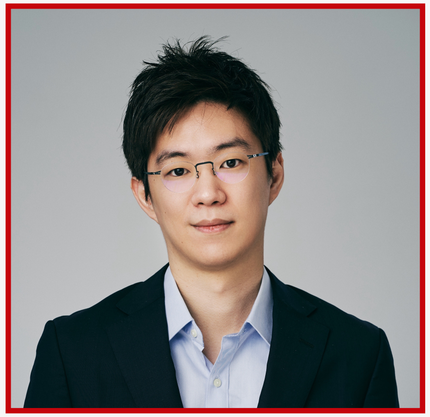
The 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '22)

Kyuin Lee University of Houston
Yucheng Yang University of Wisconsin–Madison
Omkar Prabhune University of Wisconsin–Madison
Aishwarya Lekshmi Chithra University of Wisconsin–Madison
Jack West University of Wisconsin–Madison
Kassem Fawaz University of Wisconsin–Madison
Neil Klingensmith Loyola University Chicago
Suman Banerjee University of Wisconsin–Madison
Younghyun Kim University of Wisconsin–Madison



AeroKey: Using Ambient Electromagnetic Radiation for Secure and Usable Wireless Device Authentication

September 13, 2022

WISCONSIN UNIVERSITY OF WISCONSIN–MADISON

LOYOLA UNIVERSITY CHICAGO
Preparing people to lead extraordinary lives

Explosive Growth of IoT

2010
12 billion

x 3

2020
35 billion

x 4

2030
125 billion

https://www.csoonline.com/article/2942596

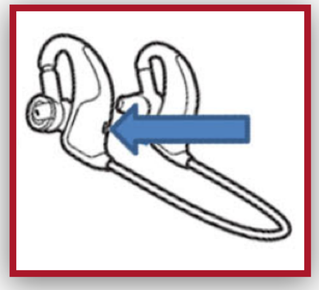
Challenges in Pervasive Computing

Managing secure wireless connections between devices are labor-intensive

https://www.cnet.com/tech/mobile/new-apple-watch-iphone-how-to-unpair-pair/
https://datastorageasean.com/blogs/building-secure-byod-environment-workspace-one

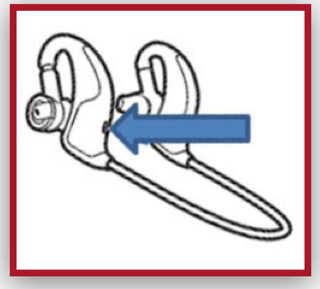
Typical Device Authentication Scenario

Open Bluetooth settings



Pairing mode

Select device



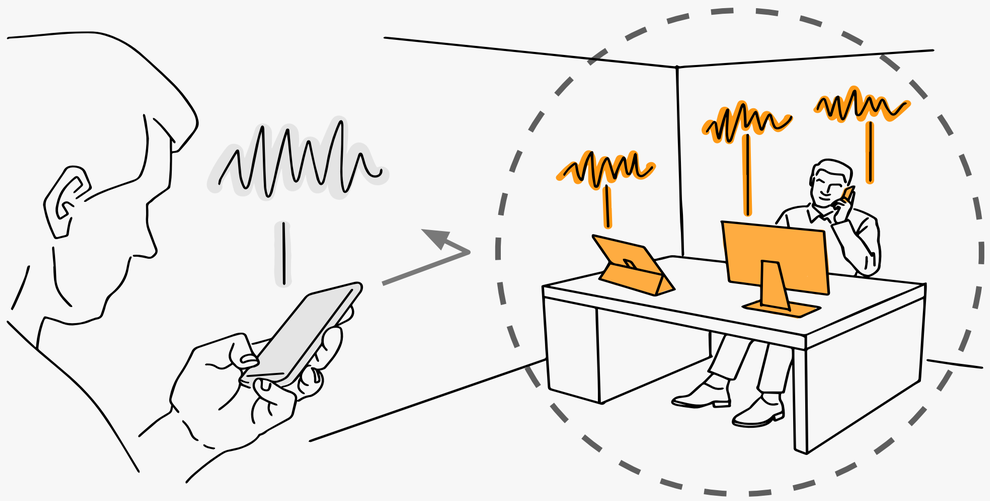
Listen for authentication key

Enter the key

Time-consuming (27 s), and not secure

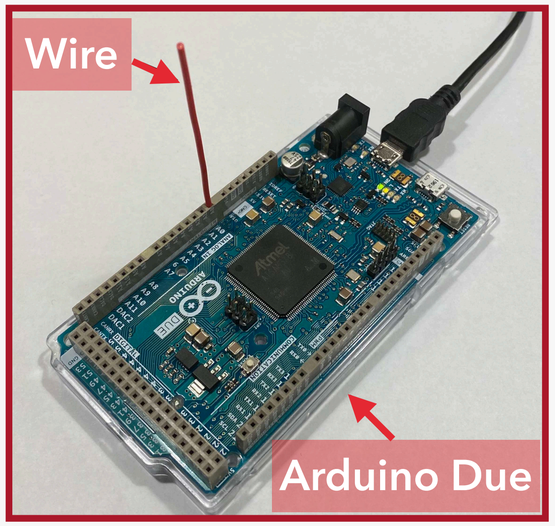
Ersin Uzun, Kristiina Karvonen, and N. Asokan. 2007. Usability Analysis of Secure Pairing Methods. InFinancial Cryptography and DataSecurity. 307–324

