BLE-Guardian: Protecting the Privacy of BLE Users

Kassem Fawaz*, Kyu-Han Kim†, Kang G. Shin*

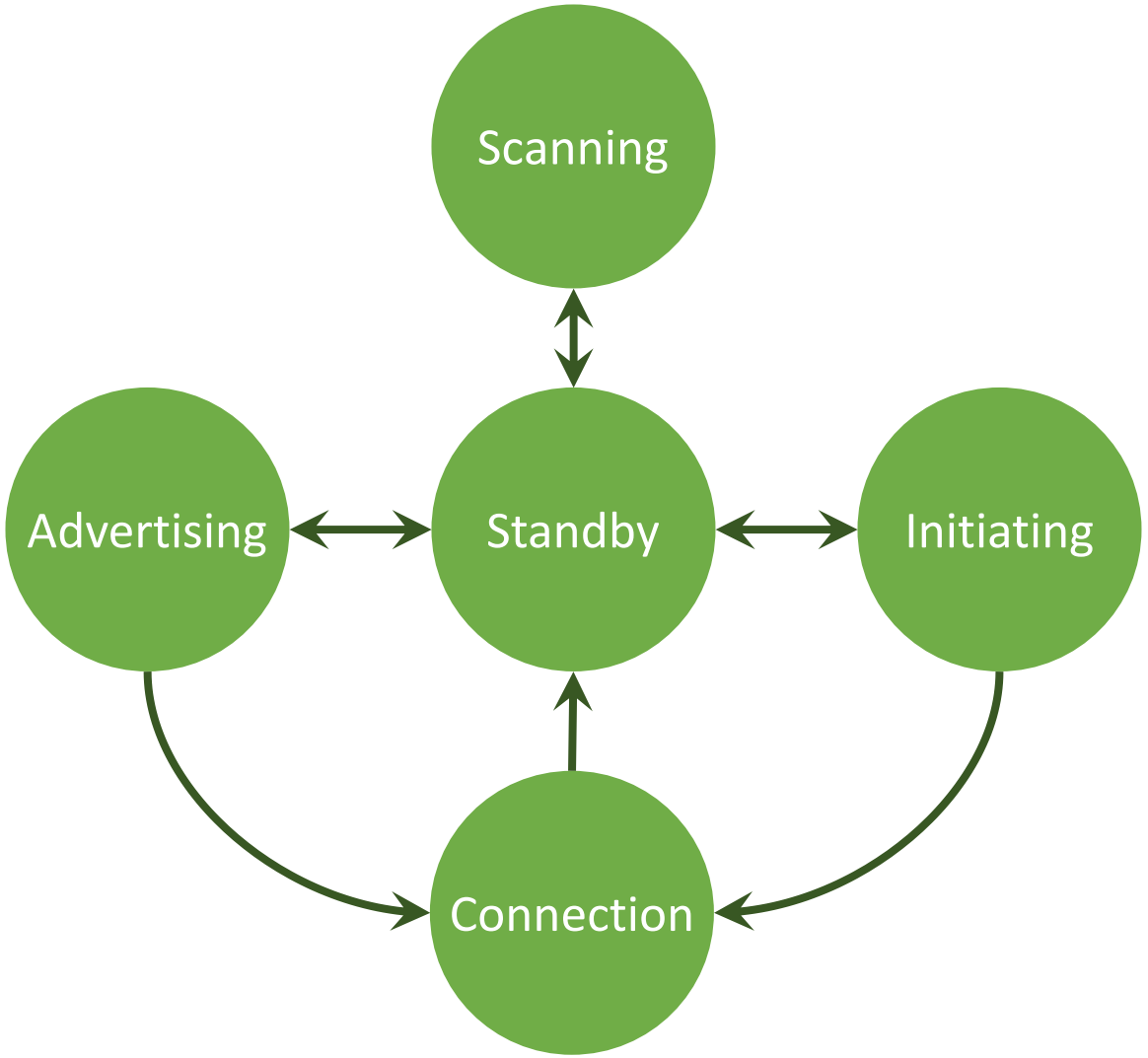
*Computer Science and Engineering, University of Michigan

†Hewlett Packard Labs

What is Bluetooth Low Energy?

- Attractive communication technology
  - Short range
  - Low energy footprint
  - Supported by most hosts
- Currently:
  - 74K unique products with BLE support
- 2013:
  - 1.2 billion BLE products shipped
- 2020:
  - 2.7 billion BLE products expected

BLE Primer

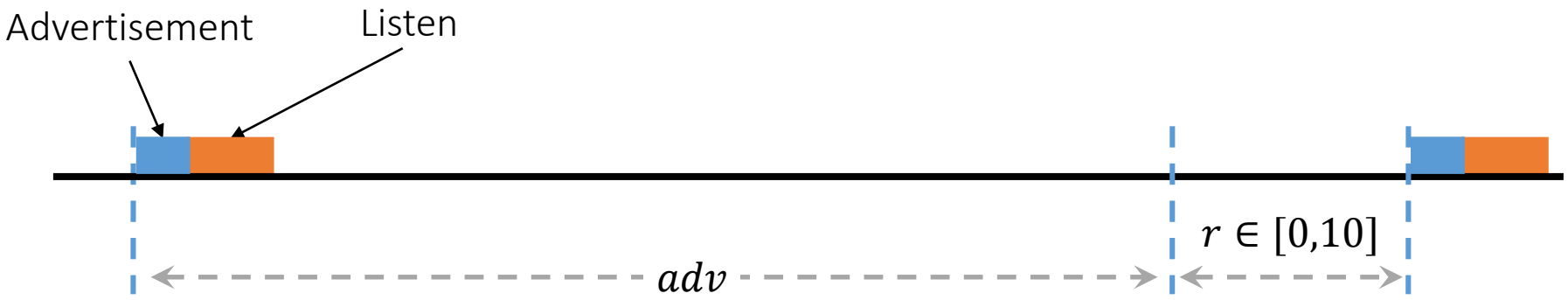


- **Standby:** Low Power Mode. Receiver and transmitter switched ‘off’
- **Advertising:** Used by low power ‘Server’. Only transmitter required.
- **Scanning:** Used by ‘Client’. Receiver listens to advertising channels.
- **Initiating:** ‘Server’ sends connection request
- **Connection:** After scanning, ‘Client’ responds to ‘Server’ advertisement

BLE Advertisements

- 3 dedicated advertising channels:
  - 2402 MHz (*37*), 2426 MHz (*38*), 2480 MHz (*39*)

Type	Description	Frequency
ADV_DIRECT_IND	Connect to a particular device only	3.75 ms, but only for 1.28 seconds
ADV_IND	General presence known + connections	20ms – 10.24s



