Precise Power Delay Profiling with Commodity Wi-Fi

Yaxiong Xie, Zhenjiang Li, Mo Li
Communication is Sensing
Resolution of Power Delay Profile

Power Delay Profile

Power Intensity

Time

$\tau$
Resolution of Power Delay Profile

Power Delay Profile

Time

Power Intensity

$t_0$, $t_1$, $t_2$, $t_3$, $t_4$, $\tau$
Resolution of Power Delay Profile

Power Delay Profile with 2x resolution
The resolution is decided by the **signal bandwidth**

- Wider bandwidth leads to higher resolution

**Channel bandwidth of commodity Wi-Fi is regulated by the 802.11 protocol**

<table>
<thead>
<tr>
<th>Physical layer</th>
<th>Maximum bandwidth</th>
<th>Time resolution $\tau$</th>
<th>Distance resolution $\epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 a/g</td>
<td>20MHz</td>
<td>50ns</td>
<td>15m</td>
</tr>
<tr>
<td>802.11 n</td>
<td>40MHz</td>
<td>25ns</td>
<td>7.5m</td>
</tr>
</tbody>
</table>
The resolution is decided by the **signal bandwidth**

- **Wider** bandwidth leads to **higher** resolution

**Channel bandwidth of commodity Wi-Fi is regulated by the 802.11 protocol**

<table>
<thead>
<tr>
<th>Physical layer</th>
<th>Maximum bandwidth</th>
<th>Time resolution $\tau$</th>
<th>Distance resolution $\epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 a/g</td>
<td>20MHz</td>
<td>50ns</td>
<td>15m</td>
</tr>
<tr>
<td>802.11 n</td>
<td>40MHz</td>
<td>25ns</td>
<td>7.5m</td>
</tr>
</tbody>
</table>

**Can we do better?**
Observation

2.4GHz

5GHz

160MHz

200MHz

100MHz
# Goal: breaking the **bandwidth limit** of Commodity Wi-Fi devices and deriving a **high resolution** Power Delay Profile
Availability on Commodity Wi-Fi devices

Not available from commodity Wi-Fi devices

✓ But CSI is reported from Wi-Fi NICs

It can be derived from CSI via iFFT
Availability on Commodity Wi-Fi devices

Not available from commodity Wi-Fi devices

✓ But CSI is reported from Wi-Fi NICs

It can be derived from CSI via iFFT

\[ f_n - f_1 \]

High resolution Power Delay Profile

= Wideband CSI
CSI splicing
Our Solution

CSI splicing

Intensity dB

frequency
Our Solution

CSI splicing

Intensity dB

frequency

Channel Center Frequency (GHz)
Our Solution

CSI splicing

![Diagram showing frequency and intensity with CSI splicing labels and values]
Our Solution

CSI splicing

3x bandwidth $\rightarrow$ 3x resolution enhancement
Challenges

#1 CSI measurement errors
- Channel and hardware will contribute to the reported CSI value
- We must eliminate the impact from hardware

#2 Stringent timing requirements
- Wireless channel is time-varying
- CSI must be collected within channel coherence time
Challenges

#1 CSI measurement errors

#2 Stringent timing requirements
CSI measurement error

Preliminary Experiment

- Atheros 9580 NICs
- 5 CSI from each individual channel
- 10 continuous Wi-Fi channels at 2.4GHz
Let’s look at the amplitude first!
However, the phase of measured CSI ...
PHASE vs FREQUENCY
Measurement error prohibit us from directly splicing them!
CSI estimation in PHY

The phase of wi-fi signal will be changed after it goes through the channel.
CSI estimation in PHY

\( f_s \) and \( f_r \) is the sampling frequency of the sender and receiver

\[
\lambda_o = \frac{f_s}{f_r} - 1
\]
Packet boundary detection shift $\tau_b$

$$\lambda_b = \frac{2\pi}{N} \cdot \tau_b$$
CSI estimation in PHY

It is caused by residual central frequency offset
We denote it as $\beta$
CSI estimation in PHY

It is caused by residual central frequency offset
We denote it as $\beta$
CSI estimation in PHY