AeroKey



Adversary

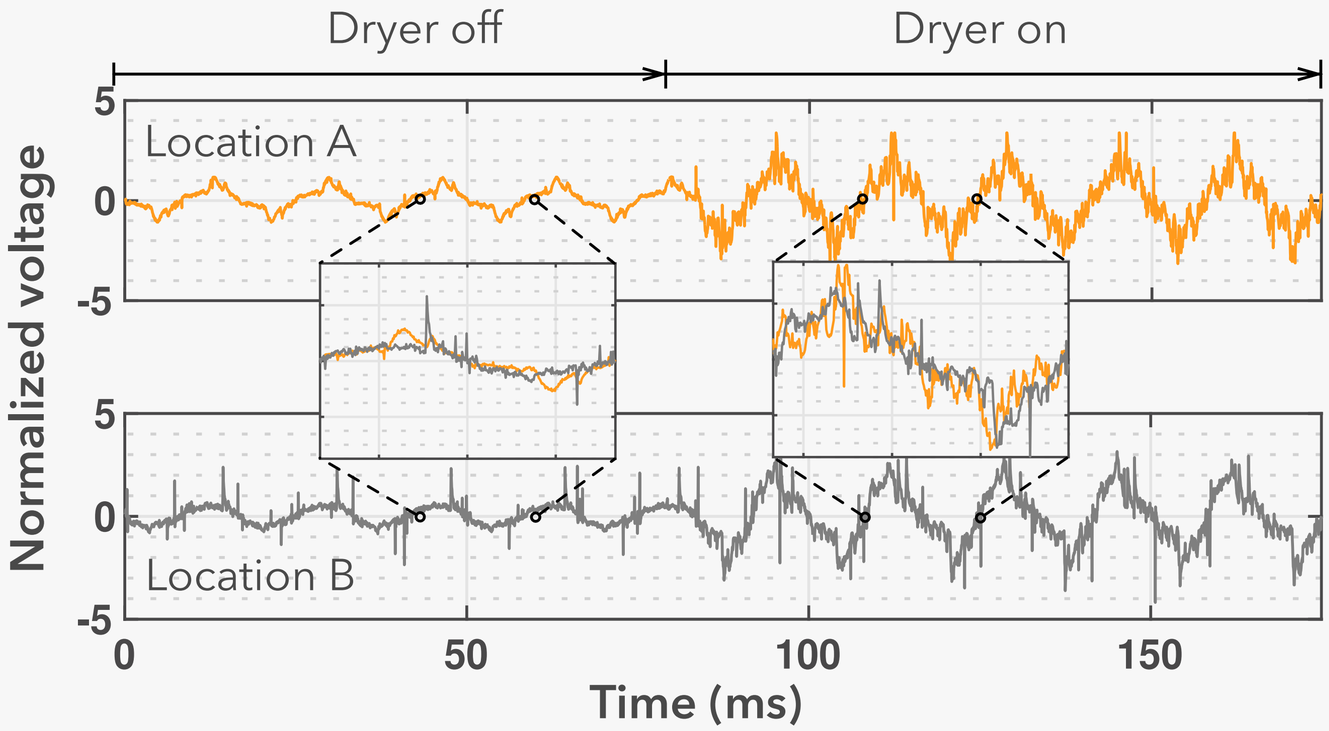
Personal authenticated region

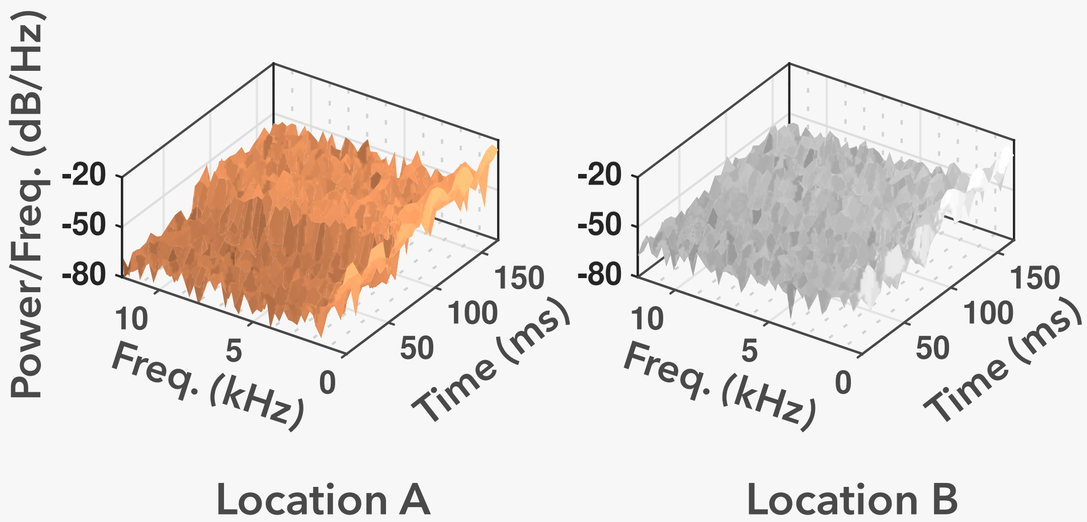


AeroKey hardware

- **Co-located devices periodically generate identical authentication key based on ambient electromagnetic radiation (EMR)**
- **Usability: Automatically authenticate devices only in small area we call the *personal authenticated region***
- **Security: Periodic update of authentication key**
- **Practicality: The only additional hardware required is wire**

Ambient Electromagnetic Radiation (EMR)