BLE Security and Privacy

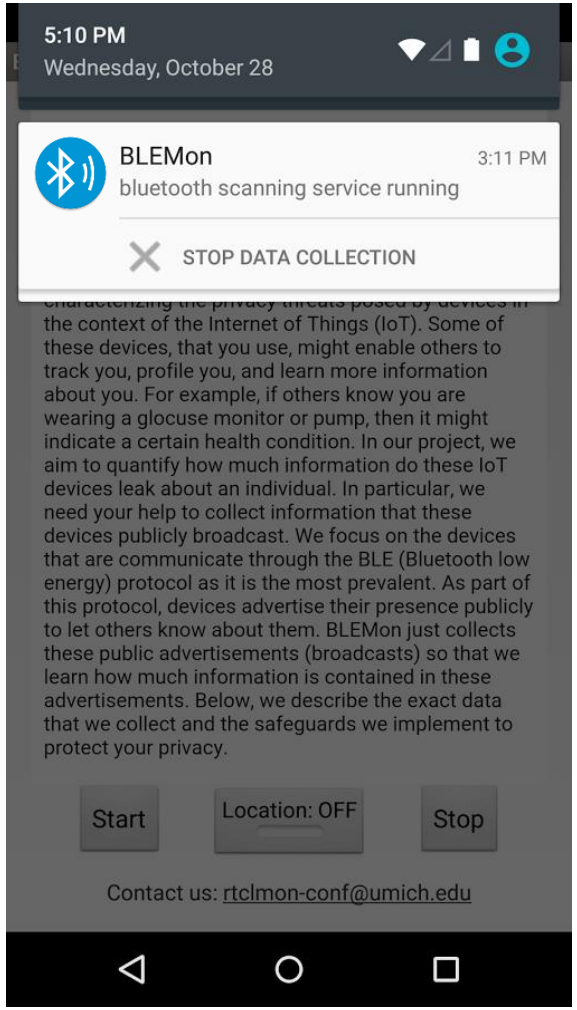
- Pairing & bonding
  - Prevent unauthorized access to device or secured services
- Address randomization
  - Prevent user tracking
- Direct Advertisements
  - Prevent user tracking and profiling

BLE Privacy & Security Effectiveness

- *Passively* scan for BLE advertisements
- Collect:

`<Timestamp, BT Address, advertisement content, RSSI>`

Site	Participants	Period
Hewlett Packard Labs	1	40 days
Ann Arbor	13	2 months
Phone LAB/ SUNY Buffalo	86	2 months



BLE Privacy & Security Effectiveness

- Indirect Advertisements
  - Detected 214 different unique **types of** devices
- Address Randomization

Name	Description
ihere	key finder
DEXCOMRX	Glucose monitor
Frances's Band ea:9d	smartband
Otbeat	heart rate monitor
JS00002074	digital pen

