RNYF

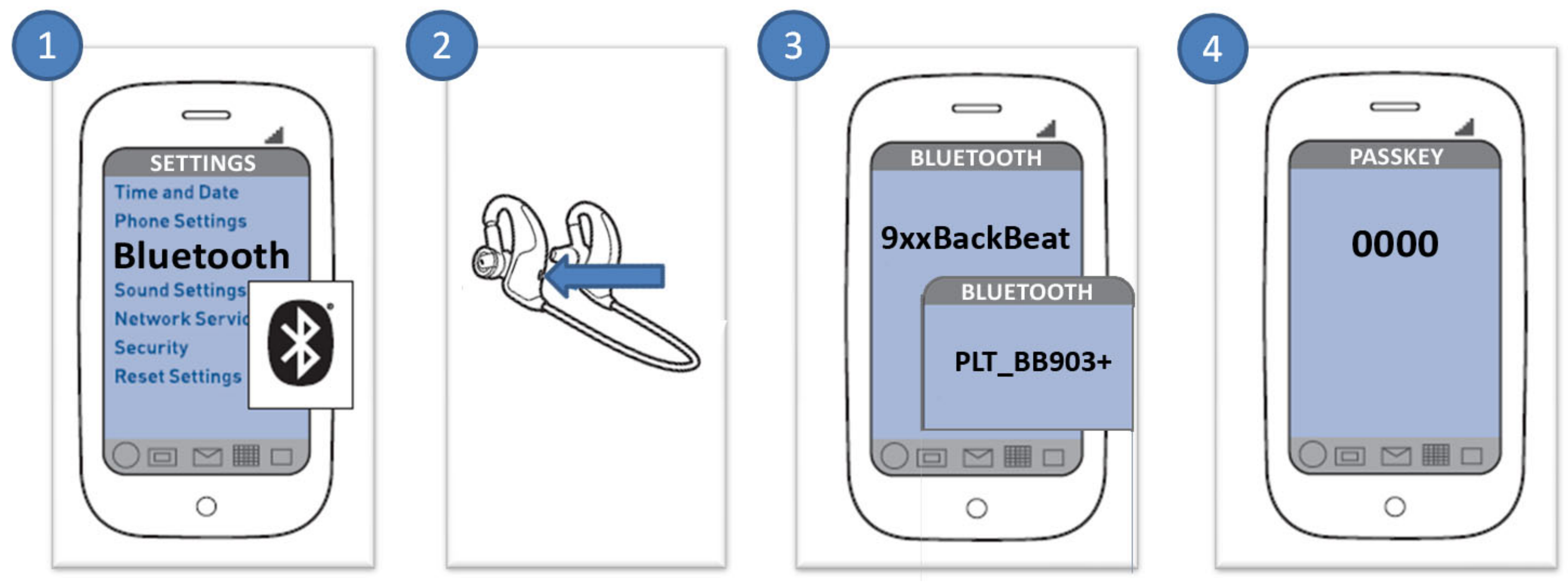
DESIGN AUTOMATION CONFERENCE 56
FROM CHIPS TO SYSTEMS – LEARN TODAY, CREATE TOMORROW

