Indoor navigation using WiFi round-trip time

Berthold K.P. Horn

- Fine Time Measurement (FTM) Round Trip Time (RTT)
- IEEE 802.11mc
- Background: Timing Advance (TA) in GSM and LTE
- Recovering initiator position from distances to responders
- Dilution of Precision (DOP) — a.k.a. Noise Gain
- Non-Gaussian, non-stationary measurement error
- Best spatial arrangement for responders
- Some issues, problems, and current limitations
- When will it happen?
Here, we made you a maze!
What’s is indoor location good for?

- **Navigation:** Turn-by-turn wayfinding. Show me the way to the meeting.
- **Asset Management:** Where is the fork-lift? wheel-chair? ultra-sound machine?
- **Location based marketing:** Alert consumer to nearby item or trigger coupon.
- **Emergency Services:** Locate situation within building. Civic address and floor.
- **Internet of Things:** Dim the light in the room I am in. Lock the correct door.
- **Warehousing and robotics:** Guide autonomous forklifts.
- **Network management:** Pinpoint equipment failures and activate replacements.
- **Smart cities:** Public parking structures, street lighting, security cameras.
- ...
Background: Timing Advance in cellular networks

- Timing Advance in GSM
- Timing Advance in LTE

Both use time-division duplex (TDD)

Unlike CDMA which uses code-division duplex (CDD)
VoLTE 310:260 12870:21878274 (0x14DD602) NW
VoLTE voice connection (GSM) \nLTE EARFCN 2250 TA * LTE 00 00 00 12 \nGPS 21.33276 -157.92477 alt 9 /
acc 17 vel 0.0 azi -1 Sat 0/22 |
BASE N/A \nGSM 21.34093 -157.92948 s 1523 R L 0:0 /
LTE 21.34093 -157.92948 s 1523 R I
IP 192.0.0.4 136.22.79.149 -
BAT 68% 3.93 V 37 C (SIM: T-Mobile) -
LTE 310:260 12870:21878274 (0x14DD602) 90 \nLTE SS 19 RP -103 RQ -11 SN 30.0 CQ * (S) -
Device DOES support WIFI RTT
Background: using Received Signal Strength:

- Estimate distance based on RSSI (dBm)

  Does signal strength obey the inverse square law?

- “Fingerprinting” a venue

  Tedious. Repeat when access point configuration changes
Use RSSI?

- Horizontal axis: actual distance (meter)
- Vertical axis: signal strength (dBm)
- Green line: linear fit \(-53 - 3.7 \times R \text{ dBm}\)
- Red curve: expected \(-50 - 20 \times \log(R) \text{ dBm}\)
802.11mc

- Fine Time Measurement (FTM)
- Round Trip Time (RTT)
WiFi 802.11mc

PHONE

TIME

ACCESS POINT (AP)

FTM: Fine Timing Measurement

2 * distance = ((t4-t1) - (t3-t2)) * c

t total round trip
t turnaround time
Burst Size: B (typically = 8)
Burst Successes: N (where N > 0, N < B)

Distance Mean: \( \frac{\sum \text{distance}[i]}{N} \)
Distance Variance: \( \frac{\sum \text{distance}[i]^2}{N} - (\text{mean})^2 \)
Clients range relative to APs/beacons

But how does that relate to ‘location’?

- Requires knowledge of AP locations
- Requires a map with frame of reference
get permissions: ACCESS_FINE_LOCATION, CHANGE_WIFI_STATE

register BroadcastReceiver for: SCAN_RESULTS_AVAILABLE

Call WifiManager.ScanStart(...)

   receive ScanResults in BroadcastReceiver
   create RangingRequest from ScanResults

Call WifiRttManager.startRanging(...)

RangingResultsCallback onRangingResults

† Throttled to 4 calls per 2 minutes (and “grey listed”)
‡ Disabled when app is in background
<table>
<thead>
<tr>
<th>ID</th>
<th>MAC Address</th>
<th>Delay (d)</th>
<th>Time (s)</th>
<th>TTL</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>b8:08:cf:a0:8b:f6</td>
<td>-55</td>
<td>-3.33</td>
<td>0.40</td>
<td>36811</td>
</tr>
<tr>
<td>1</td>
<td>b8:08:cf:a0:88:04</td>
<td>-88</td>
<td>1.94</td>
<td>0.41</td>
<td>36812</td>
</tr>
<tr>
<td>2</td>
<td>b8:08:cf:a0:7a:ad</td>
<td>-80</td>
<td>4.58</td>
<td>0.35</td>
<td>36813</td>
</tr>
<tr>
<td>3</td>
<td>b8:08:cf:a0:7a:00</td>
<td>-82</td>
<td>3.90</td>
<td>0.59</td>
<td>36814</td>
</tr>
<tr>
<td>4</td>
<td>b8:08:cf:a0:7a:a3</td>
<td>-106</td>
<td>5.31</td>
<td>2.07</td>
<td>36815</td>
</tr>
<tr>
<td>5</td>
<td>38:8b:59:c4:f0:a0</td>
<td>-58</td>
<td>4.02</td>
<td>0.23</td>
<td>google@...</td>
</tr>
<tr>
<td>6</td>
<td>38:8b:59:c4:f3:55</td>
<td>-76</td>
<td>8.80</td>
<td>0.06</td>
<td>google@...</td>
</tr>
<tr>
<td>7</td>
<td>38:8b:59:c4:f7:ee</td>
<td>-87</td>
<td>11.22</td>
<td>0.16</td>
<td>google@...</td>
</tr>
<tr>
<td>8</td>
<td>4c:ed:fb:b7:5a:3c</td>
<td>-76</td>
<td>7.95</td>
<td>0.13</td>
<td>ASUS_38...</td>
</tr>
<tr>
<td>9</td>
<td>0c:9d:92:b5:c4:1c</td>
<td>-81</td>
<td>7.95</td>
<td>0.09</td>
<td>ASUS_18...</td>
</tr>
</tbody>
</table>
FTMRTT • 10 RTT responses from 16 APs