Revealing Names

Device	Days observed
One	37
Flex	37
Zip	37
Forerunner 920	36
Basis Peak	25

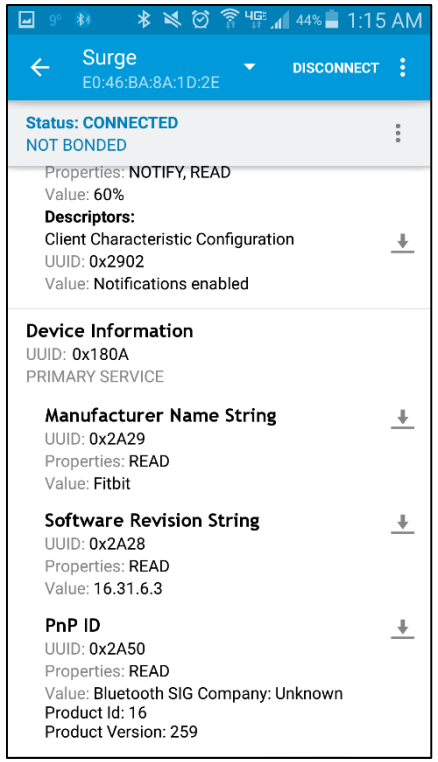
Consistent Addresses

Address
00:17:E9:CB:F3:61
00:17:E9:CB:F5:01

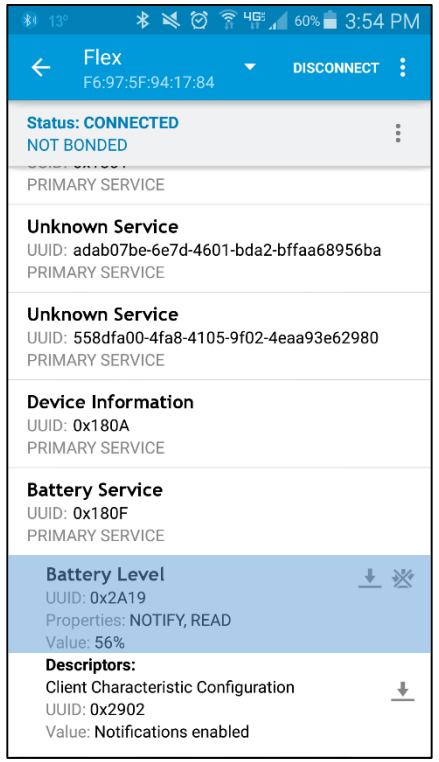
Poor Randomization

BLE Privacy & Security Effectiveness

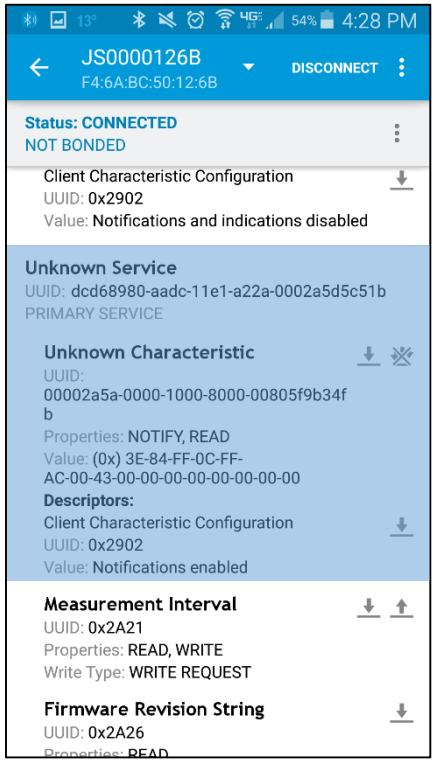
- Device Pairing



Advertise and accept connections

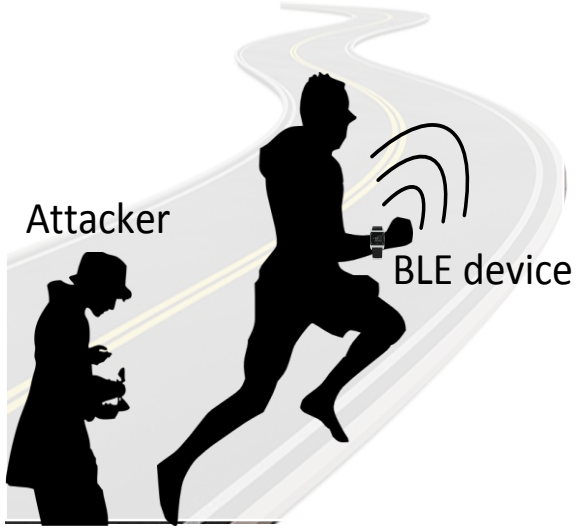


Battery level



Unique identifiers

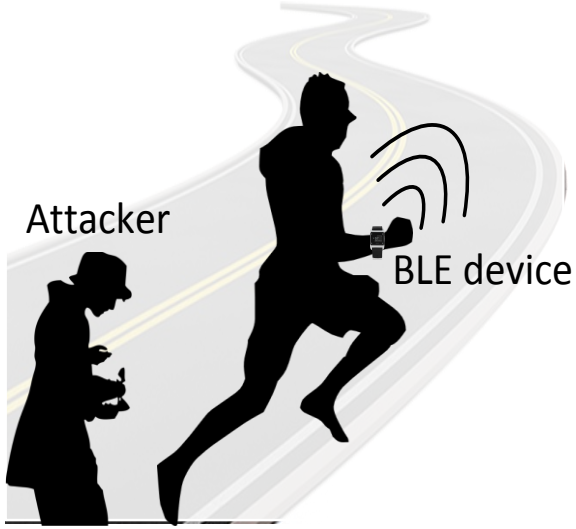
It all starts with the advertisements…

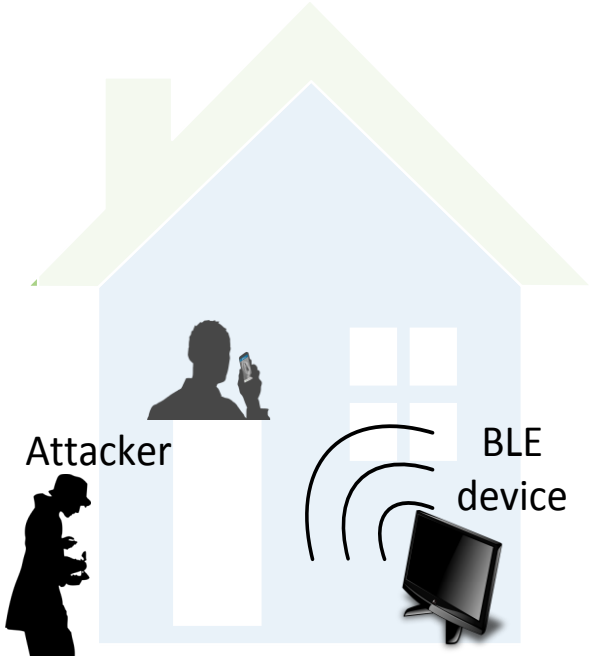


Tracking User

Consistent addresses, poor randomization, unique device names and identifiers

It all starts with the advertisements…



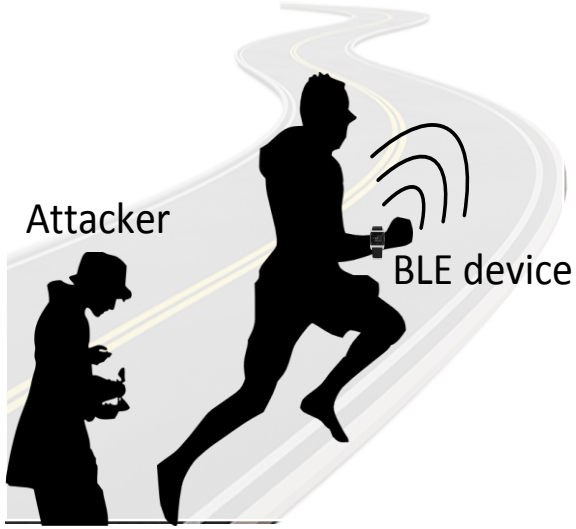


Tracking User

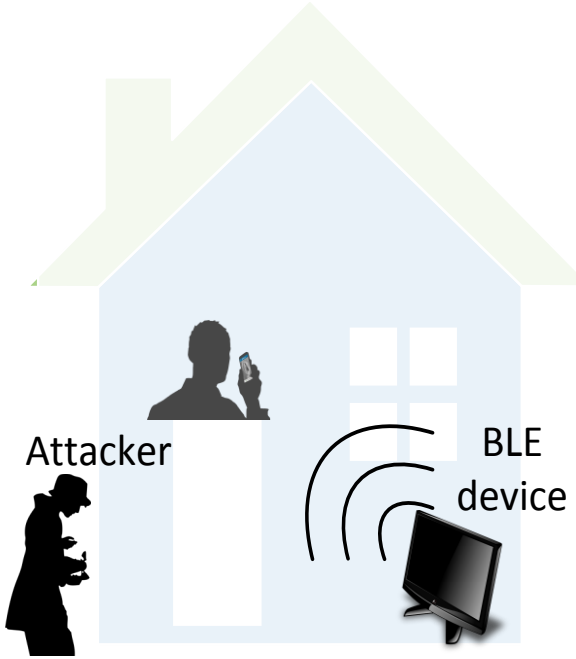
Profiling User

Health situation, user's lifestyle, behavior, preferences, and personal interests