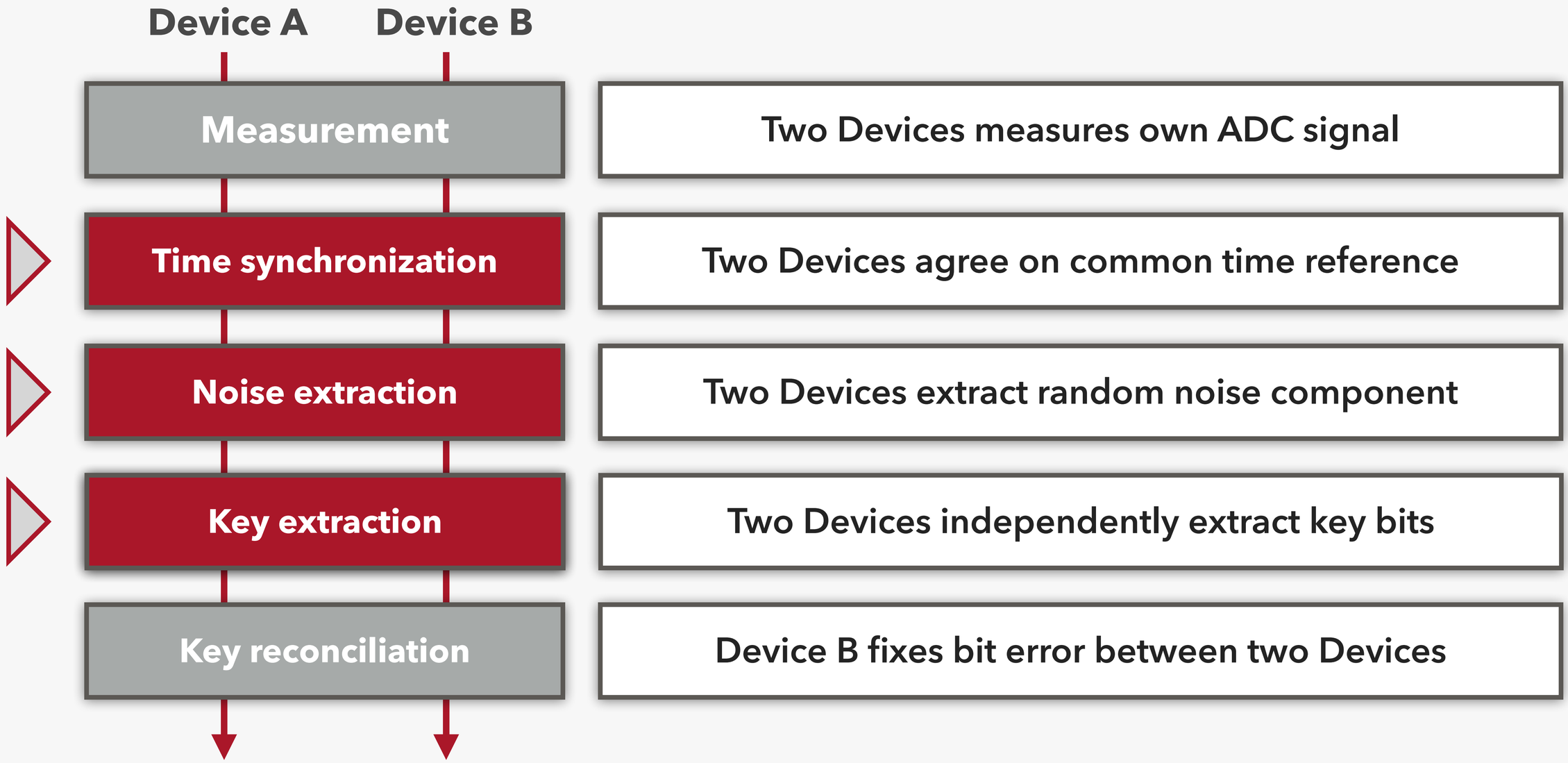




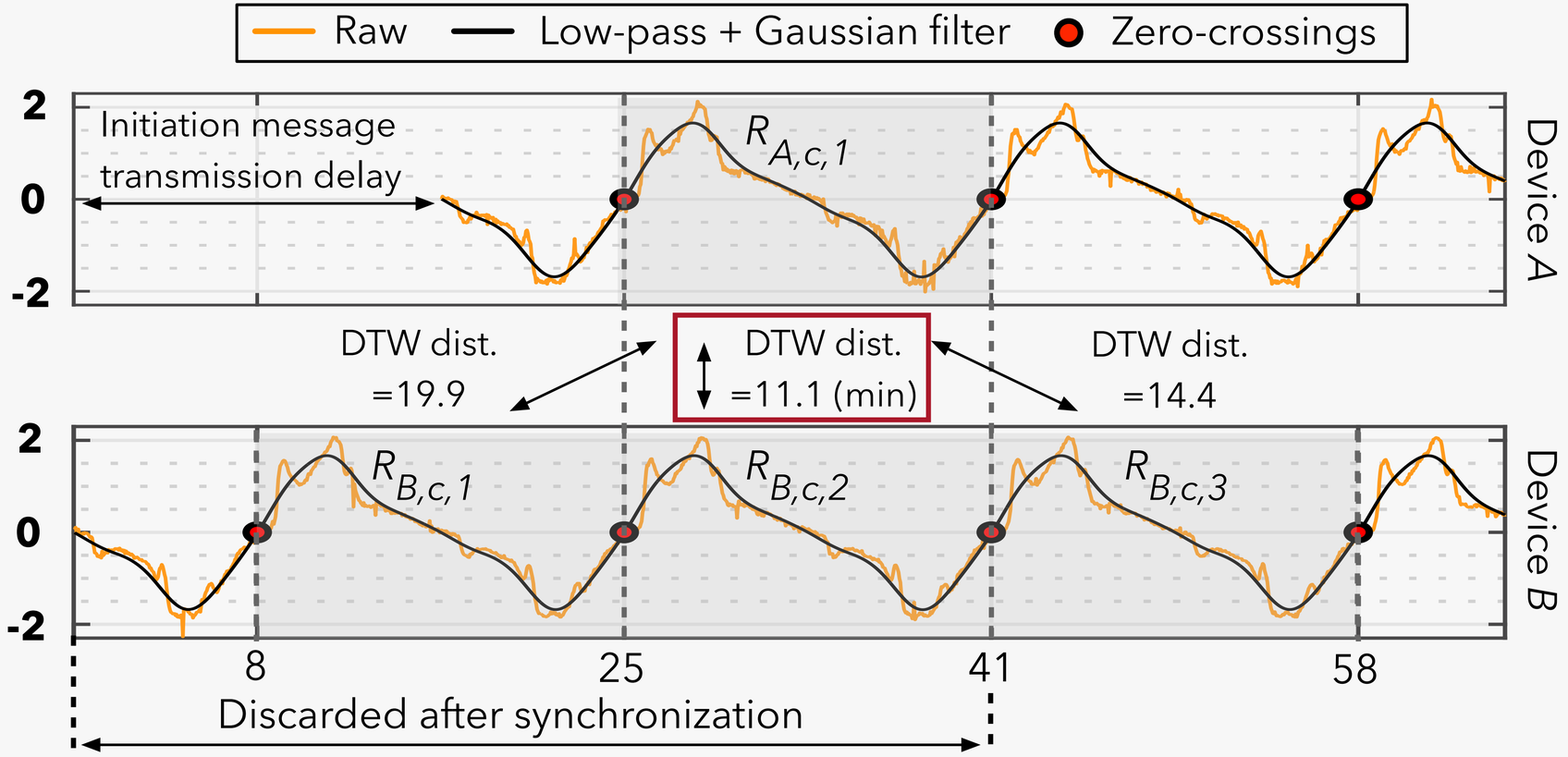
- **Surrounding power lines and appliances produce ambient EMR**
- **Measured using ADC with conductor wire connected to the input pin**
- **Two locations are 5 m apart while power cycling hairdryer in the middle**

