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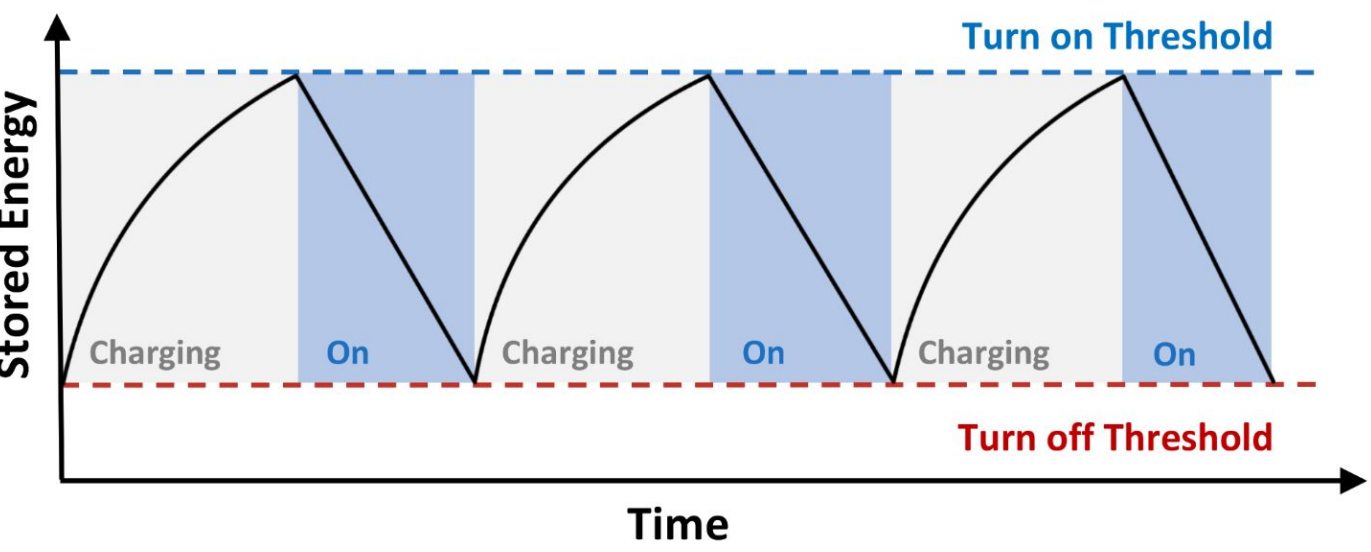
An example of batteryless device execution.
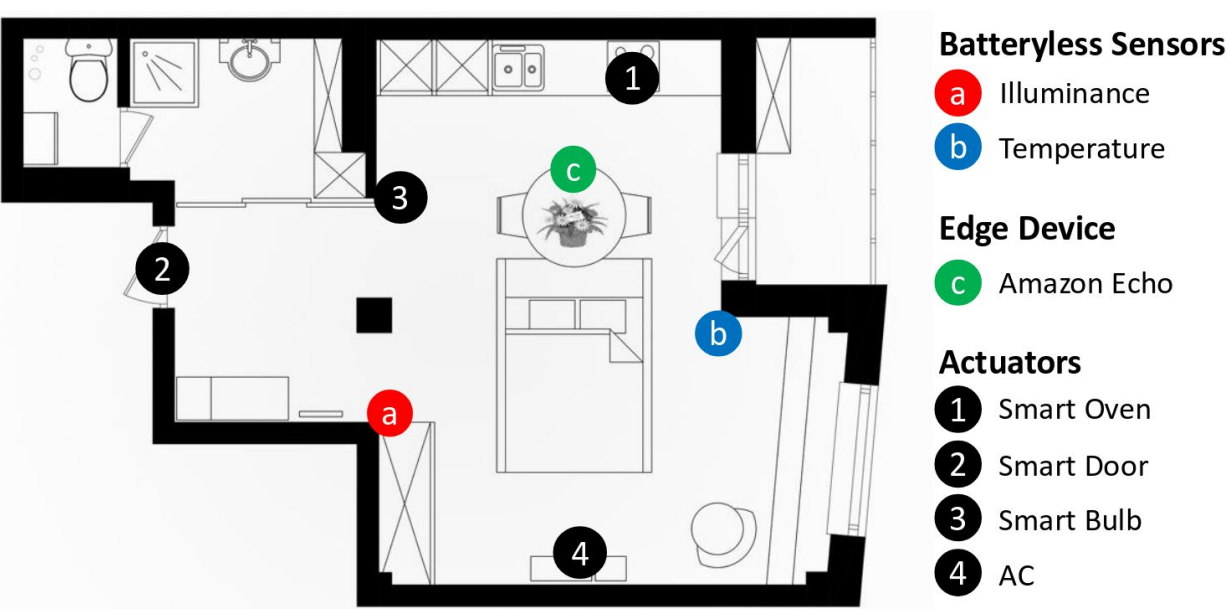
An illustration of a smart home with batteryless sensors, an edge device, and smart actuators.

