2023 - ESS - **64D-189** - Secure Pairing of Energy Harvesting Devices - bandyopr@purdue.edu - Rwitam Bandyopadhyay

CERIAS

The Center for Education and Research in Information Assurance and Security

# Secure Pairing of Energy Harvesting Devices

**Rwitam Bandyopadhyay, Satyam Sachan, Muslum Ozgur Ozmen, Habiba Farrukh, Z. Berkay Celik**

{bandyopr, ssachan, mozmen, hfarrukh, zcelik}@purdue.edu

## Introduction

- Context-based pairing allows devices to pair without human-device interaction by using environmental cues.
- Existing work on context-based pairing focuses on traditional IoT devices with batteries, which capture all ambient changes.
- We propose a system that pairs energy harvesting devices using at least one common sensing modality.

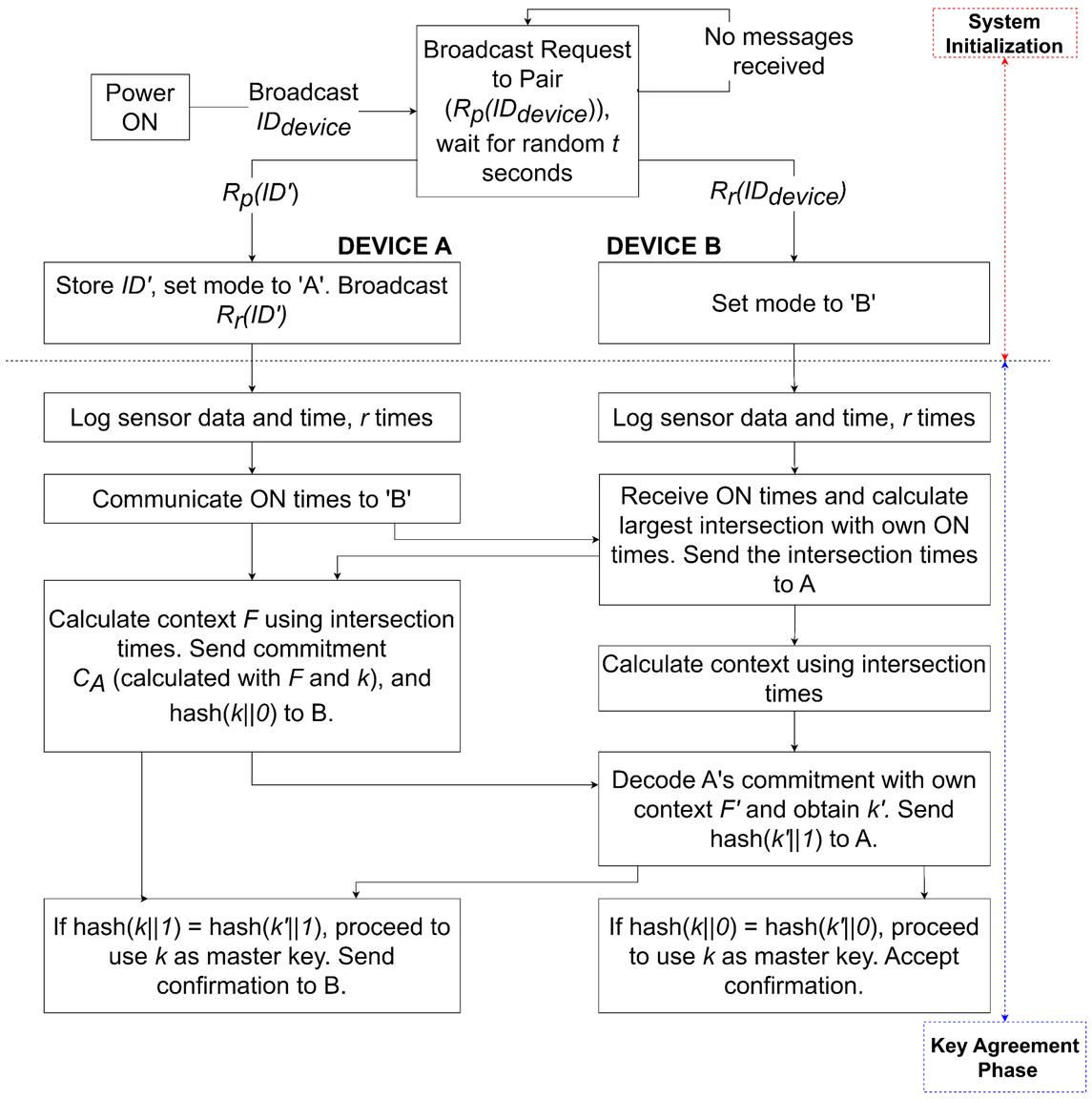
## Motivation

- As the number of deployed IoT devices increase, the effort required for Human-in-the-Loop based pairing becomes significant.
- Public Key Infrastructure for pairing may not be feasible in resource-constrained, low powered IoT devices.
- Prior works have focused on devices that are equipped with the same sensors [1] and extended them to heterogeneous sensor modalities by leveraging inter-event timings for pairing [2,3]. However, secure pairing methods that leverage the devices' energy harvesting mechanisms have not been investigated.

## Methodology

- Our system works by probing the voltage levels of the energy harvesting devices (solar energy in our experiments).
- Our system extracts an evidence of co-location from the voltage levels of the device harvesters.
- It then leverages fuzzy commitment schemes to derive a shared secret between devices from the evidences.

