On Practical Selective Jamming of Bluetooth Low Energy Advertising

S. Brauer, A. Zubow, S. Zehl, M. Roshandel, S. M. Sohi
Technical University Berlin & Deutsche Telekom Labs
Germany
Outline

• Motivation,
• Problem Statement,
• System Model,
• Bluetooth LE Advertising Primer,
• Proposed Jamming Solution,
• Evaluation,
• Countermeasures,
• Conclusion & Future Work.
Motivation

• The *Bluetooth Low Energy* (BLE) protocol stack gave rise to whole new class of devices: **BLE beacons**

• Beacons are small, often battery-powered devices, that continuously broadcast information by using the *BLE Advertising* process

• Despite their limited functionality they can be used to implement complex services, e.g.:
  
  – Targeted advertisement
  
  – Mobile Payment authentication (e.g. PayPal)
  
  – Indoor Navigation
Motivation (II)

• BLE beacons have seen a steady rise in popularity:
  – 72% of all retailers are expected to have beacon technology installed until 2019,
  – Hence the security of BLE beacons is worth investigating.

• BLE is prone to jamming attacks like any wireless technology,

• Purpose of this work is to discuss the risk of such a jamming attack on BLE beacons,

• Common definition for risk:

\[ \text{Risk} = \text{Likelihood} \times \text{Impact} \]
Problem Statement

- We devised **five criteria** to evaluate the risk of a jammer:
  - Jamming success (impact),
  - Energy-efficiency (impact),
  - Cost (likelihood),
  - Possible countermeasures/detection methods (likelihood & impact),
  - Ability to selectively jam targets (impact).

- Can we build a jammer that is optimized for this criteria?
  - A low-cost, energy-efficient selective jammer
System Model

- We consider the basic scenario consisting of:
  - A BLE beacon source emitting BLE advertisement packets,
  - A receiver which performs passive scanning for BLE adv packets,
  - A single jammer node.
Bluetooth LE Advertising Primer

- BLE operates in 2.4 GHz ISM band,
- Bit rate: 1 Mbit/s  →  1 bit = 1 µs air time
- 40 channels, 2 MHz each:
Bluetooth LE Advertising Primer (II)

- Advertising channel: channels 37, 38 and 39 (yellow),
- Advertising Channel are spread across the spectrum to avoid interference (Wi-Fi),
- Advertising uses a **frequency hopping** scheme to improve **robustness**, i.e. a beacon is transmitted on different adv. channels.
Bluetooth LE Advertising Primer (III)

- Advertising takes place at a regular interval `advInterval` (>20ms) with an added pseudo-random delay `advDelay` (between 0.625ms and 20ms) for collision avoidance.

- **Note**: During each `Advertising Event` the beacon is transmitted on all (!) three advertising channels.
Bluetooth LE Advertising Primer (IV)

- During each *Advertising Event* a beacon **hops** through all used advertising channels (mostly all 3) in **ascending order**.

  ![Diagram](image)

  - Advertising event entered
    - Adv_idx = 37
    - \( \leq 10 \text{ms} \)
  - Advertising event entered
    - Adv_idx = 38
    - \( \leq 10 \text{ms} \)
  - Advertising event entered
    - Adv_idx = 39
    - \( \leq 10 \text{ms} \)

- Two subsequent advertising packets within one Adv. Event must be less than 10 ms apart. **A minimum time is not specified.**
Bluetooth LE Advertising Primer (V)

- Basic BLE framing:
  - Preamble + Access Address used as correlation code,
  - No Forward Error Correction (FEC), so every bit error results in a corrupted packet (detected using CRC)
Jammer Design Principles

• We use commercially off-the-shelf (COTS) hardware that is BLE capable
  – Minimizes the cost,
  – This hardware is often already optimized for low energy consumption

• To save energy we employ a narrow-band jamming scheme with frequency hopping
  – Doesn’t waste energy on unused bandwidth,
  – Makes our jammer harder to detect.

