Poster: Proximity Detection with Single-Antenna IoT Devices

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

ABSTRACT

Close physical proximity among wireless devices that have never shared a secret key is sometimes used as a basis of trust. In these cases, devices in close proximity are deemed trustworthy while more distant devices are viewed as potential adversaries. Because radio waves are invisible, however, a user may believe a wireless device is communicating with a nearby device when in fact the user's device is communicating with a distant adversary. Researchers have previously proposed methods for multi-antenna devices to ascertain physical proximity with other devices, but devices with a single antenna, such as those commonly used in the Internet of Things, cannot take advantage of these techniques.

We investigate a method for a single-antenna Wi-Fi device to quickly determine proximity with another Wi-Fi device. Our approach leverages the repeating nature Wi-Fi's preamble and the characteristics of a transmitting antenna's *near field* to detect proximity with high probability. Our method never falsely declares proximity at ranges longer than 14 cm.

ACM Reference Format:
Timothy J. Pierson, Travis Peters, Ronald Peterson, David Kotz . 2018. Poster: Proximity Detection with Single-Antenna IoT Devices. In *The 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), October 29-November 2, 2018, New Delhi, India*. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3241539.3267751

1 INTRODUCTION

People and the devices they wear or carry may soon encounter dozens, possibly hundreds, of new devices each day if predictions about the Internet of Things (IoT) come true. These IoT devices are envisioned to share data and actuator control information among themselves, and some of that information may be privacy sensitive or have security implications. This situation suggests that devices that have never met, nor shared a secret, must somehow have a way to securely communicate.

Researchers have previously proposed using physical proximity as a basis of trust between devices that have not met [2, 4, 5]. The idea is that a user is able to bring legitimate devices within a few centimeters of each other, at least temporarily, whereas an adversary is assumed to be unable to come into such close proximity (e.g., an adversary does not break into a home to gain close physical access to devices). The physical proximity between legitimate devices then forms a basis of trust. A distant adversary, however, may attempt to trick a user's devices into accepting a malicious wireless payload by impersonating a legitimate device.

To prevent such an attack, researchers have proposed using multiple antennas to simultaneously measure signal strength to determine proximity [2, 5]. Single-antenna IoT devices, however, cannot use these techniques.

Here we present a novel method for a single-antenna Wi-Fi device to quickly determine when it is in close proximity to a transmitting antenna. Our technique leverages the repeating nature Wi-Fi's preamble and the characteristics of a transmitting antenna's *near field* (i.e., the region physically close to the antenna) to detect proximity with a transmitter. When a receiving device is physically close to a transmitter, near-field effects will cause repeated portions of the preamble to differ in phase and amplitude, whereas when the device is far from the transmitter, the repeated portions of the preamble will be received with a consistent phase and amplitude. We use the presence or absence of phase and amplitude mismatches to determine proximity.

2 WI-FI PREAMBLE

Wi-Fi frames begin with a physical (PHY) layer preamble to aid in synchronizing the transmitter and receiver. The format of the PHY layer preamble is shown in Figure 1 and consists of a Short Training Field (STF) followed by a Long Training Field (LTF).

The STF is used by the receiver for frame detection, automatic gain control, coarse frequency offset estimation, and rough symbol timing synchronization. The

MobiCom '18, October 29-November 2, 2018, New Delhi, India

ACM ISBN 978-1-4503-5903-0/18/10.
https://doi.org/10.1145/3241539.3267751

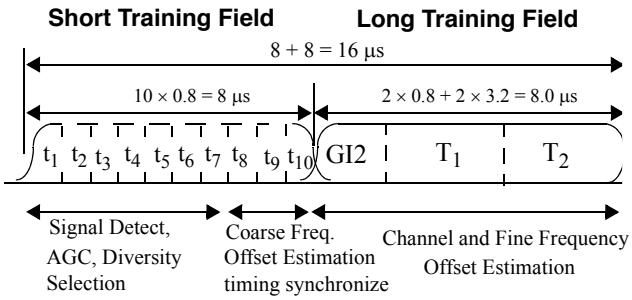

Figure 1: Wi-Fi frames begin with a PHY layer preamble that contains a Short Training Field (STF) and a Long Training Field (LTF). The LTF includes two identical 64-sample symbols denoted T_1 and T_2 [3].

LTF is used for channel estimation and fine frequency offset correction. It consists of a 32-sample guard interval denoted GI2, followed by two identical pre-defined 64-sample OFDM symbols denoted T_1 and T_2. Because T_1 and T_2 are identical, the phase and amplitude of sample i in symbol T_1 matches the phase and amplitude of sample $i+64$ in T_2, where $i = 0 \ldots 63$. This relationship between samples is shown in Figure 2.