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

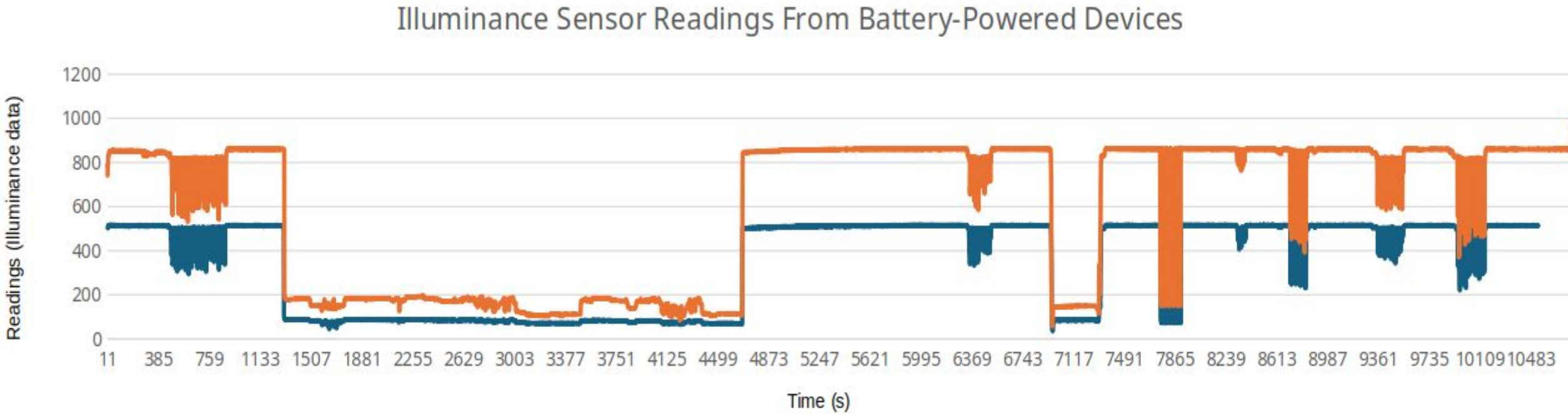(3) Quantized data from selected intervals to confirm whether it is possible to derive keys
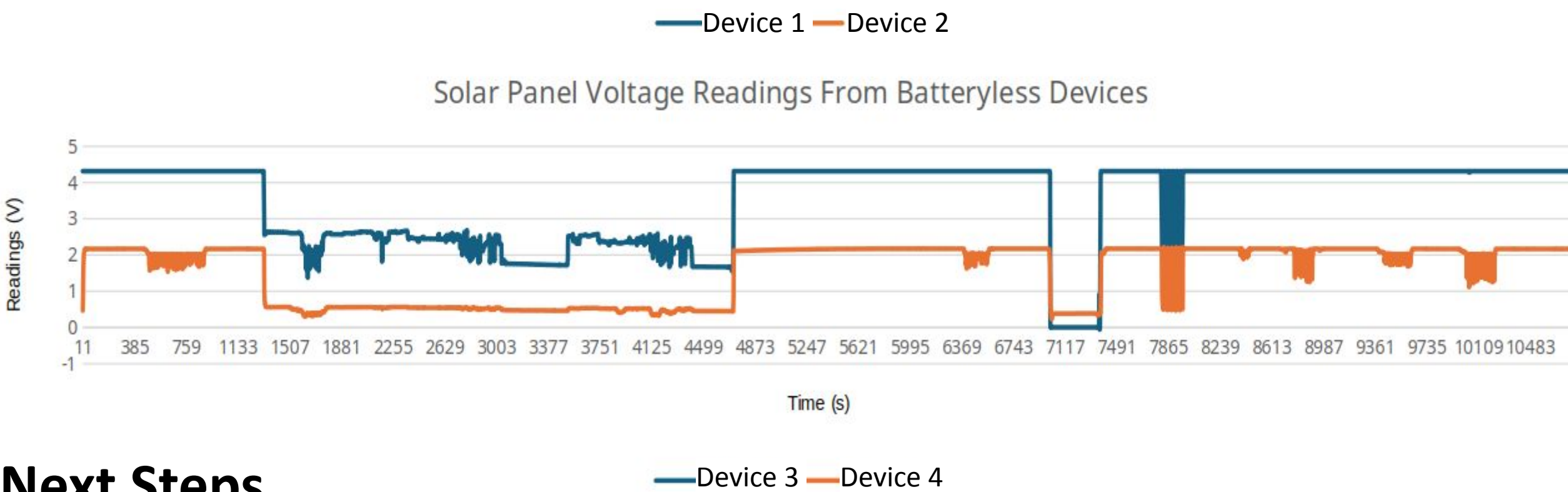
Experimental Setup
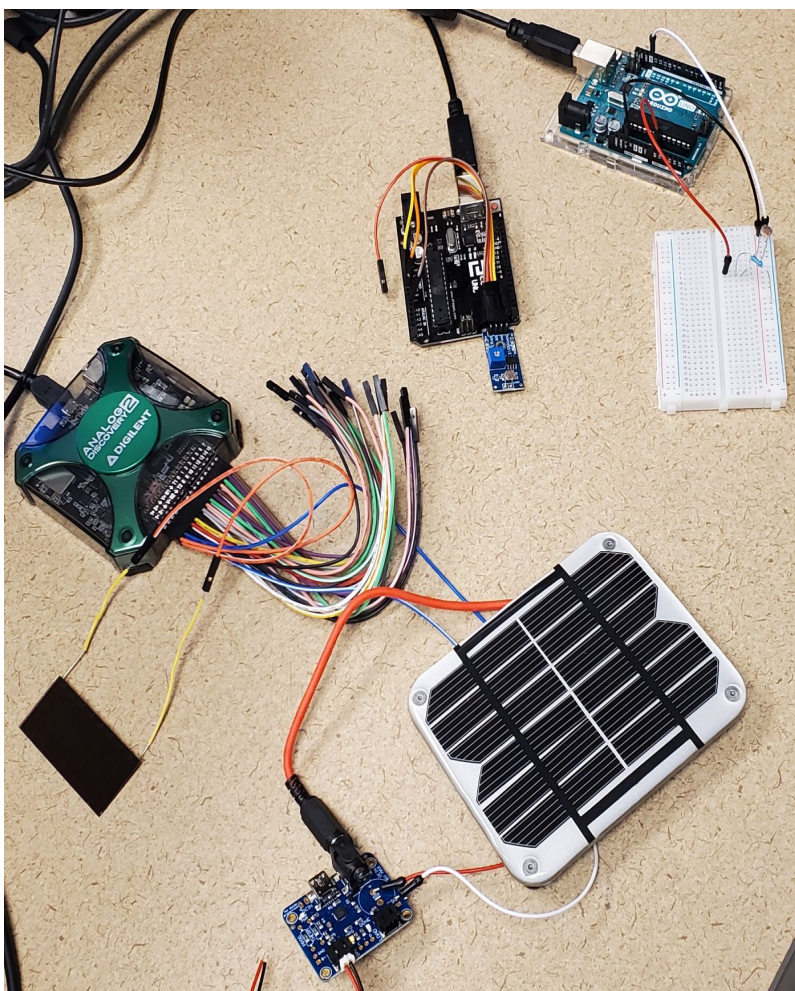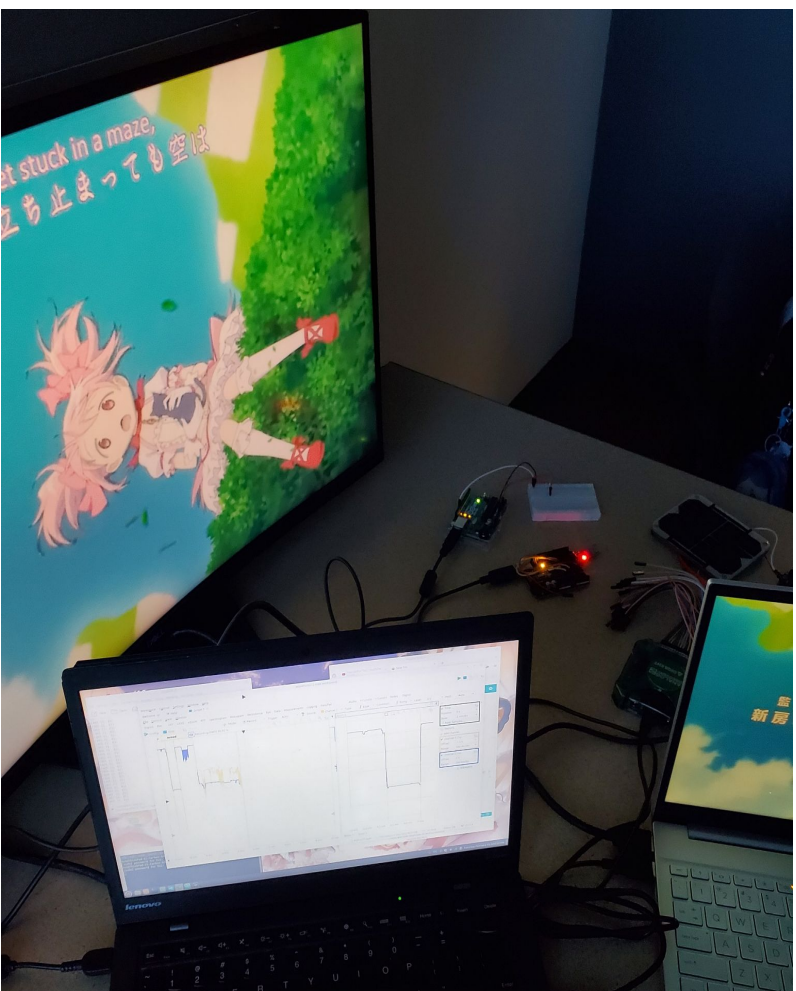
(Left) Playing videos in the dark to affect lighting conditions.

(Right) The devices laid out on the table.

Preliminary Results

Illuminance Sensor Readings From Battery-Powered Devices

The sensor data are strongly correlated, and it is indeed possible to derive keys.

Solar Panel Voltage Readings From Batteryless Devices

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 refining the key establishment process to exclude low entropy bits from sensor data, ensuring that the derived keys are highly improbable for an adversary to guess.

[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.

FURI

Ira A. Fulton Schools of Engineering
Arizona State University