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

- Analysts predict billions of IoT devices will be deployed in the near future
- 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

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

- T1 and T2 are identical 64-sample portions of the Long Training Field in the Wi-Fi preamble
- Repeated LTF portions T1 and T2 are used for channel estimation
- T1 and T2 are expected to match at the receiver (plus noise)
- All Wi-Fi receivers must evaluate T1 and T2
- Even single-antenna devices can measure T1 and T2

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
- Rotation causes mismatches between T1 and T2
- With Wi-Fi, near-field effects extend to roughly 14 cm from transmitter

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

T1 and T2 on all Wi-Fi subcarriers

Proximity is detected if the mismatch is above a fixed threshold

Average phase and amplitude error

- A is the sum of the Euclidean distance between T1 and T2 over all 64 subcarriers
- A is high at close range, low at long range
- Declare proximity if A is above a fixed threshold

National Science Foundation Award CNS-1329686