Secure Pairing Methods for Ubiquitous IoT Devices

Kyuin Lee, Prof. Younghyun Kim, University of Wisconsin–Madison

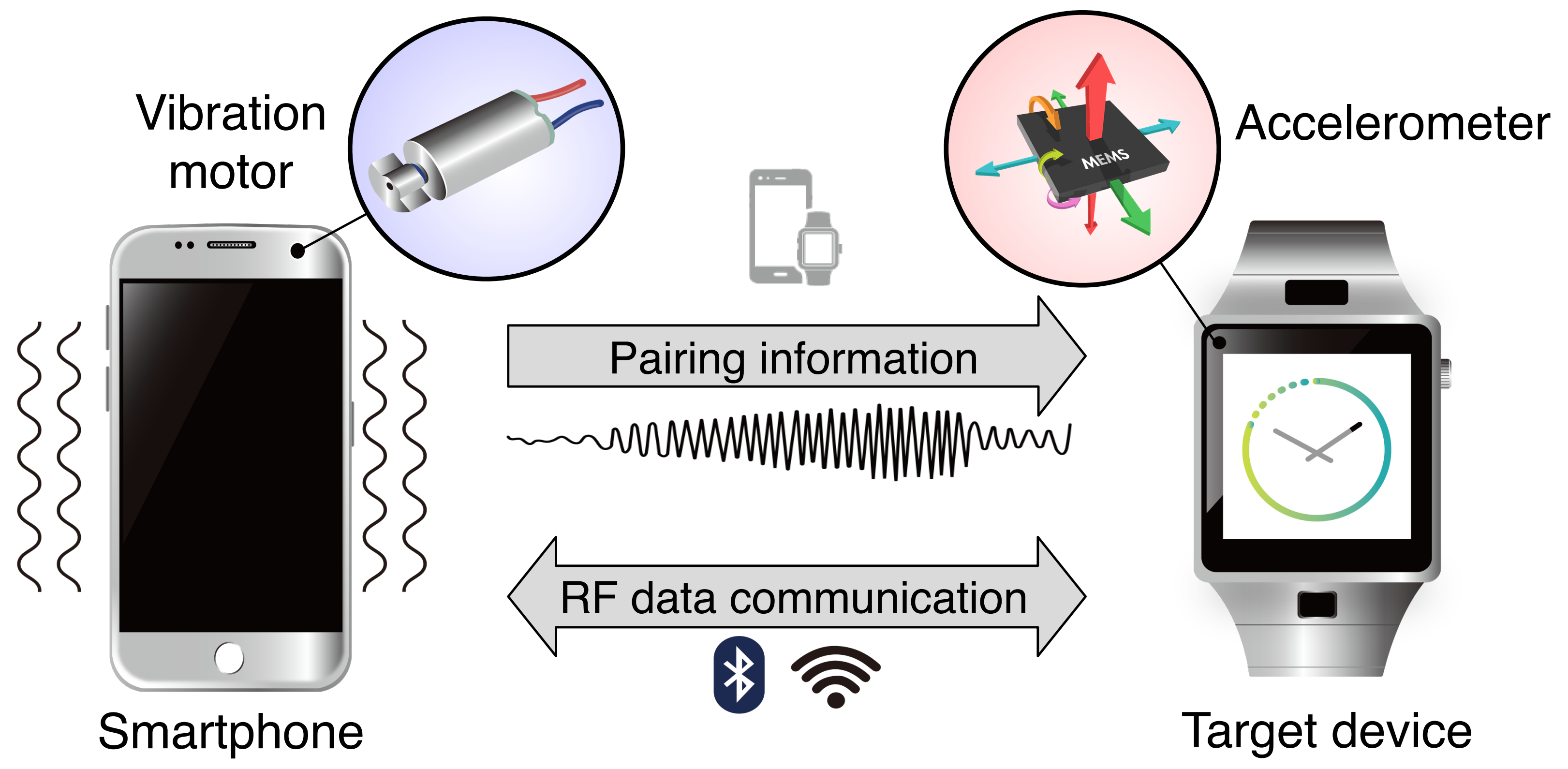
1. Motivation

- Proliferation of IoT devices challenges in **securely** and **conveniently** connecting devices with limited user interfaces.
- Discovering and bootstrapping a initial wireless connection **(pairing)** is **cumbersome** and **requires expensive input abilities**.
- Example of pairing procedure between mobile devices (Bluetooth):



- Stationary IoT devices (i.e., Alexa, Nest) delegates input abilities to mobile application, which further complicates pairing procedures.
- As devices become smaller and more ubiquitous, it is unreasonable to utilize current pairing paradigm for mobile and stationary devices.

