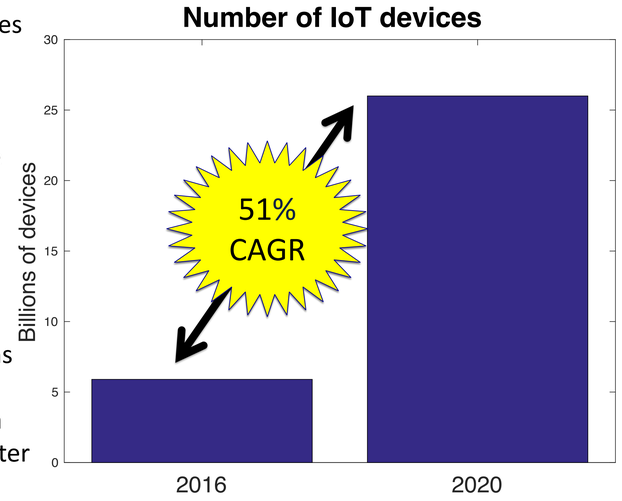
Proximity Detection with Single-Antenna IoT Devices

Timothy J. Pierson, Travis Peters, Ronald Peterson, and David Kotz
Department of Computer Science, Dartmouth College, Hanover, NH, USA 03755

Internet of Things (IoT) devices may frequently encounter new devices

- Analysts predict billions of IoT devices will be deployed in the near future[1]
- IoT devices are envisioned to share data among themselves
- Some shared data may be privacy sensitive or have security implications
- With billions of devices deployed, a device may encounter dozens of new devices every day



Proximity can be a basis for trust when devices are first encountered

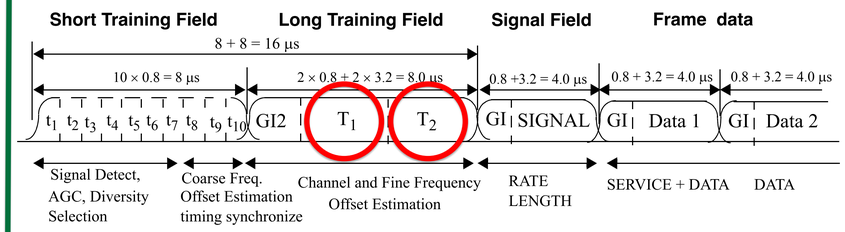
- Assume an adversary is not able to gain close physical proximity to devices (e.g., adversary does not break into a home to gain physical proximity)
- Proximity can then serve as a basis for trust
- Techniques exist for multi-antenna devices to detect proximity
- No proximity techniques exist for single-antenna devices

Distant adversary

Nearby legitimate devices

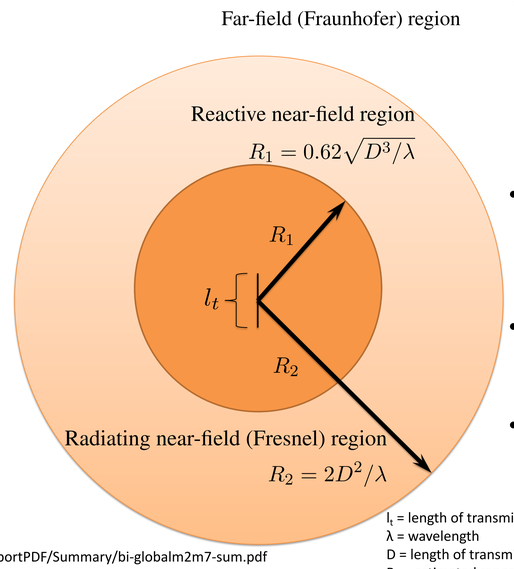
Use repeating portions of Wi-Fi Long Training Field (LTF) for proximity

Wi-Fi Preamble



- T_1 and T_2 are identical 64-sample portions of the Long Training Field in the Wi-Fi preamble[2]
- Repeated LTF portions T_1 and T_2 are used for channel estimation
- T_1 and T_2 are expected to match at the receiver (plus noise)
- All Wi-Fi receivers must evaluate T_1 and T_2
- Even single-antenna devices can measure T_1 and T_2

Near-field effects can cause mismatches in the repeating LTF

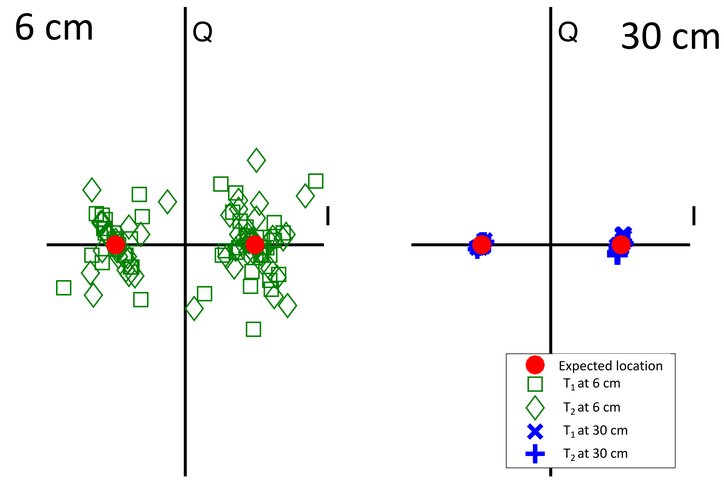


- In the reactive and radiating near-field regions around a transmitter, the electric and magnetic fields are not yet aligned
- Fields form a vector that rapidly rotates in time in a plane parallel to the direction of propagation[3]
- Rotation causes mismatches between T_1 and T_2
- With Wi-Fi, near-field effects extend to roughly 14 cm from transmitter

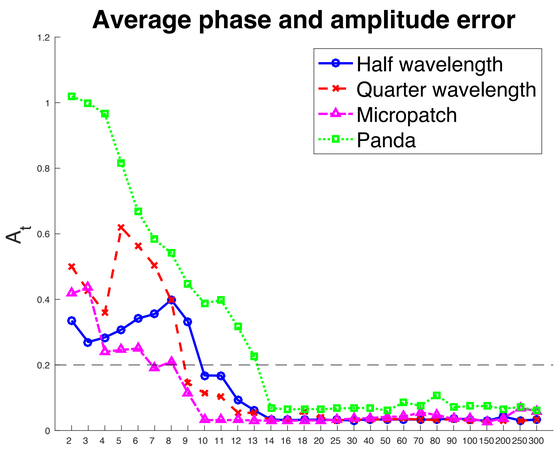
l_t = length of transmitting antenna
λ = wavelength
D = length of transmitting antenna + length of receiving antenna
R_1 = estimated range of reactive near-field region
R_2 = estimated range of radiating near-field region

Repeating portions mismatch at close range, but not at long range

T_1 and T_2 on all Wi-Fi subcarriers



Proximity is detected if the mismatch is over a fixed threshold



Average A_t of 1,000 frames transmitted from each antenna type shown

- 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

National Science Foundation
Award CNS-1329686

CAGR = Compound Annual Growth Rate

[1] Berg Insight. *Wireless IoT connectivity technologies and markets.* Online at http://www.berginsight.com/ReportPDF/Summary/bi-globalm2m7-sum.pdf
[2] Institute of Electrical and Electronics Engineers. 802.11n standard. Online at http://standards.ieee.org
[3] Constantine A. Balanis. Antenna Theory: Analysis and Design. Wiley, third edition, 2005