EMR is spatiotemporally unique

AeroKey Processing Pipeline

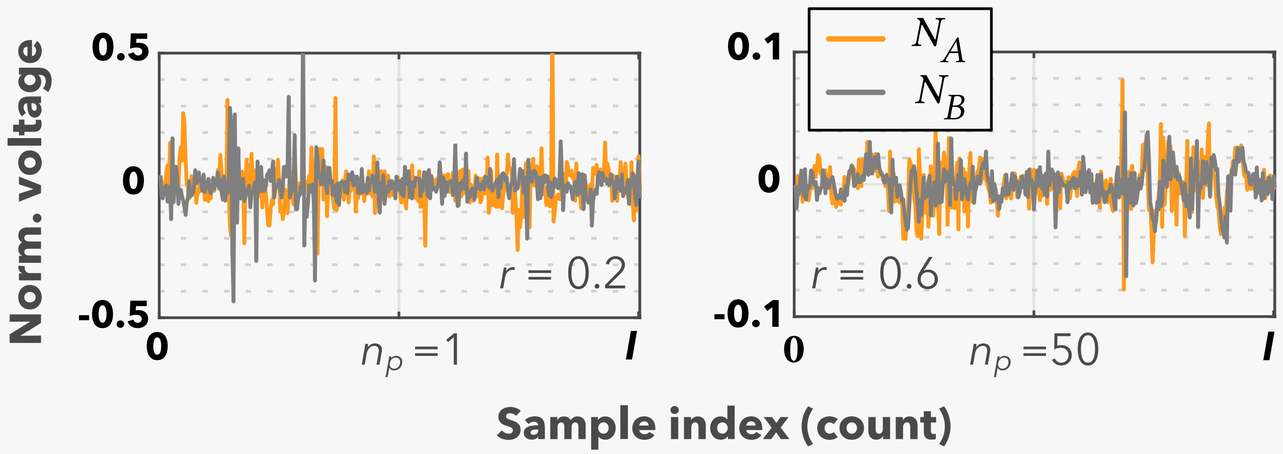


AeroKey Time Synchronization



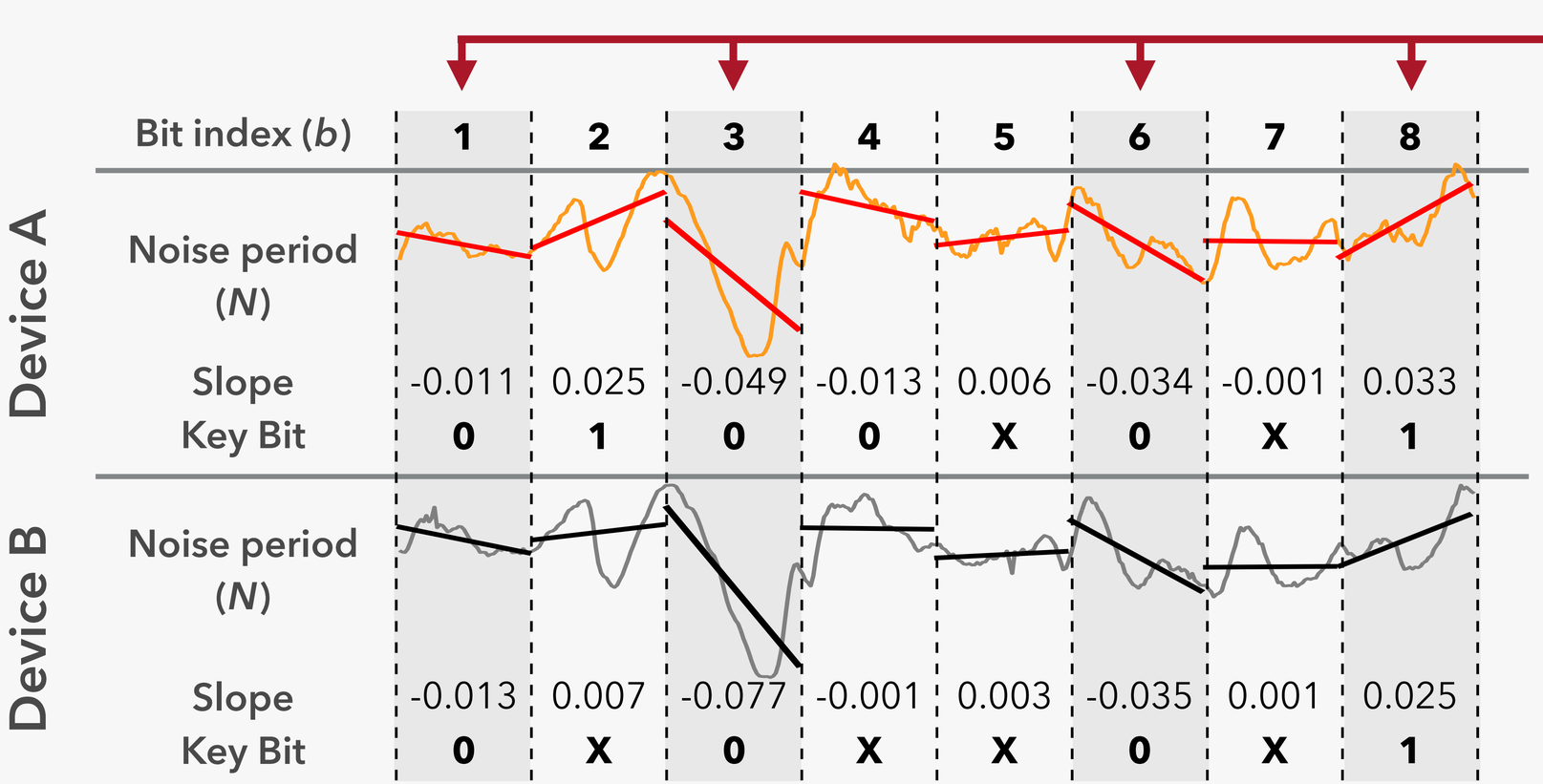
- **Two devices need to agree on common time base**
- **Each 60 Hz periods are marked with zero-crossing indices**
- **Dynamic time warping (DTW) metric used to find most correlated period**