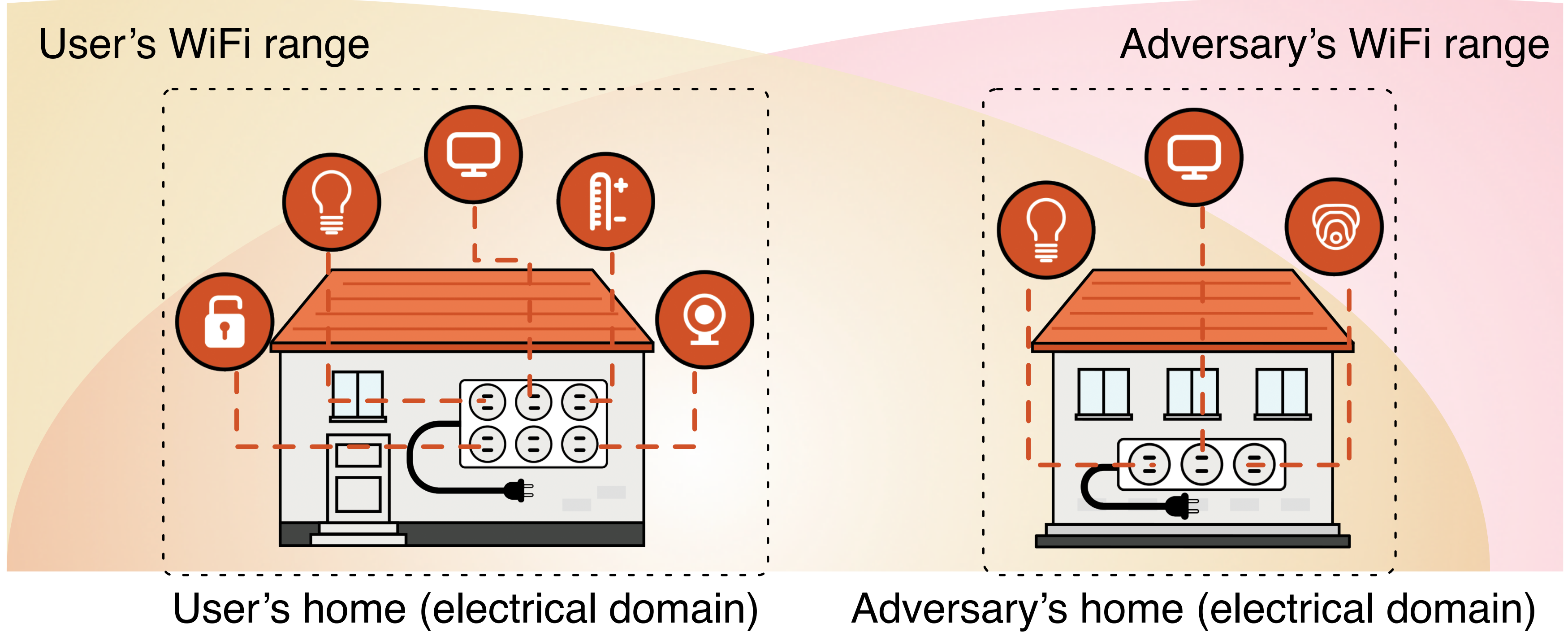
2. SyncVibe for mobile devices



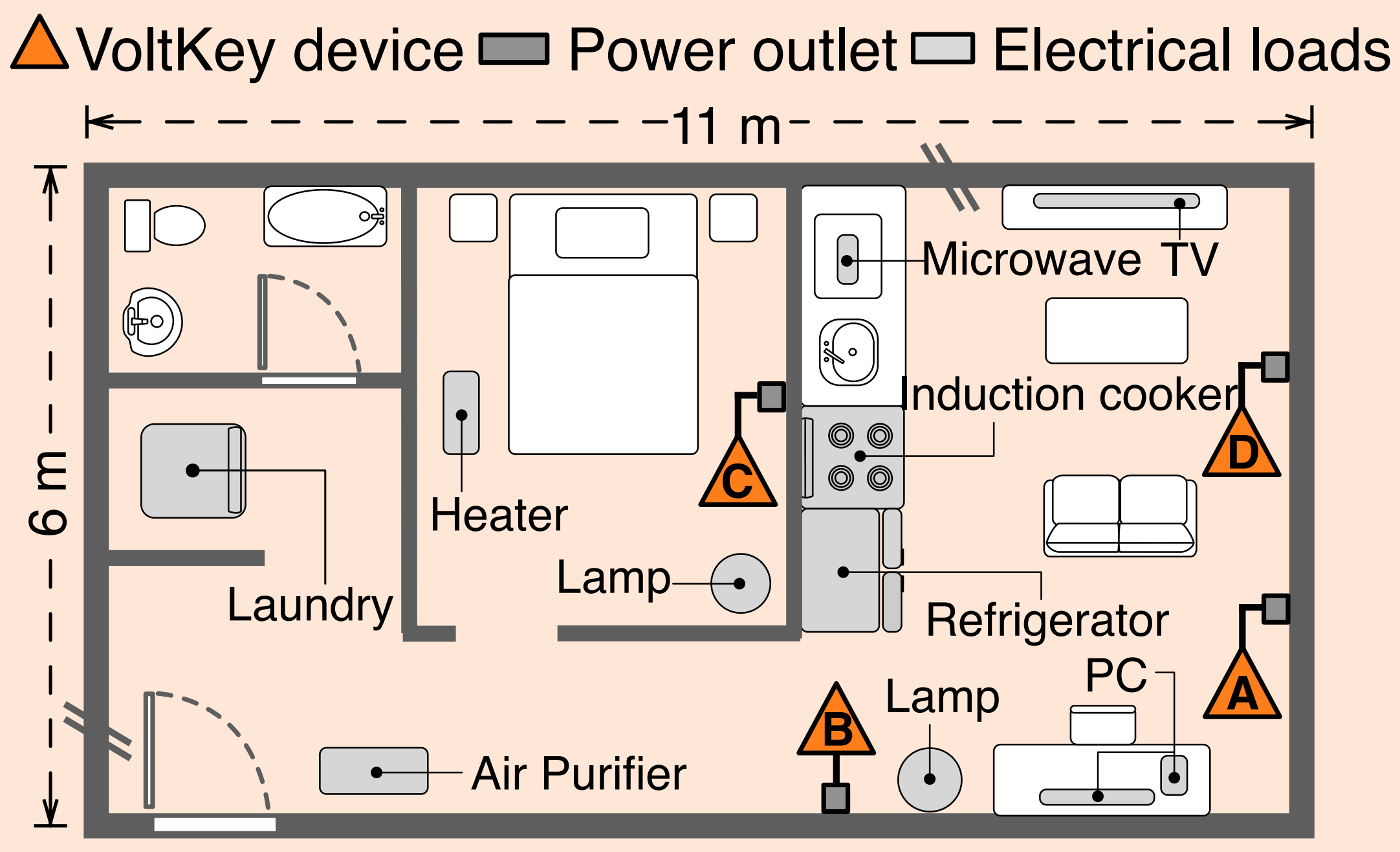
- SyncVibe [1] uses **vibration motor** and **accelerometer** to transmit and receive **pairing information**.
- By keeping two devices in direct contact, wireless connection is established.
- Vibration is proximity channel which makes eavesdropping more difficult than RF channel.
- Maximizes bit transfer rate with *vibration clock recovery*, which extracts timing information from vibration waveform of data bits.
- Evaluation of SyncVibe transferring 150-bit pairing key :

Vibration period	Pairing success rate	Bit-error rate	Pairing time
40 ms	92%	0.95%	6.74 s
50 ms	97%	0.61%	7.87 s
60 ms	98%	0.67%	9.34 s