The repeating nature of T_1 and T_2 in the LTF allows the receiver to estimate channel effects. The channel can be mathematically expressed as [7]

$$\mathbf{y}[i] = \mathbf{H}\mathbf{x}[i] + \mathbf{w}[i] \tag{1}$$

where $\mathbf{y}[i]$ is the i^{th} received sample, $\mathbf{H}$ represents changes to the signal caused by the channel, $\mathbf{x}[i]$ is i^{th} the transmitted sample and $\mathbf{w}[i]$ is noise received with sample i. Neglecting noise, the result is that received sample $\mathbf{y}[i]$ in T_1 still matches sample $\mathbf{y}[i+64]$ in T_2 in phase and amplitude, even though they no longer match transmitted $\mathbf{x}[i]$ and $\mathbf{x}[i+64]$ due to the effects of $\mathbf{H}$.

The matching of corresponding samples in T_1 and T_2 predicted by Equation (1), however, assumes that the receiver is located in the transmitter's far field. We see next that near-field effects can cause differences in the phase and amplitude of matching LTF samples.

3 NEAR AND FAR FIELDS

The area surrounding a transmitting antenna can be classified into the *near field* and the *far field*. The boundary between these two regions is generally estimated using the following formula [1]

$$R = 2D^2/\lambda \tag{2}$$

where $D = l_t + l_r$ is the combined length of the transmitting antenna, l_t, and the length of the receiving antenna, l_r, and λ is the signal wavelength. In Wi-Fi's 2.4 GHz band, and with quarter-wavelength dipole antennas, this boundary is roughly 6 cm from the transmitter. The boundary between the near field and far field, however, is not sharp, but instead transitions gradually.

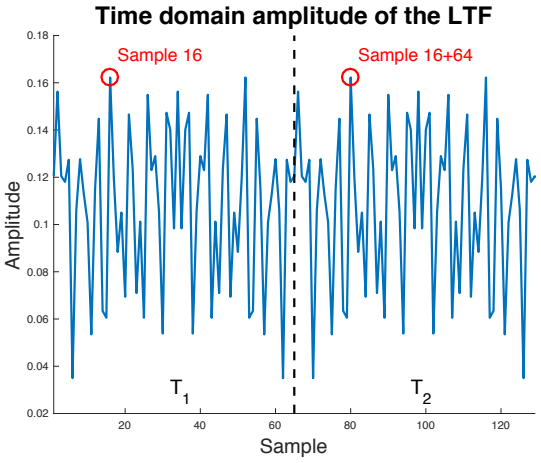

Figure 2: In the time domain, sample i matches sample $i+64$. Here we show sample 16 in T_1 matches sample 80 (16 + 64) in T_2.

In the near field the signal's electric and magnetic fields form a vector that rotates in time in a plane parallel to the direction of propagation, rather than the stable orthogonal relationship seen in the far-field region [1]. Wi-Fi samples taken in the near field can result in different phase and amplitude readings between corresponding samples in the LTF. It can be shown that after roughly 14 cm from the transmitter, near-field effects have attenuated to nearly zero, the electric and magnetic fields do not rotate in time, and corresponding samples in the LTF match as predicted by Equation (1). We use the presence of mismatches to determine proximity.

4 PROXIMITY DETECTION

We transmitted 1,000 Wi-Fi frames from four different types of antennas using BPSK 1/2 encoding on Wi-Fi channel 1 at distances ranging from 2 cm to 3 m. We calculate the total Euclidean distance between the phase and amplitude of subcarriers in T_1 and T_2 as:

$$E_j = \sum_{k=-32}^{31} \Big[(\Re(Y_1[k]) - \Re(Y_2[k]))^2 + (\Im(Y_1[k]) - \Im(Y_2[k]))^2 \Big]^{\frac{1}{2}} \tag{3}$$

where E_j is the total Euclidean distance between the phase and amplitude of all subcarriers k for frame j, Y_x is the result of an FFT over T_x, $\Re(Y_x[k])$ and $\Im(Y_x[k])$ are the real and imaginary components of the phase and amplitude of each subcarrier k in Y_x, for $x \in \{1, 2\}$. We

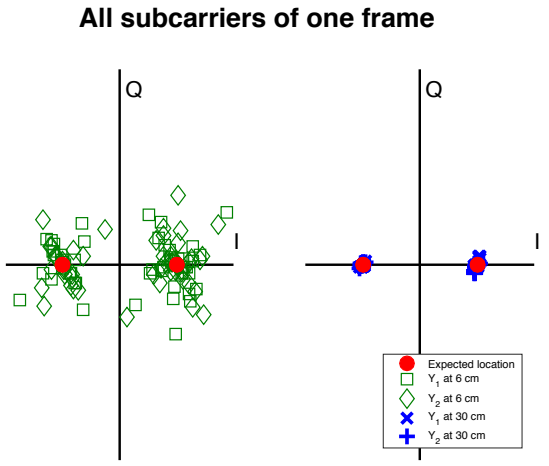

Figure 3: Y_1 and Y_2 match at long (30 cm) range, but do not match at close (6 cm) range.