AeroKey Noise Extraction



- **To increase correlation between two devices, each extracts mean period (M_u)**
  - Mean period: sample wise mean of all measured periods.
  - n_p represents number of periods
- **To remove 60 Hz component, each device extracts noise period (N_u)**
  - Noise period: sample wise subtraction of mean periods from different time
  - It represents amplitude variation between two timestamps
- **Correlation *r* is highest with higher n_p**

AeroKey Key Extraction

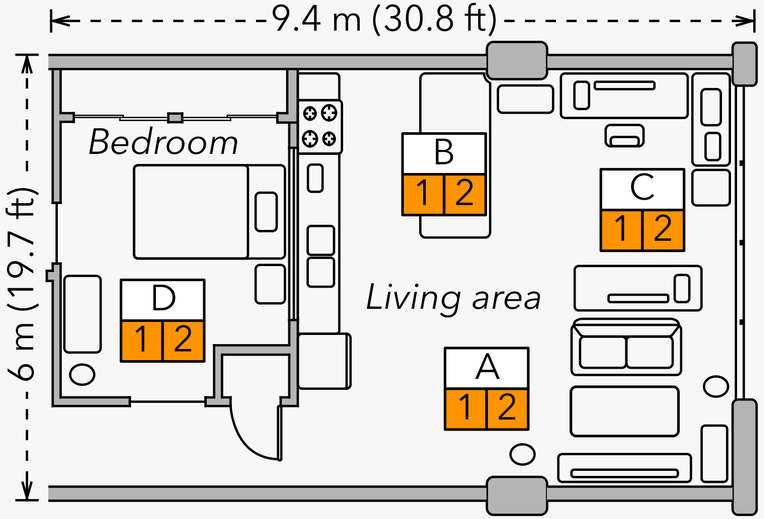


Only extract bits from index 1,3,6,8

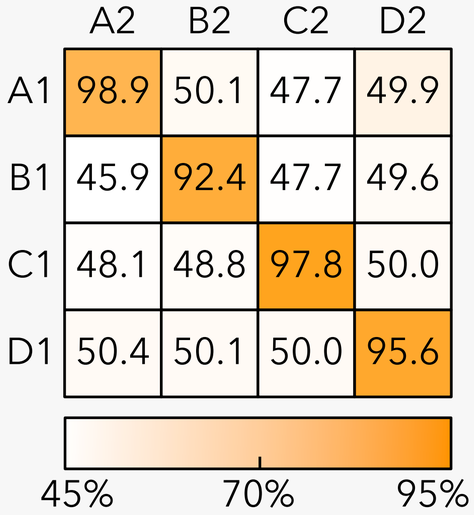
Threshold (th) = 0.015

- **Noise period (*N*) is sliced into bins (b) and the slope is extracted**
- **If slope is greater than positive threshold, bit 1 is extracted**
- **If slope is less than the negative threshold, bit 0 is extracted**
- **If slope is in between threshold, bit is discarded (x)**

Distance Evaluation



One bedroom apartment

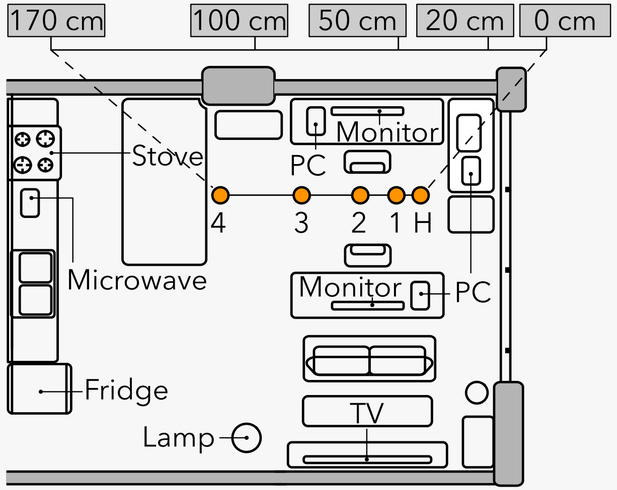


Bit agreement rate between devices

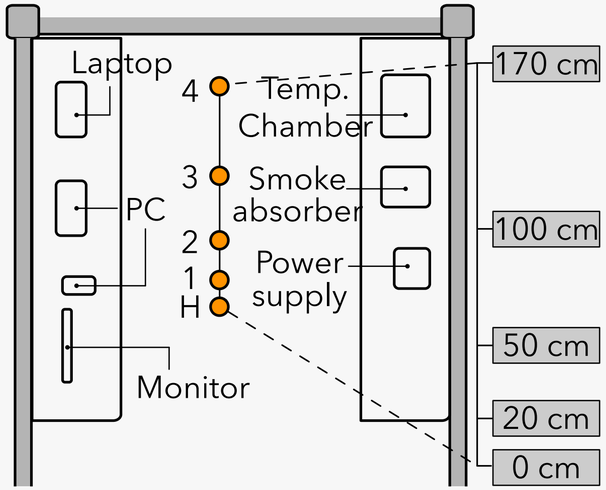
- In four regions (A,B,C and D) pair of devices are placed within 20 cm
- All devices attempt to authenticate with each other