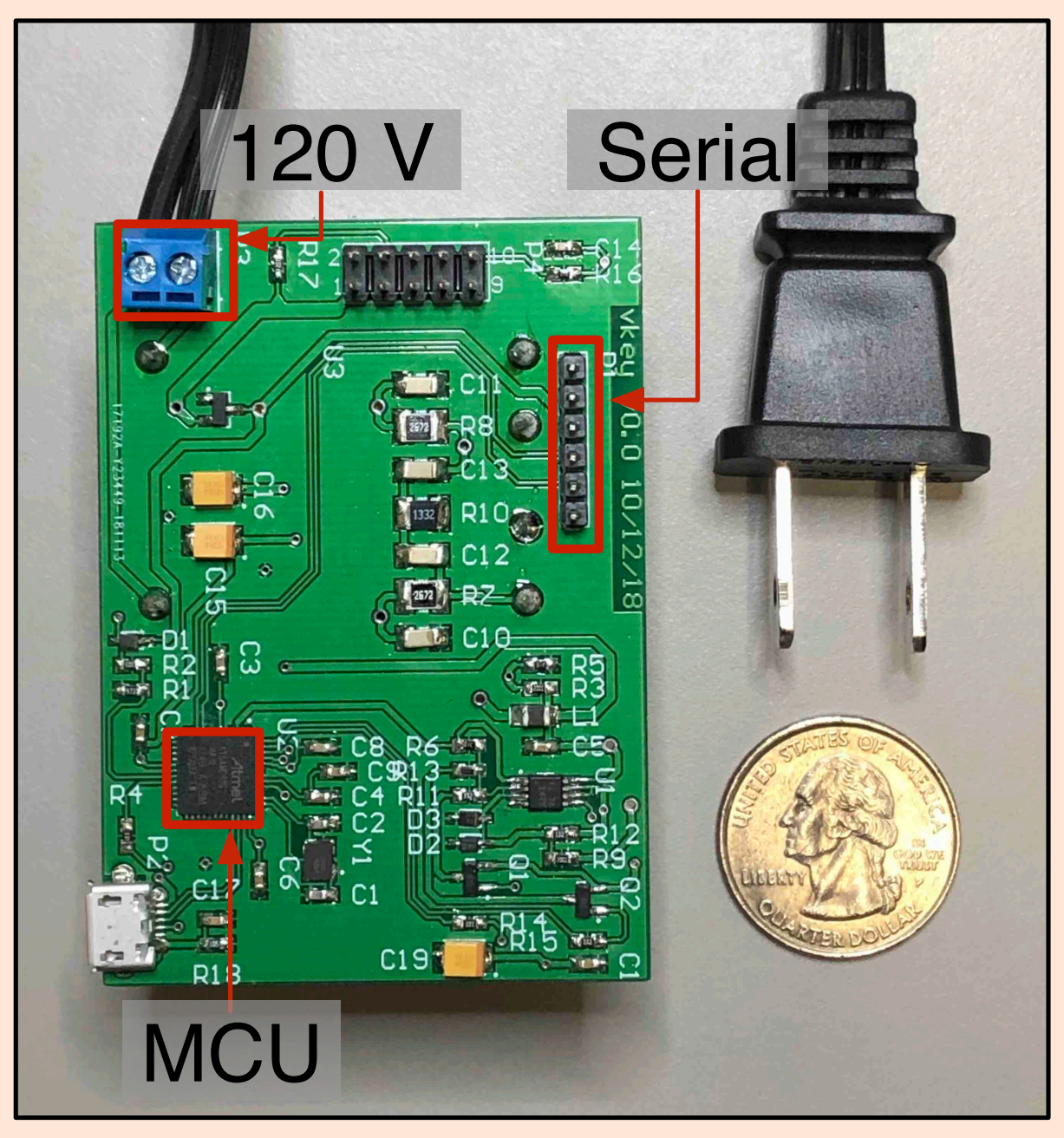
3. VoltKey for stationary devices


User's WiFi range
Adversary's WiFi range
User's home (electrical domain)
Adversary's home (electrical domain)