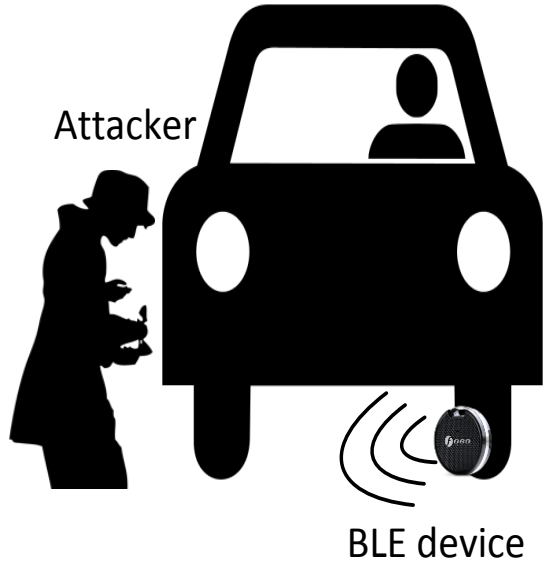
It all starts with the advertisements…



Tracking User



Profiling User



Harming User

Fingerprinting of and unauthorized access for sensitive systems and devices

Research Questions

Can we effectively fend off the threats to BLE-equipped devices

(1) in a device-agnostic manner,

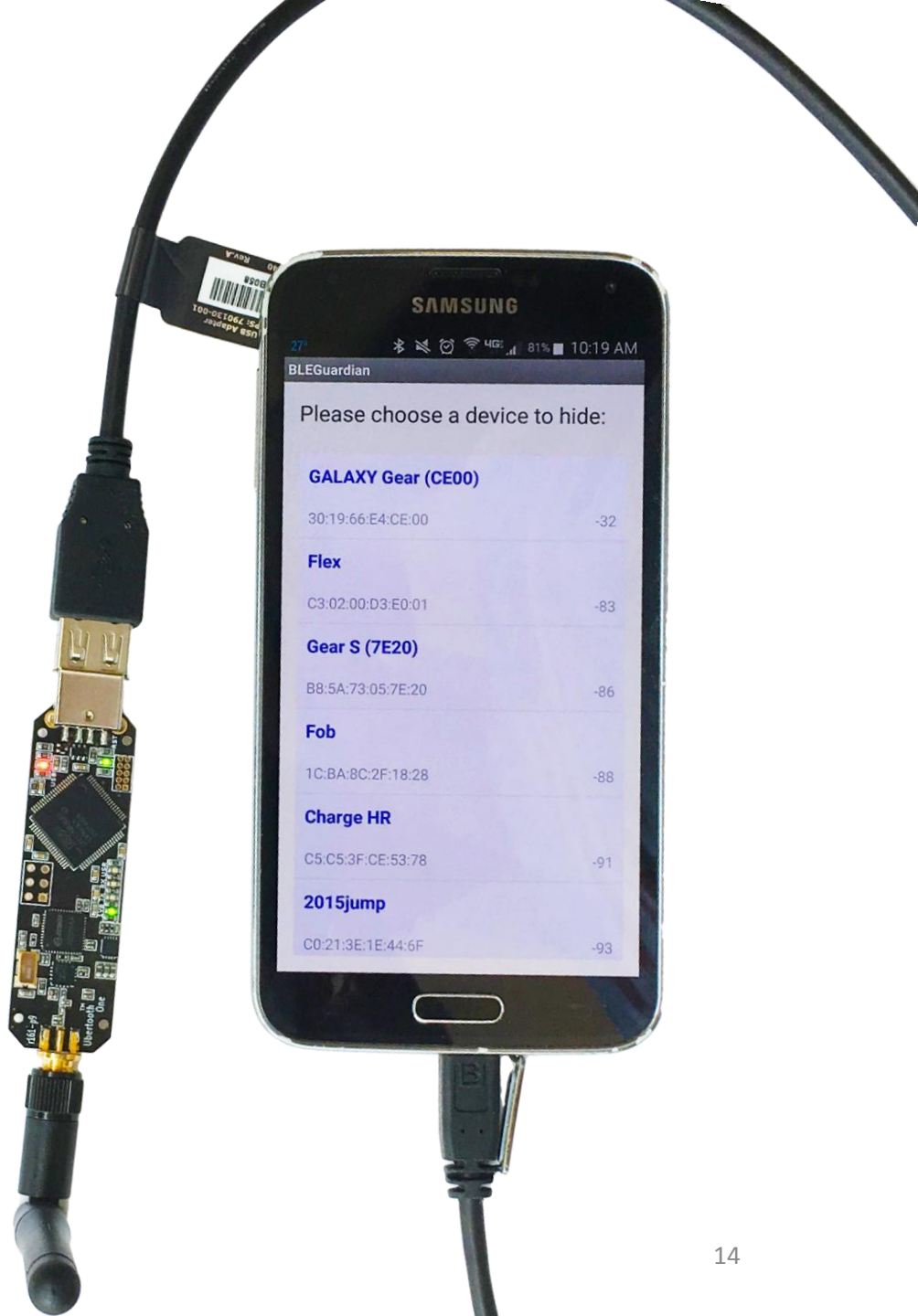
(2) using COTS (Commercial-Off-The-Shelf) hardware only, and

(3) with as little user intervention as possible?

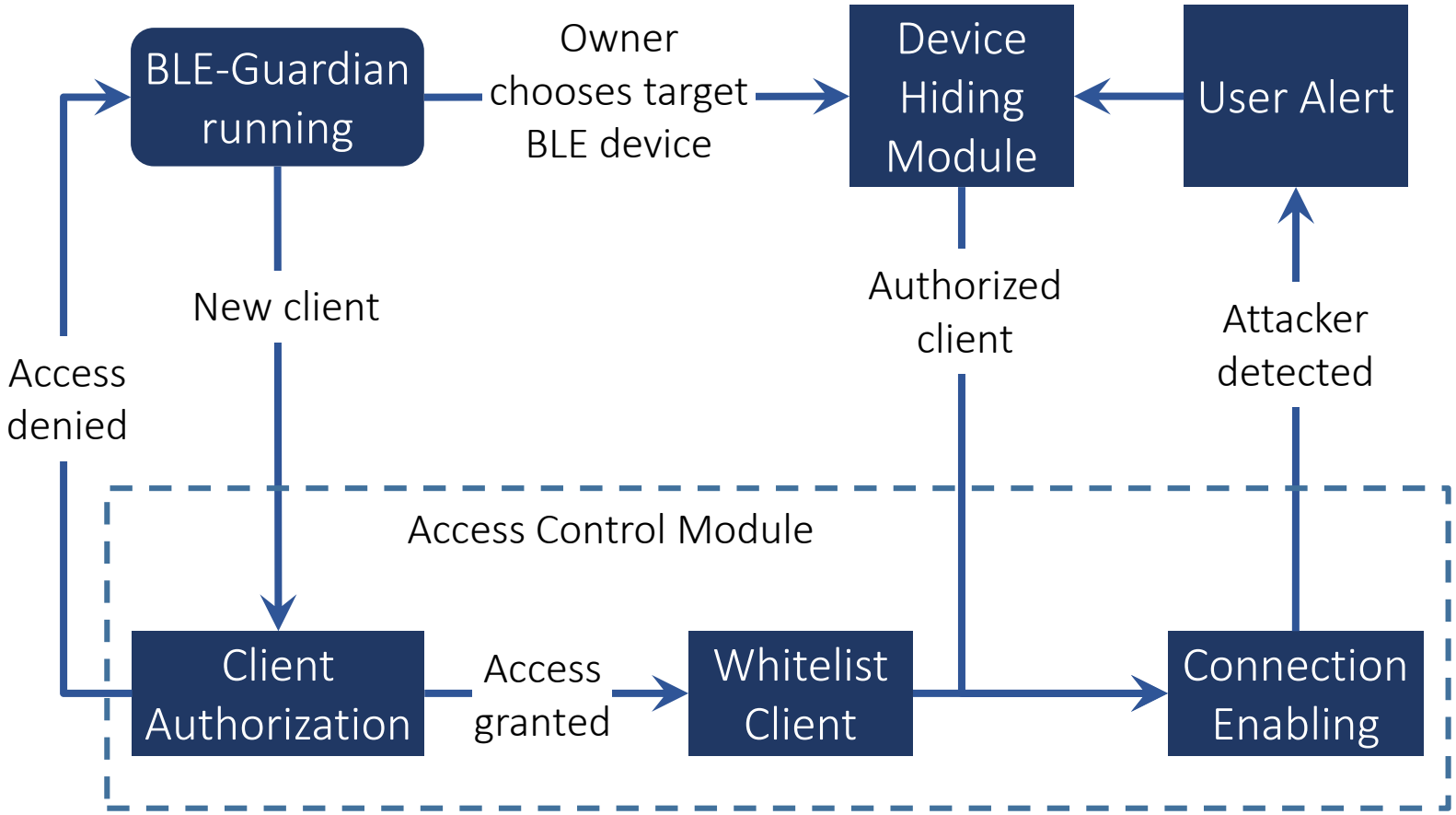
BLE-Guardian

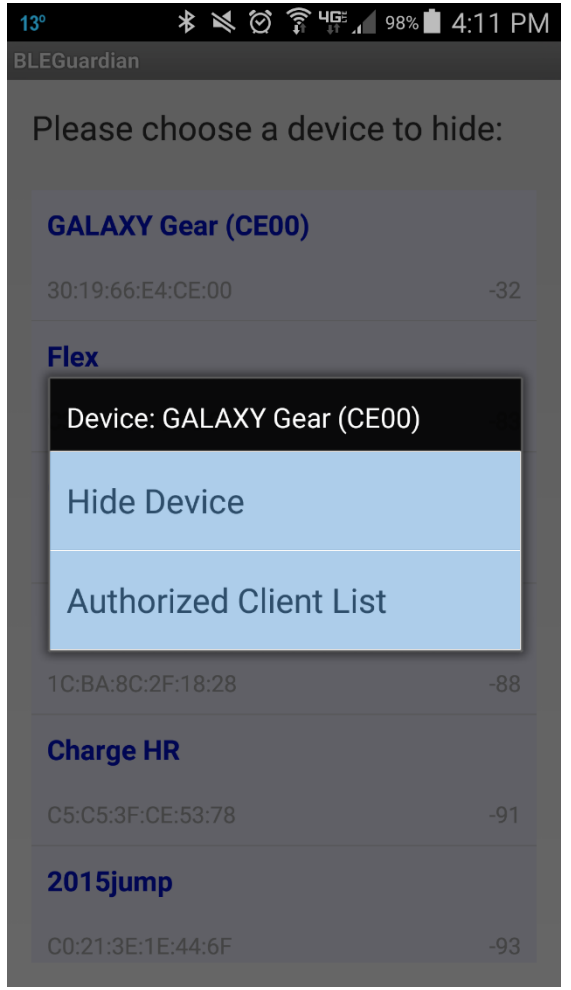
BLE-Guardian

- Ubertooth One
  - Programmable BT radio
  - Open source firmware
  - Rx/Tx on each BT channel
- User-level app
  - Control BLE-Guardian
  - Update firmware seamlessly