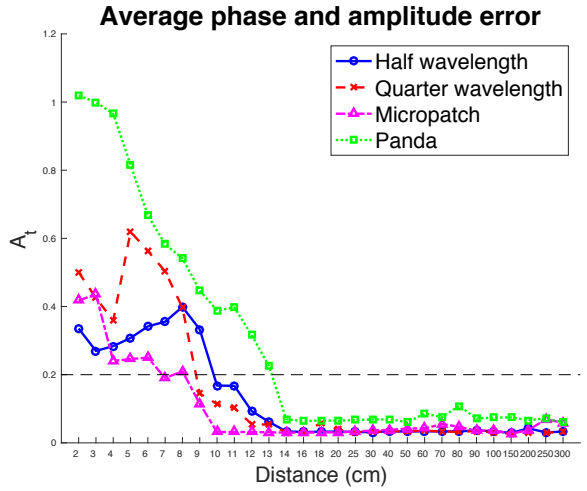

Figure 4: Average preamble error, A_t, by distance and antenna type for 1,000 Wi-Fi frames.

call this difference E_j the *preamble error* of a frame. If the receiver is in the transmitter's near field, mismatches between T_1 and T_2 will result in a large preamble error. If the receiver is in the far field, T_1 and T_2 will match (except for noise) and the preamble error will be small.

Figure 3 shows difference between Y_1 and Y_2 for all subcarriers of one frame. We see at 30 cm Y_1 and Y_2 match for all subcarriers, but at 6 cm many subcarriers do not match. Figure 4 shows the average preamble error for 1,000 frames sent at distances ranging from 2 cm to 3 m for four different antenna types. As expected, the average preamble error is large at close range and small at long range for each antenna type.

We use the data from Figure 4 to make a proximity determination. We set a threshold, $\tau = 0.2$, where if the preamble error is greater than τ, the single antenna device declares proximity, otherwise it does not. At close range this method determines proximity with high probability and never falsely declares proximity over 14 cm.

5 RELATED WORK

Exploiting the repeating nature of Wi-Fi OFDM preambles for proximity detection has not been explored in the literature. Work thus far has focused on covertly embedding a small amount of data into the Wi-Fi frame using PHY layer techniques. For example, Rahbari and Krunz proposed a technique called *P-modulation* to modulate the STF to include up to eight user-chosen bits in a Wi-Fi preamble [6]. These bits can be used to inform other devices of the transmitter's status, possibly eliminating the need for additional control frames. This technique, however, is different from ours in that we use the repeating nature of the LTF to establish proximity, not to include a small number of indicator bits.

6 CONCLUSION

In this poster we demonstrate that a single-antenna device can reliably determine when it is in close proximity to a transmitting device by leveraging the repeating nature of Wi-Fi's preamble and the physical characteristics of signals in the transmitter's near-field region. We focused our testing on dipole and micropatch antennas because they are the most common antennas used in consumer devices, but there are a myriad of other types of antennas that we may test in the future. We believe, however, that our work here is a starting point and opens an important new area of research that warrants further investigation.

REFERENCES

[1] Constantine A. Balanis. *Antenna Theory: Analysis and Design.* Wiley, third edition, 2005.
[2] Liang Cai, Kai Zeng, Hao Chen, and Prasant Mohapatra. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In *Proceedings of NDSS*, 2011.
[3] Institute of Electrical and Electronics Engineers. 802.11n standard, https://www.ieee.org, visited 7/20/2018.
[4] Suhas Mathur, Rob Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. ProxiMate: Proximity-based Secure Pairing using Ambient Wireless Signals. In *Proceedings of MobiSys*, pages 211–224. ACM, June 2011.
[5] Timothy J. Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Wanda: securely introducing mobile devices. In *Proceedings of INFOCOM*, pages 1–9. IEEE, April 2016.
[6] Hanif Rahbari and Marwan Krunz. Exploiting frame preamble waveforms to support new physical-layer functions in OFDM-based 802.11 systems. *IEEE Transactions on Wireless Communications*, 16(6):3775–3786, June 2017.
[7] David Tse and Pramod Viswanath. *Fundamentals of wireless communication.* Cambridge University Press, 2005.