It is caused by residual central frequency offset
We denote it as $\beta$

CSI describes signal distortion introduced by channel + hardware
Reported CSI phase value $\phi_k$ can be expressed as:

$$\phi_k = \theta_k + k \cdot (\lambda_b + \lambda_o) + \beta$$

- $\theta_k$ is the phase rotation due to channel propagation (ground truth)
- $k$ is the subcarrier index (known)
- $\lambda_b$ is the phase errors introduced by packet boundary detection shift
- $\lambda_o$ is the phase errors introduced by sampling frequency offset
- $\beta$ is the phase errors introduced by central frequency offset
Phase error $\beta$

- Caused by residual central frequency offset

Observation

- It has NO impact on the derived power delay profile

Problem is simplified

- No need to know the exact $\beta$

\[
\phi_k = \theta_k + k \cdot (\lambda_b + \lambda_o) + \beta
\]

\[
\gamma_k = \theta_k + \beta
\]

\[
\phi_k = \gamma_k + k \cdot (\lambda_b + \lambda_o)
\]
Phase error correction

Phase error $\lambda_b$

✓ Caused by packet boundary detection shift

Observation

✓ Zero mean Gaussian distribution $N(0, \sigma^2)$

Solution

✓ Averaging over multiple CSI measurements

$$\phi_k = \gamma_k + k \cdot (\lambda_b + \lambda_o)$$

$$\overline{\lambda_b} = 0$$

$$\phi_k = \gamma_k + k \cdot \lambda_o$$
Phase error $\lambda_o$

✓ Caused by sampling frequency offset

Observation

✓ Sampling frequency offset keeps stable in the order of minutes

✓ $\lambda_o$ is a constant across multiple CSI measurement and across different channel
Phase error correction

Solution

✓ Observation: power delay profile derived using different wi-fi channel should be the same
✓ Search the best value of $\lambda_o$
✓ With stable multipath distribution, correct $\lambda_o$ will maximize the similarity between the PDP derived from two Wi-Fi bands
Challenges

• #1 CSI measurement errors

• #2 Stringent timing requirements
**Assumption:** the channel is stable during the CSI measurement

**Wireless channel is time-varying in natural**

✓Channel coherence time

**Constraint:** one round of CSI measurement must be finished within coherence time
High quality phase error correction

Requirement: enough CSI must be collected on each individual channel

Problem: we may not able to scan the whole frequency band.
Tradeoff

- Error compensation quality
- Total bandwidth we can scan

Formulated as an optimization problem
Evaluation
Experiment Setting

**Wi-Fi devices**
- TP-link N750 Wi-Fi routers
- Atheros 9580 NIC

**Software**
- Modified driver
- CSI value for each individual subcarrier is reported
  - CSI tool using Intel 5300 only reports 30 out of 56/114 subcarriers

**Scenarios**
- Lab office
- Corridor
- Car park
- Lecture Hall
Ranging with Power Delay Profile
- Received signal strength of direct path
- Path loss model

High resolution Power Delay Profile $\rightarrow$ accurate ranging result
Ranging error as metric
Phase Error Correction

Experiment:
Ranging using raw CSI, CSI after removal of $\lambda_b$ and CSI after removal of $\lambda_b \lambda_o$

- 10.7m without compensation
- 6.3m after removal of $\lambda_b$
- 4.3m after removal of $\lambda_b \lambda_o$
Experiment:

Ranging using CSI with different bandwidth

Splicer-120MHz outperforms Splicer-20MHz by **22.7%** on average

Splicer-200MHz outperforms Splicer-20MHz by **55.5%** on average
Case Study: indoor localization

**CUPID**: a single AP indoor localization system

![Diagram showing a single AP and three devices A, B, and C with distances and angles labeled.](image)

- **Signal Strength (dB)**
- **Power Delay Profile**
- **Direct Path**

Diagram showing the localization system setup with distances $d_A$, $d_B$, and $d_{AB}$, angles $\theta_A$ and $\theta_B$, and a time scale with points $t_1$, $t_2$, $t_3$, ..., $t_n$.
Case Study: indoor localization

**Splicer-CUPID:** use the high resolution Power Delay Profile as input and leave the rest of system unchanged

- 7.9m for CUPID
- 2.3m for Splicer-CUPID at speed of 1m/s
- Reduce to **0.95m** with 5AP
Conclusion

Splicer

✓ A system that can deliver precise power delay profile on commodity Wi-Fi devices

✓ Leverages the CSIs from individual Wi-Fi bands to obtain the CSI of an equivalent wider Wi-Fi band after splicing

✓ Benefits massive applications based on PDP or CSI
Thank you!

&

Questions?