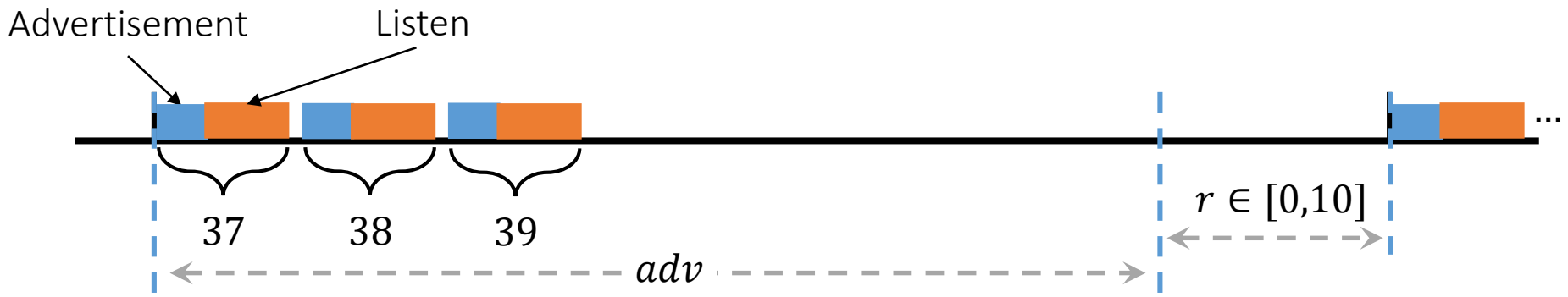
High-level Description



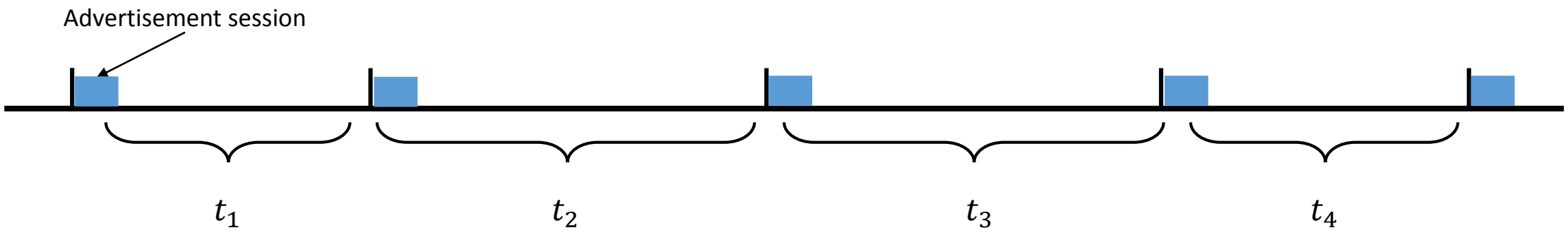


Device Hiding

- Jam BLE device advertisements to hide its existence
- Need to learn device advertising Sequence
  - Otherwise jamming will be ineffective or inefficient