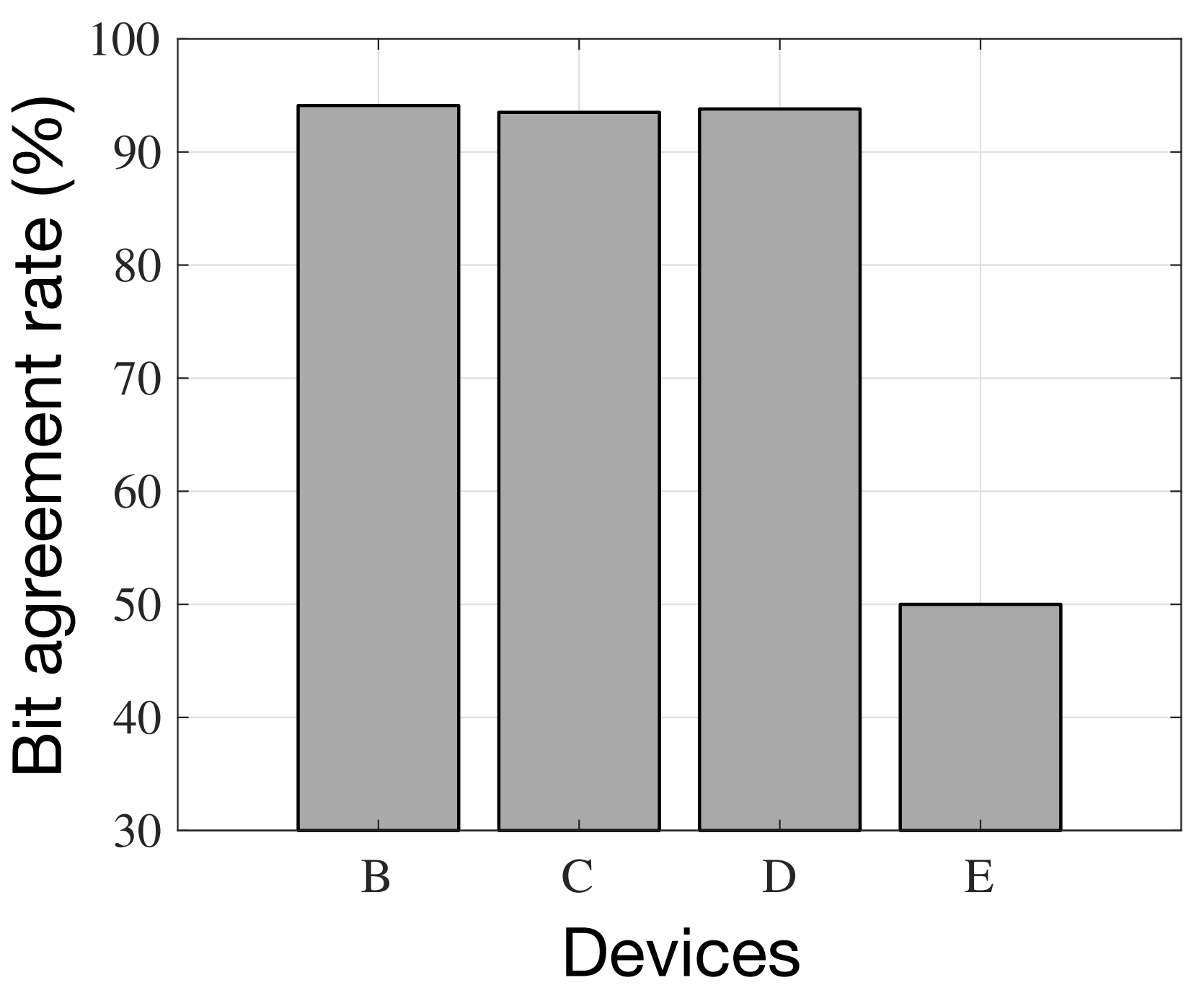
- VoltKey [2] **transparently** and **continuously** generates **secret keys** for colocated devices, leveraging spatiotemporally unique noise contexts observed in commercial power line.
- Power line noise is dependent on number and type of surrounding electrical devices.
- Simple key extraction algorithm suitable for low-cost hardware for scalable deployment.
- Evaluation in one bedroom apartment with periodic establishment of 128-bit keys every 10 minutes for six days:

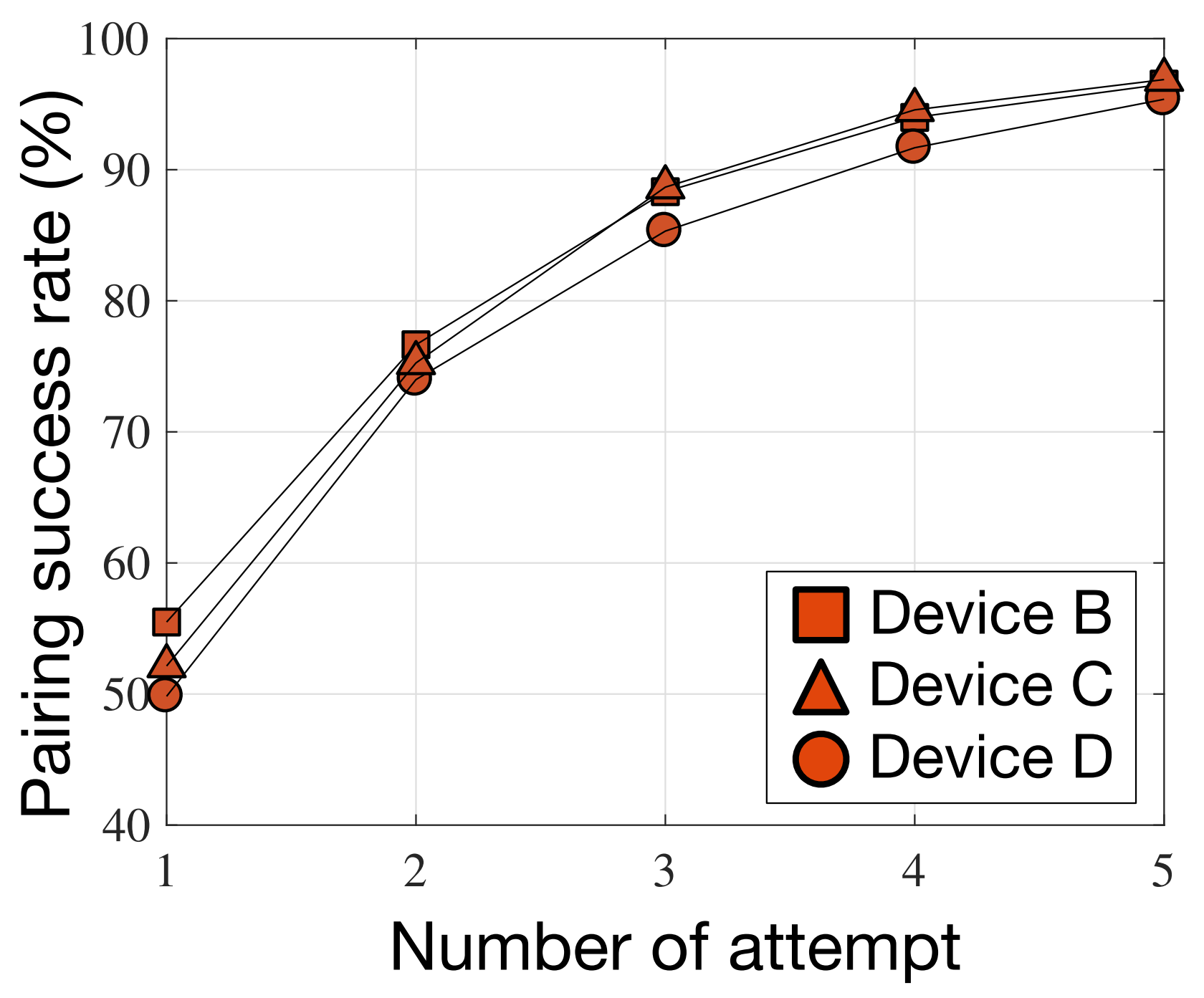


One bedroom apartment



VoltKey Hardware





4. Research interests

- **Security of IoT**: researching usable and secure HW/SW system design for various kinds of emerging IoT devices.
- **Embedded Cyber Physical Systems**: designing and implementing practical embedded applications leveraging various surrounding contextual information.

- [1] K. Lee, V. Raghunathan, A. Raghunathan and Y. Kim, "SyncVibe: Fast and Secure Device Pairing through Physical Vibration on Commodity Smartphones," *2018 IEEE 36th International Conference on Computer Design (ICCD)*, Orlando, FL, USA, 2018, pp. 234-241.
- [2] K. Lee, N. Klingensmith, S. Banerjee and Y. Kim, "VoltKey: Continuous Secret Key Generation based on Power Line Noise for Zero-Involvement Pairing and Authentication," *Under Review*