Devices in the same region achieves 96.2% compared to 49.0% achieved by the distant pairs

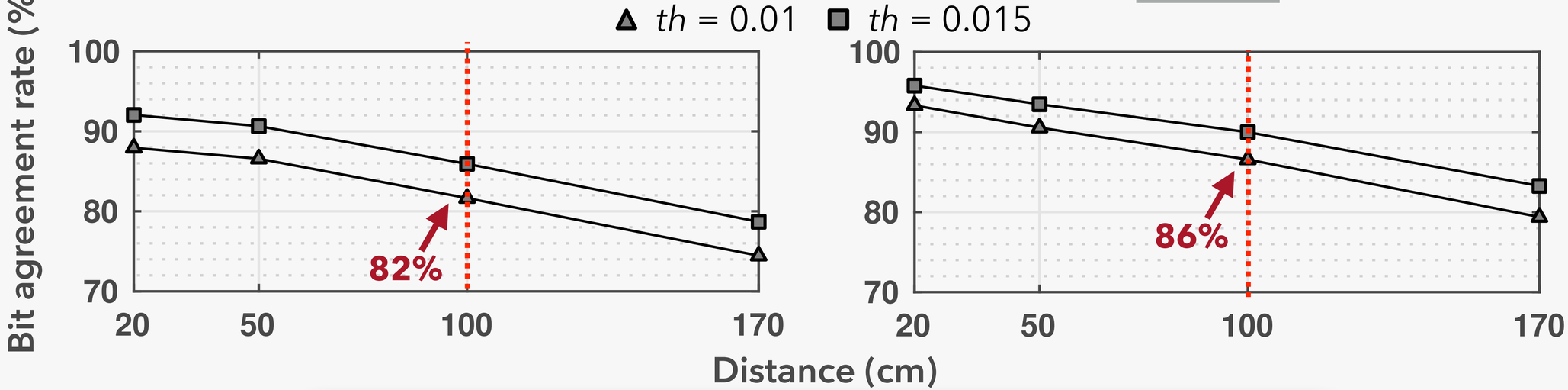
Distance Evaluation



One bedroom apartment



Lab

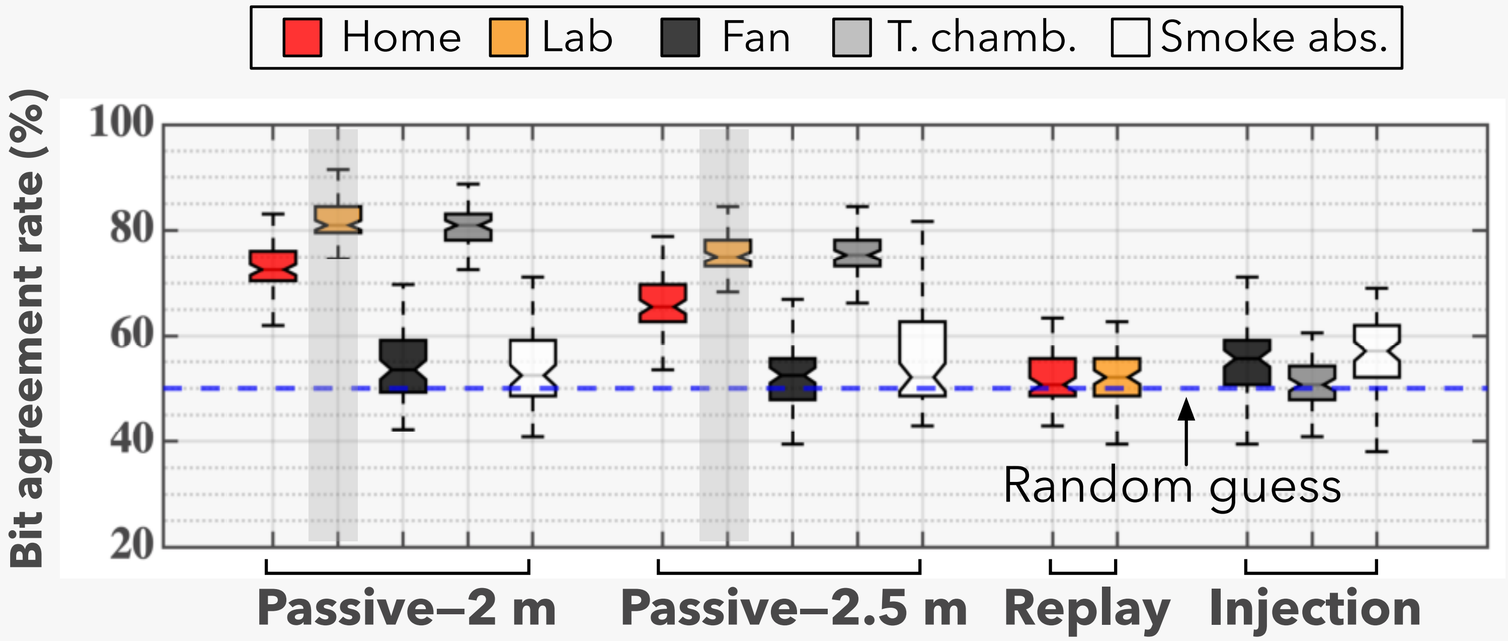


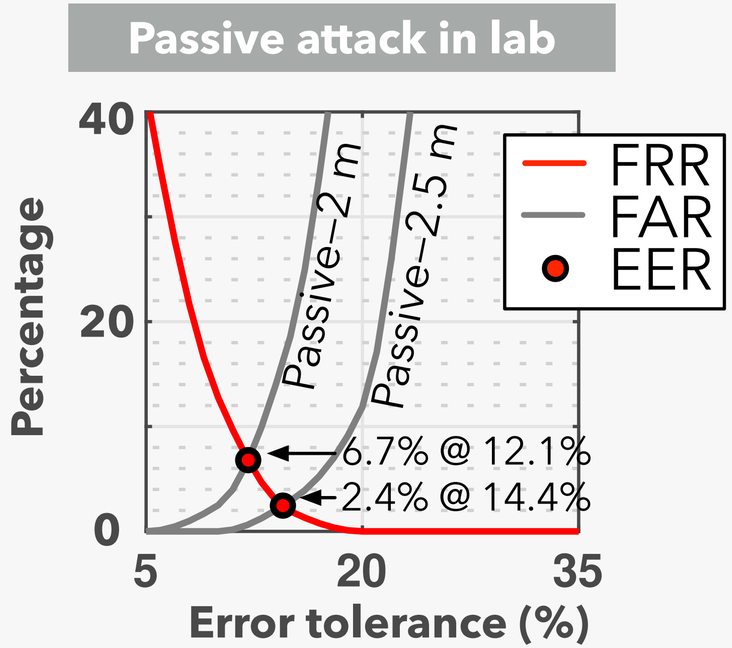
High bit agreement rate under 100 cm

Adversarial Evaluation

- **Threat model**
  - **Adversary resides outside of personal authenticated region and tries to authenticate**
  - **Fully aware of the protocol, can eavesdrop on publicly exchanged messages**
  - **Passive attack**
    - Resides outside of authenticated region and uses measured EMR to initiate authentication
  - **Replay attack**
    - Gains access to future authentication location and timestamp