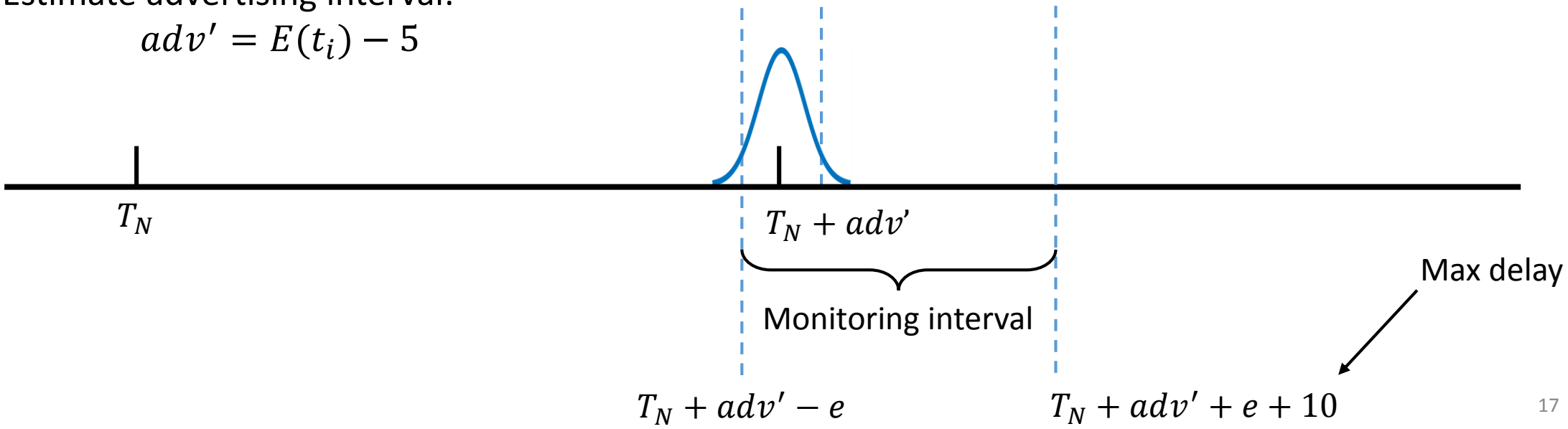


Device Hiding

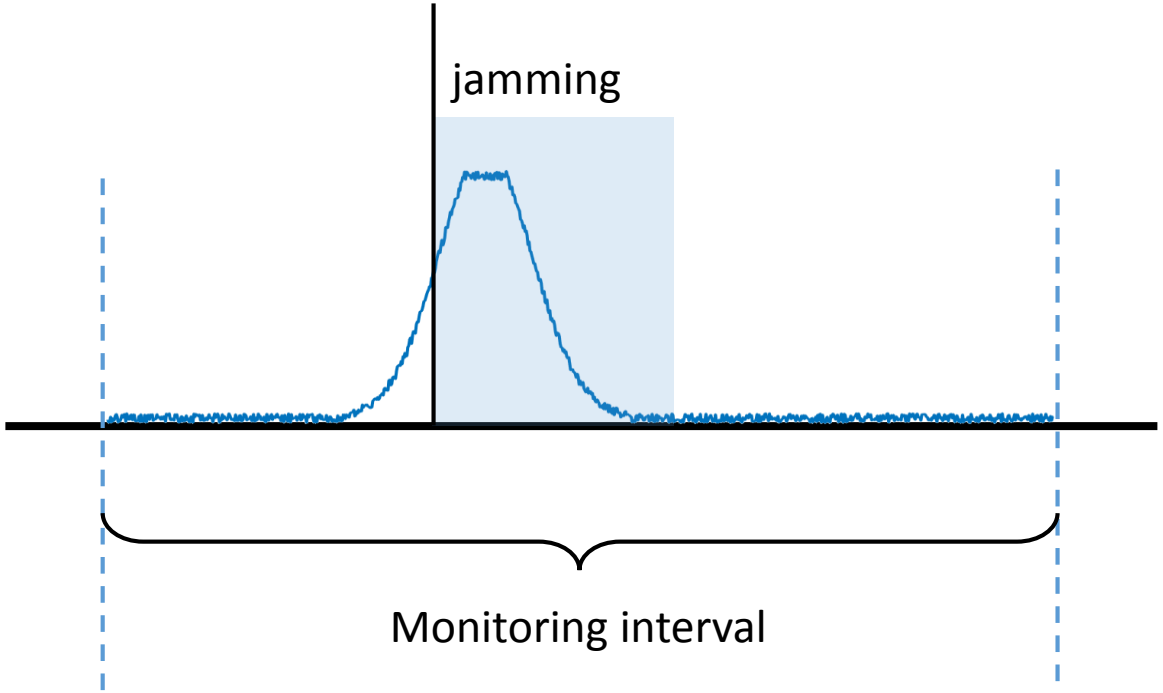


Estimate advertising interval:

$$adv' = E(t_i) - 5$$



Device Hiding



- Detect RSSI (received signal strength indication) increase
- Apply jamming and follow advertising sequence

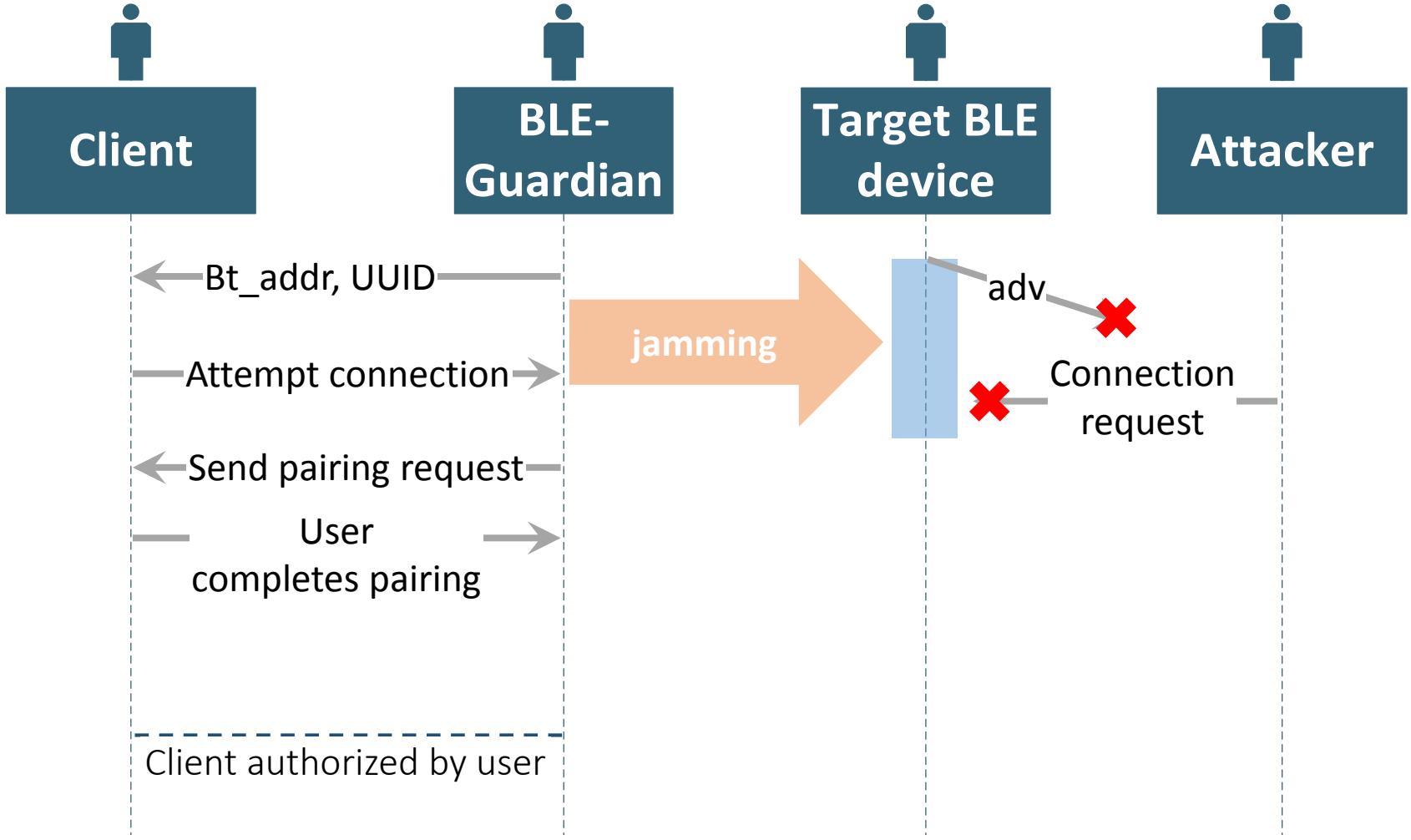
At this point, the target BLE device is hidden.

How to enable access to it?

Access Control

Authorization:

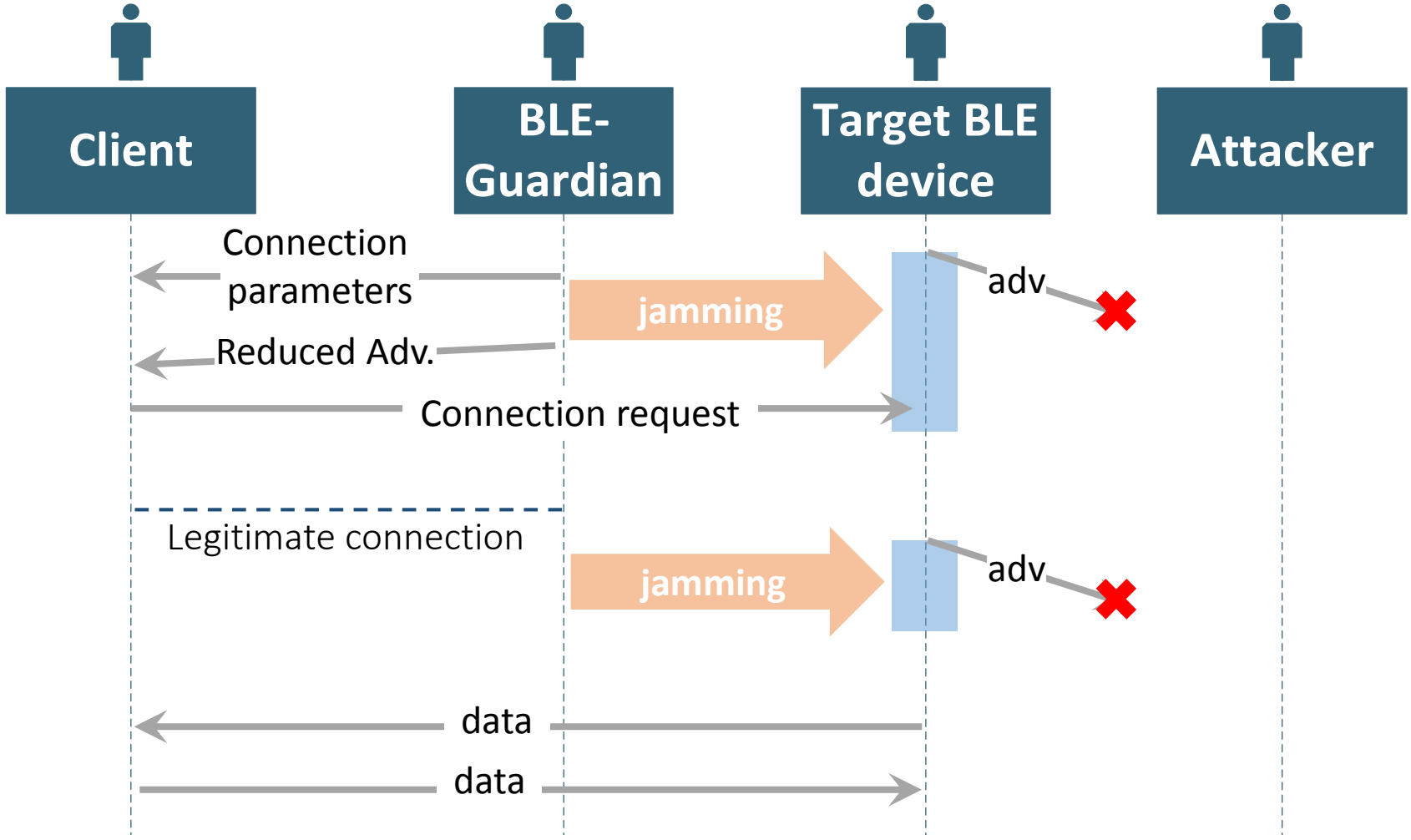
Bluetooth classic as an OOB channel.



Access Control

Connection Enabling:

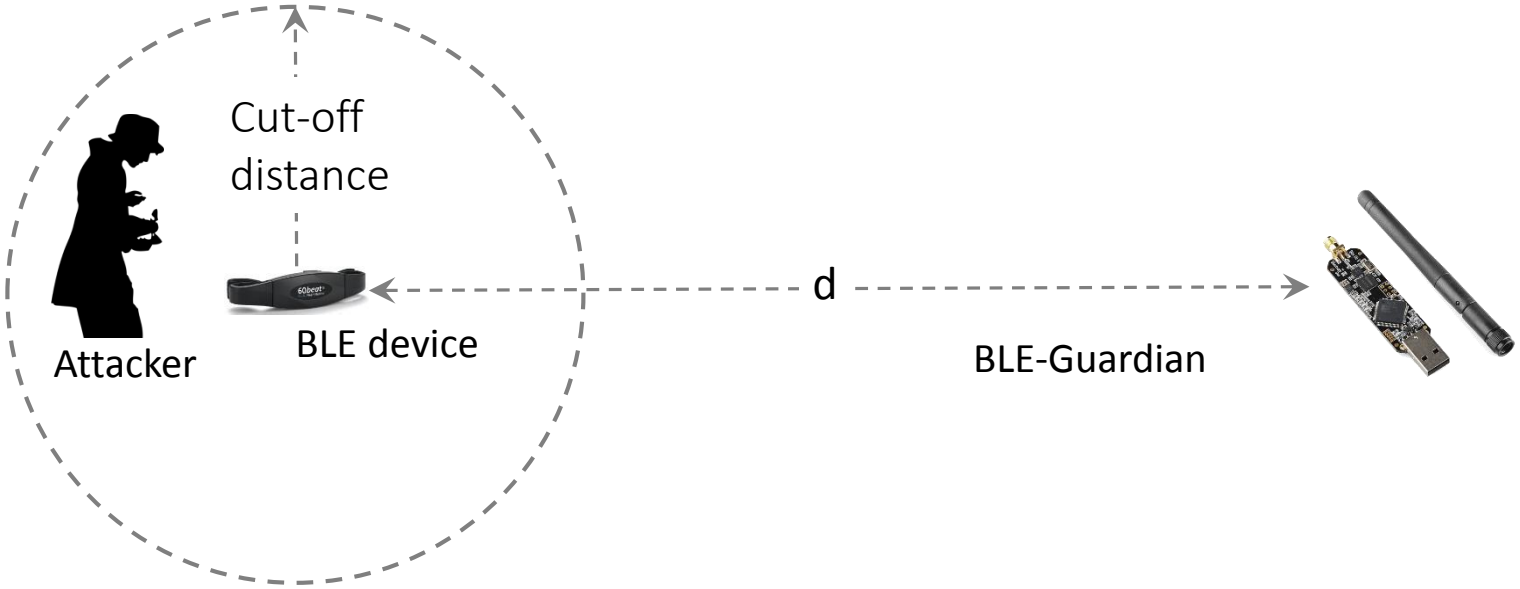
Connection parameters to distinguish legitimate connection request.



