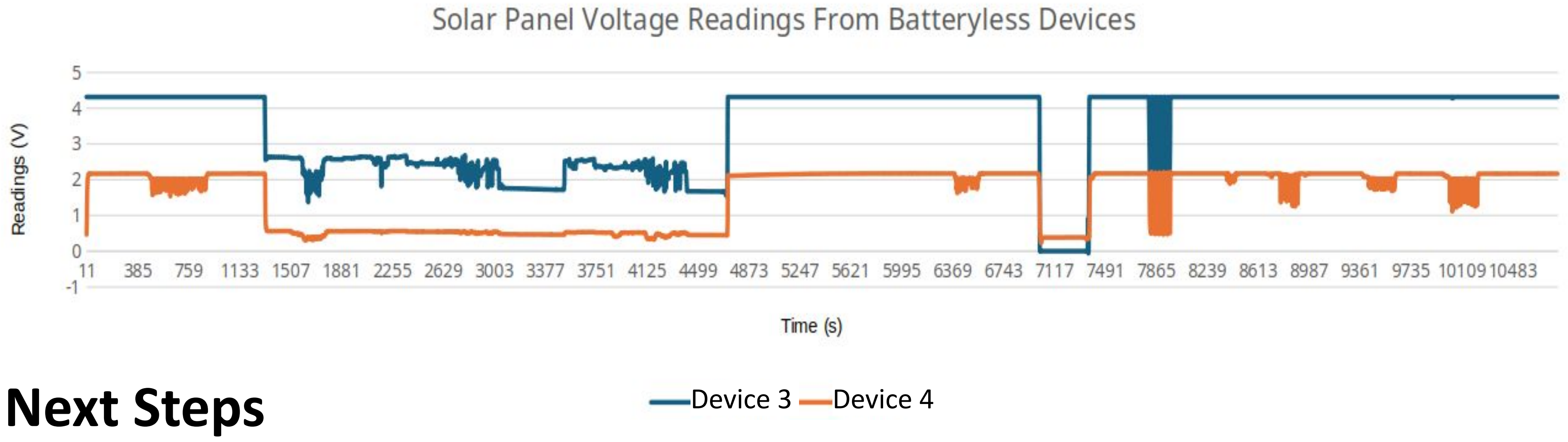
(Left) Playing videos in the dark to affect lighting conditions.

(Right) The devices laid out on the table.

Preliminary Results



The sensor data are strongly correlated, confirming our initial inference.



Moreover, we were able to create 5 precise matches from raw data in the window during which we played videos in the dark.

Next Steps

The next steps involve using the derived bitstrings as input to our key exchange protocol (GPAKE) to demonstrate that our method can be used to establish secure communication. We are also writing a paper to submit to conferences.

[1] Thea U. Kjeldsmark*, Hui Zhuang*, Habiba Farrukh, and Muslum Ozgur Ozmen. 2025. Intermittent Power, Continuous Protection: Security and Privacy for Batteryless Devices in IoT. In Proceedings of Sensors S&P.