• The duration of the jamming signal can be kept at a minimum (no FEC in BLE)
Proposed Jamming Solution

• Selective, reactive narrow-band jammer:
  – Because we can only jam a single BLE channel at a time (→ narrowband) fast channel hopping has to be applied,

• The jammer is pre-programmed using an API:
  – Two options: **white list or black list** of device addresses to be jammed,
  – Configuration of the BLE adv. channels being used.
Proposed Jamming Solution (II)

• Jammer consists of two components:
  1. **Detection**: jammer **decodes packets on-the-fly** to decide whether to jam this particular packet based on the **device address**,
  2. **Jamming**: on successful detection the jammer emits a short jamming signal.
Selective, Reactive Narrow-band Jammer

- FSM of jammer w/ all 3 Adv channels used:
Implementation Details

• Jammer node: RedBearLab BLE Nano
  – BLE devkit equipped with a Nordic nRF51822 SoC and an integrated antenna,
  – nRF51822 is equipped with a BLE capable transceiver,
  – Max TX power: +4dBm,
  – Cheap: ca. 20 €,
  – Fast turn-around time (time needed to switch from receiving to transmitting): 140 µs,
  – Easily programmable
Evaluation Methodology

- Primary performance **metric** is **Advertising Success Rate**:
  
  \[
  ASR = \frac{\text{# correctly received BLE adv. events}}{\text{total number of transmitted BLE adv. events}}
  \]

- **Objective**: min. ASR, i.e. ASR=0 is perfect jamming.

- Another **metric** is the area covered by the jammer:
  - Spatial area around the jammer with ASR < \( \tau \)

Experiment setup.

![Diagram of interference and distances between devices]

- **d_{sj}**: Sensing distance between Jammer and Beacon source
- **d_{sr}**: Distance between Jammer and Receiver
- **d_{jr}**: Distance between Jammer and Receiver (interference)
Evaluation Methodology (II)

• Receiver:
  – Optimal receiver, i.e. dedicated Rf receiver (BLE Nano) for each BLE Adv. channel,
  – Every packet is logged (+CRC packets) using *Nordic Sniffer* and written to PCAP file for post-analysis in MATLAB,

• Sender:
  – Commercial beacon (Gigaset G-Tag)
    • Adv. interval of 1 sec + all 3 Adv channels
Evaluation Methodology (III)

- We set-up an outdoor experiment:
  - Beacon source, jammer and receiver are put on a line elevated by 1 m from the ground (grass field),
  - Distance between beacon source and the receiver was set to $d_{sr}=3.7$ m,
  - The distance between the jammer and receiver ($d_{jr}$) nodes were varied from 1 to 10 meters.
Results

- At $d=76$ cm the ASR is zero, i.e. jammer successfully jam each transmitted BLE adv. frame transmitted on each channel (37, 38 and 39),
- At $d=100$ cm the ASR=3%,
- Note: TX power of jammer was just 4 dBm.
Countermeasures

• We can divide countermeasures into two categories

  1. Attack Detection
     - Detect the presence of the jammer to allow further actions to be taken, e.g. removal of jammer,
     - Decoy packets & K-mean clustering

  2. Attack Mitigation
     - Actions that limit the impact of the jammer.
Countermeasures – Attack Mitigation

• **Use random channel hopping**
  – Our jammer cannot adapt to random hopping pattern, i.e. adv. channels are used in random order,
  – But, we can use three jammer nodes, each configured to listen on a particular channel => no hopping required.

• **Use randomized device addresses** for BLE beacons,

• **Use of short BLE frames**
  – Our jammer’s ability to jam is limited by its reaction time, i.e. 174 µs, => BLE payloads > 19 bytes,
  – But, the two most popular beacon protocols *iBeacon* and *Eddystone* both have larger payloads.
Conclusions & Future Work

• Can we build a low-cost, energy-efficient selective BLE jammer?
  – Yes, we can (with some limitations)
• Due to the low effort necessary, potential victims should anticipate jamming attacks
  – Especially if they have a commercial interest in their beacon network (e.g. retailers)
• Ongoing research: how to deal with BLE beacons whose device addresses is randomized.