Evaluation

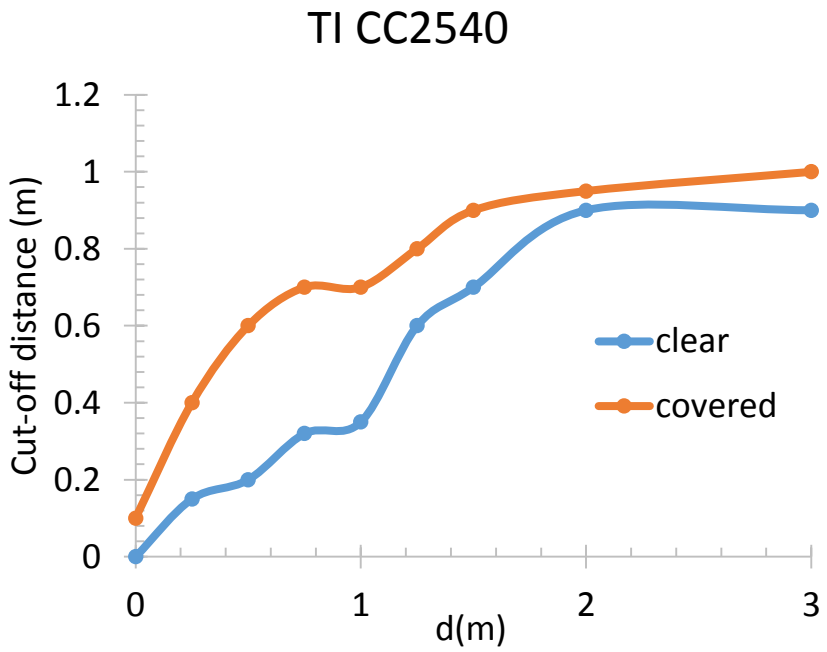
Evaluation

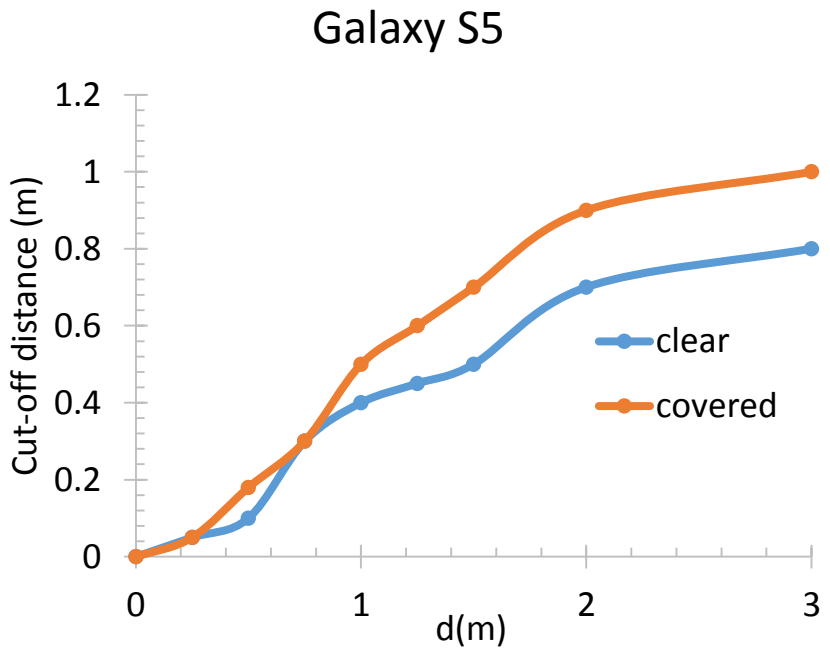
Cut-off Distance



Evaluation

Cut-off Distance



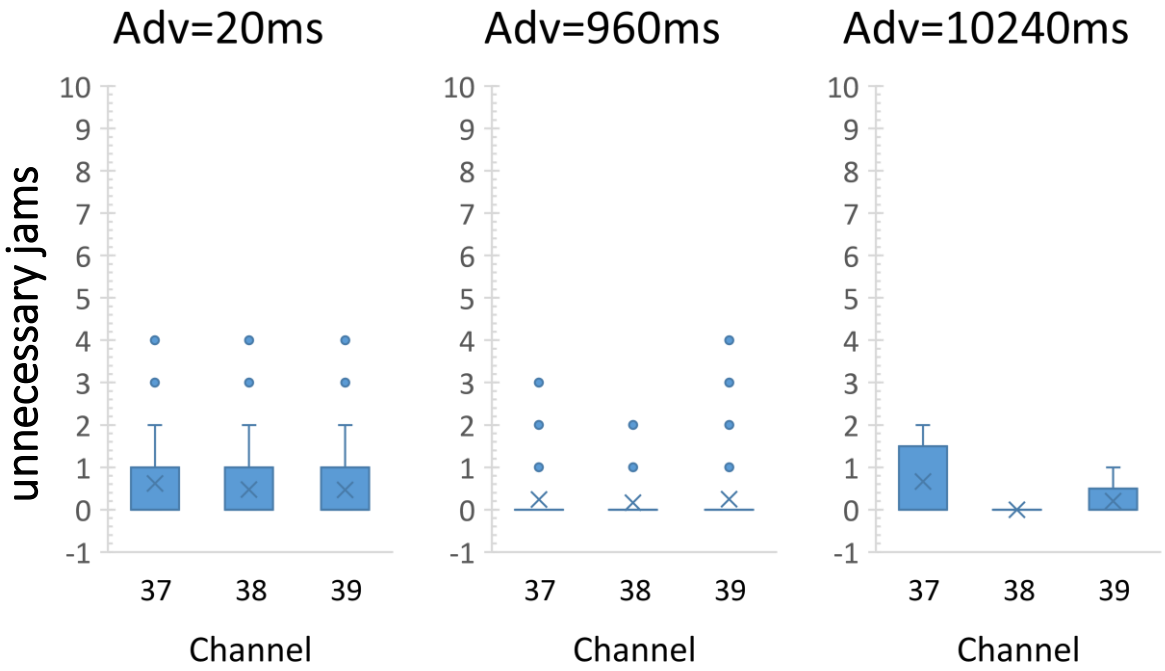


Adversary has to be within 1 m of BLE device to read its advertisements

Evaluation

Impact on Advertising Channels

1. Protect single device at advertising intervals:
   - 20ms, 960ms, and 10.24 sec
2. Two devices advertising at 20 ms
3. 15 other devices
   - With varying advertising frequencies

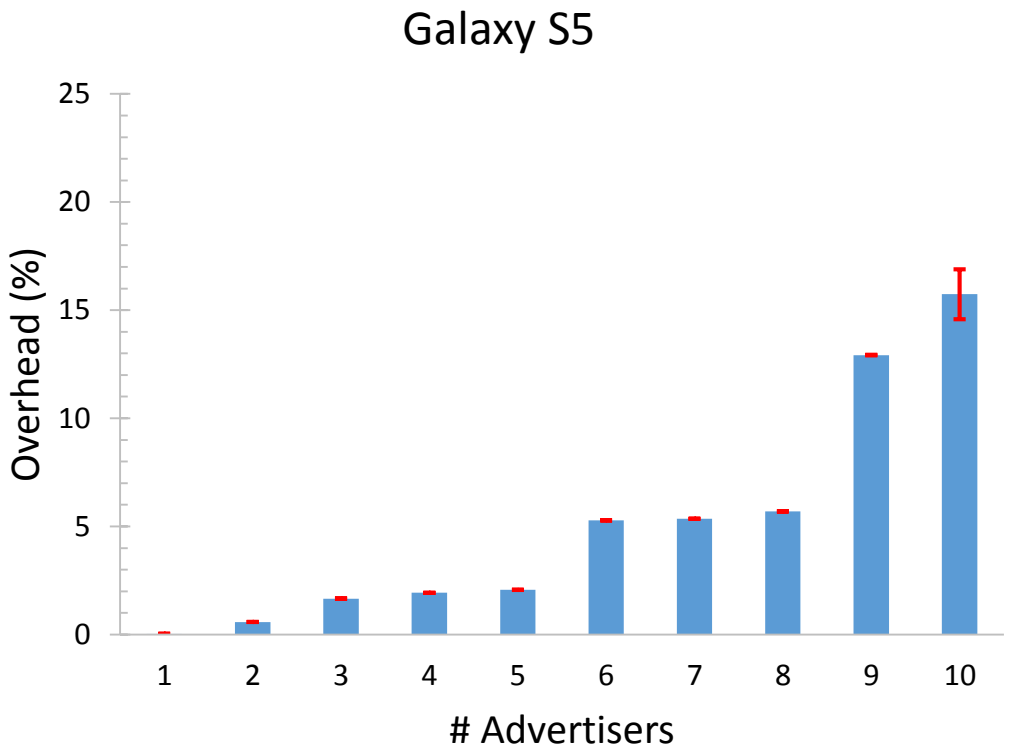


The number of unnecessary jamming instance is minimal

Evaluation

Energy Overhead

1. BLE-device and authorized clients
   - No overhead
2. Smartphone as a gateway
   - Idle power: 1370mW
   - Overhead: less than 16%



Conclusion

- BLE-Guardian
  - Privacy protection for BLE device users
  - Device agnostic and relies on COTS hardware
  - Low overhead on advertisement channels

- Future work
  - Explore other M2M protocols such Zigbee
  - Implement without needing external hardware (need firmware access)

Thank You

kmfawaz@umich.edu

kassemfawaz.com