## Protocol Overview




## Experiments

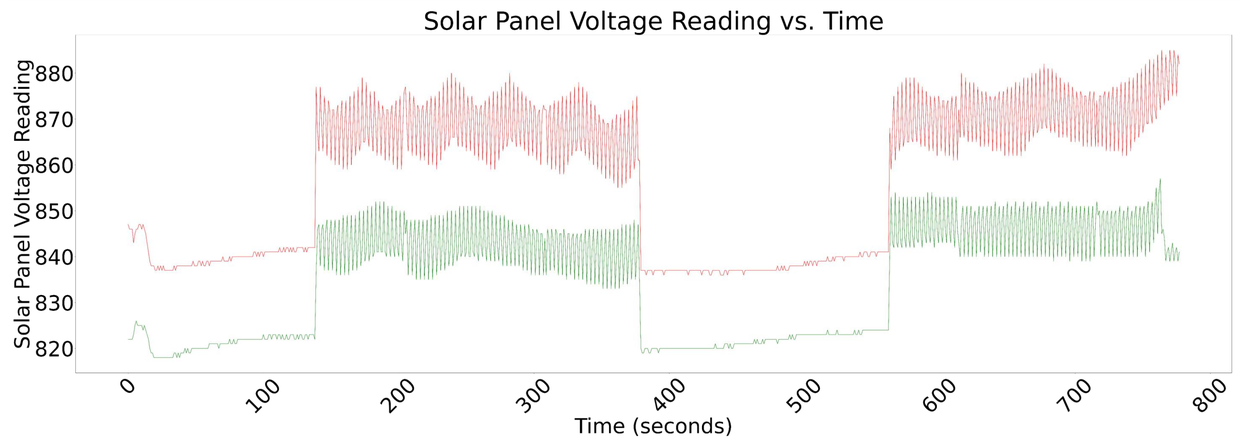



**Figure 1: Uninterrupted Data Capture**

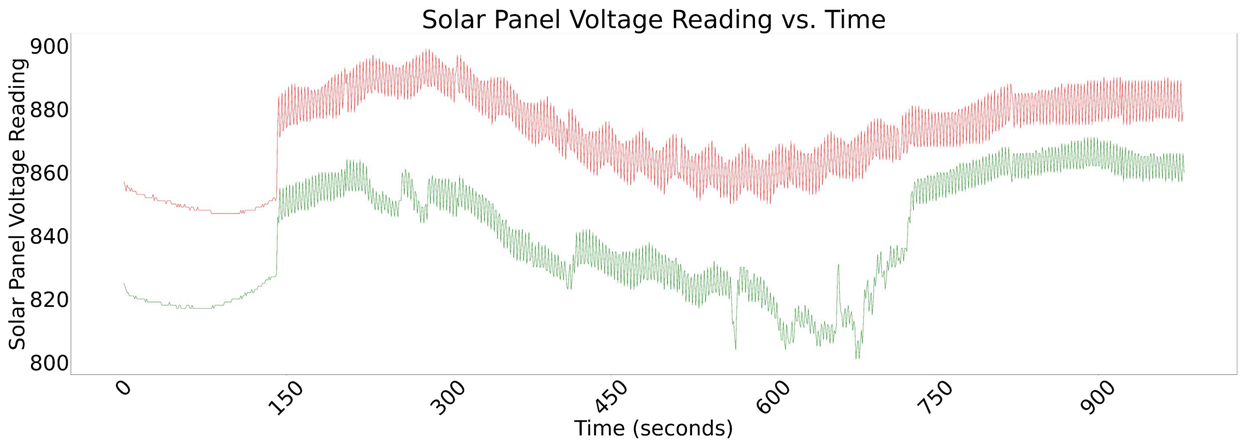



**Figure 2: Data Capture With Minor Disturbances**

## Experimental Results

| Setup Number | 1 | 2 | 3 |
|---|---|---|---|
| Device A | 0106090700040af6 | f8f8f6f9f9f80a | 00040a0803010205 08f6 |
| Device B | 0207090702060af6 | f706f7f8f8f60a | 0004070401000007 0af6 |
| Context Change Percentage | 25% | 50% | 35% |
| Key Exchanged | Yes | No | No |

## Limitations and Future Advancements

- Empirically defined system parameters: System parameters that determine the key size, amount of data collected, and the number of error-correcting codes require extensive experimentation.
- Sensor calibration: There may be deployment environments where devices may not be able to appropriately measure “small” fluctuations. In future work, we will analyze the suitability of the system in various IoT deployments.
- Implementation of the complete protocol: The current implementation does not include any communication via BLE or Wi-Fi. We will finalize the implementation of the complete protocol to observe its performance in real-life deployment.

## References & Related Work

1. Han, J., Chung, A. J., Sinha, M. K., Harishankar, M., Pan, S., Noh, H. Y., Zhang, P., and Tague, P. *Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing Using Different Sensor Types*. In 2018 IEEE Symposium on Security and Privacy (SP).
2. Miettinen, M., Asokan, N., Nguyen, T. D., Sadeghi, A.-R., and Sobhani, M. *Context-based zero-interaction pairing and key evolution for advanced personal devices*. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (New York, NY, USA, 2014), CCS ’14, Association for Computing Machinery.
3. Habiba Farrukh, Muslum Ozgur Ozmen, Faik Kerem Ors, and Z. Berkay Celik, *One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices.* In 2023 IEEE Symposium on Security and Privacy (SP)

PURDUE UNIVERSITY

CERIAS