  - **Injection attack**
    - Uses high wattage loads to Induces strong EMR signal in environment

Robustness Evaluation

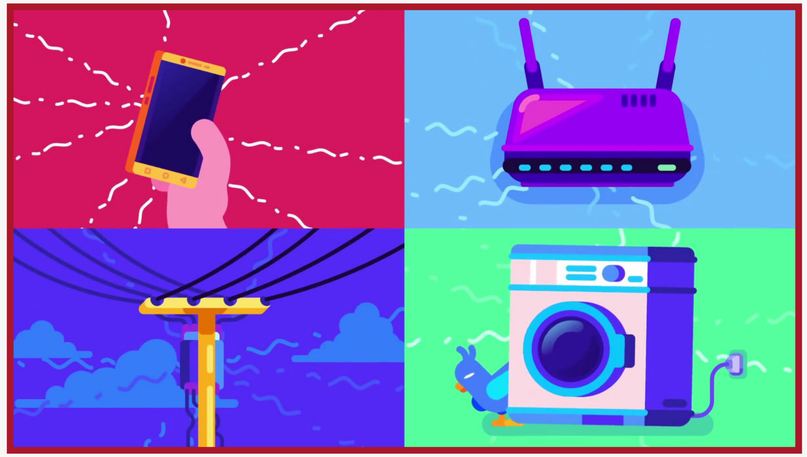


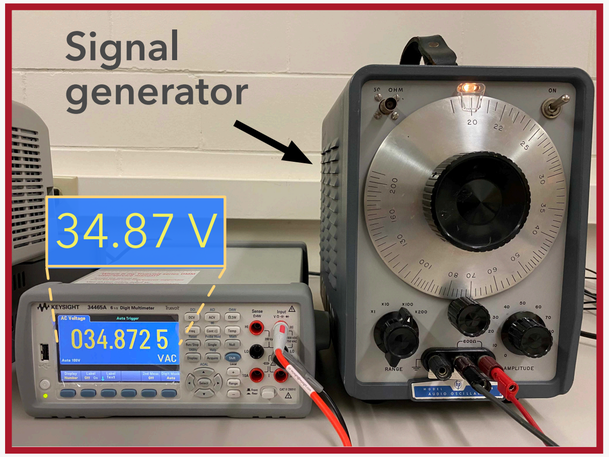


- **Passive attack in lab achieves highest adversarial BAR**
- **Replay and injection attack achieves BAR close to random guess**

The highest EER achieved from the attacker is 6.7%

AeroKey Conclusion





Usable	True zero-interaction authentication within 1 m, authentication within 24 s
Secure	Periodic update of passkey and robustness from various attackers outside personal authenticated region
Practical	Induce minimal hardware overhead (simple conductive wire)