Proximity detection with single-antenna IoT devices

Timothy J. Pierson, Travis Peters, Ron Peterson, David Kotz
Dartmouth College
October 2019
Billions of IoT devices are projected to be deployed in the next few years

- Huge growth projected for connected devices
- Many devices are likely to have limited user interfaces
- Devices that have never met will need to communicate
- No root of trust between newly encountered devices
Proximity can serve as a basis of trust when devices are first encountered.

- Assume adversary is not able to gain close physical proximity to devices (e.g., does not break into a home to gain proximity).

- Proximity can then serve as a basis for trust.

- Techniques exist for multi-antenna devices to detect proximity\(^1,2\).

- No proximity techniques exist for single-antenna devices.

---


We can use repeating portions of the Wi-Fi preamble Long Training Field (LTF) for proximity

**Wi-Fi preamble**¹

<table>
<thead>
<tr>
<th>Short Training Field</th>
<th>Long Training Field</th>
<th>Signal Field</th>
<th>Frame data</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 + 8 = 16 µs</td>
<td>10 × 0.8 = 8 µs</td>
<td>2 × 0.8 + 2 × 3.2 = 8.0 µs</td>
<td>0.8 + 3.2 = 4.0 µs</td>
</tr>
<tr>
<td>10 × 0.8 = 8 µs</td>
<td>2 × 0.8 + 2 × 3.2 = 8.0 µs</td>
<td>0.8 + 3.2 = 4.0 µs</td>
<td>0.8 + 3.2 = 4.0 µs</td>
</tr>
<tr>
<td>10 identical short training symbols</td>
<td>64-sample portions of the LTF</td>
<td>SIGNAL</td>
<td>Data 1</td>
</tr>
<tr>
<td>GI2</td>
<td>GI</td>
<td>GI</td>
<td>GI</td>
</tr>
</tbody>
</table>

- **T₁** and **T₂** are identical 64-sample portions of the preamble Long Training Field (LTF) used for fine frequency correction and channel estimation.
- **T₁** and **T₂** are expected to match at the receiver (plus noise).
- All Wi-Fi receivers, even single-antenna devices, evaluate **T₁** and **T₂**.

---

[¹] Institute of Electrical and Electronics Engineers. 802.11n standard. Online at http://standards.ieee.org
Near-field effects can cause mismatches in the repeating portions of the LTF

- In reactive and radiating near-field regions around a transmitter, electric and magnetic fields not yet aligned
- Fields form a vector that rapidly rotates in time in a plane parallel to the direction of propagation\(^1\)
- Rotation causes mismatches between \(T_1\) and \(T_2\)
- With Wi-Fi, near-field effects extend to roughly 14 cm from transmitter

---

\(R_1 = 0.62 \sqrt{D^3/\lambda}\)

\(R_2 = 2D^2/\lambda\)

---

\(l_t = \) length of transmitting antenna
\(\lambda = \) wavelength
\(D = \) length of transmitting antenna + length of receiving antenna
\(R_1 = \) estimated range of reactive near-field region
\(R_2 = \) estimated range of radiating near-field region

$T_1$ and $T_2$ mismatch at close range, but not at long range

- Rotating electric and magnetic fields at close range cause mismatch between $T_1$ and $T_2$
- Rotation dies out quickly as range increases
- Stable electric and magnetic field orientation at long range ($\approx 14$ cm) results in matching $T_1$ and $T_2$
- Matching not affected by moving objects due to 6.4 $\mu$s time between $T_1$ and $T_2$

Proximity is detected if the mismatch is above a fixed threshold

- \(A_t\) is the sum of the Euclidean distance between \(T_1\) and \(T_2\) over all 64 subcarriers
- \(A_t\) is high at close range, low at long range
- Declare proximity if \(A_t\) is above a fixed threshold
- Proximity determined with high probability at close range
- Proximity beyond 14 cm never falsely detected
- Four different antenna types perform similarly
Proximity detection with single-antenna IoT devices

Timothy J. Pierson, Travis Peters, Ron Peterson, David Kotz
Dartmouth College
October 2019

Questions, contact Tim Pierson: tjp@cs.dartmouth.edu

This research was supported by NSF award CNS-1329686.

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.

Trustworthy Health and Wellness – THaW.org