0 dBm: -56 dis: 3.03 s: 0.24 "ASUS_38_5G"
1 dBm: -85 dis: 5.34 s: 0.20 "ASUS_18_5G"
2 dBm: -77 dis: 5.87 s: 0.42 "google@176"
3 dBm: -73 dis: 2.12 s: 0.28 "🐱 36813"
4 dBm: -88 dis: -0.53 s: 0.57 "🐶 36814"
5 dBm: -91 dis: 8.17 s: 0.95 "🐱 36815"
6 dBm: -89 dis: 10.95 s: 1.10 "google@176"
7 dBm: -91 dis: 12.97 s: 0.28 "google@176"
8 dBm: -92 dis: 6.22 s: 1.60 "🐱 36811"
9 dBm: -102 dis: 2.95 s: 4.71 "🐱 36812"

Signal Spy

Mobile Network: US Cellular LTE - Band 5 (85..
Connected to WIFI (google@176)

WiFi Guard • 4d
Solution Methods

\[ \|s - r_i\| = d_i \quad \text{for} \quad i = 1, 2, \ldots n \]

$s$ is the unknown position of the initiator, and $d_i$ is the measured distance to the responder at $r_i$.

- Intersecting spheres (or circles)
- Reduction to linear equations & pseudo inverse
- Least squares & gradient descent
- Brute force grid search
- Extended Kalman filter — linearization & assumption
- Bayesian grid — transition & observation models
Reduction to Linear Equations

\[ \| \mathbf{s} - \mathbf{r}_i \| = d_i \]
\[ (\mathbf{s} - \mathbf{r}_i) \cdot (\mathbf{s} - \mathbf{r}_i) = d_i^2 \]
\[ \| \mathbf{s} \|^2 - 2 \mathbf{r}_i \cdot \mathbf{s} + \| \mathbf{r}_i \|^2 = d_i^2 \]

So we have \( n \) second order equations in \( \mathbf{s} \).
Subtract pairwise to obtain \( m = n(n - 1)/2 \) linear equations:

\[ (\mathbf{r}_j - \mathbf{r}_i) \cdot \mathbf{s} = \frac{(d_i^2 - d_j^2) - (R_i^2 - R_j^2))}{2} \]

where \( R_i = \| \mathbf{r}_i \| \). We can rewrite this in matrix-vector form:

\[ A \mathbf{s} = \mathbf{t} \]

For \( n = 3 \) we get three \textit{linearly dependent} equations.
For \( n > 3 \) can obtain least squares solution:

\[ \mathbf{s} = (A^T A)^{-1} A^T \mathbf{t} \]
Reduction to Linear Equations

\[ \| \mathbf{s} - \mathbf{r}_i \| = d_i \]

\[ (\mathbf{s} - \mathbf{r}_i) \cdot (\mathbf{s} - \mathbf{r}_i) = d_i^2 \]

\[ \| \mathbf{s} \|^2 - 2 \mathbf{r}_i \cdot \mathbf{s} + \| \mathbf{r}_i \|^2 = d_i^2 \]

So we have \( n \) second order equations in \( \mathbf{s} \).
Subtract pairwise to obtain \( m = n(n - 1)/2 \) linear equations:

\[ (\mathbf{r}_j - \mathbf{r}_i) \cdot \mathbf{s} = \left( (d_i^2 - d_j^2) - (R_i^2 - R_j^2) \right)/2 \]

where \( R_i = \| \mathbf{r}_i \| \). We can rewrite this in matrix-vector form:

\[ \mathbf{A} \mathbf{s} = \mathbf{t} \]

For \( n = 3 \) we get three linearly dependent equations. For \( n > 3 \) can obtain least squares solution:

\[ \mathbf{s} = (\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T \mathbf{t} \]

BUT: Huge noise gain!
Least Squares and Gradient Descent

Find $\mathbf{s}$ that minimizes sum of squares of errors

$$e = \sum_{i=1}^{n} (\| \mathbf{s} - \mathbf{r}_i \| - d_i)^2$$

Determine the gradient

$$\nabla(e) = 2 \sum_{i=1}^{n} (\| \mathbf{s} - \mathbf{r}_i \| - d_i) \frac{\mathbf{s} - \mathbf{r}_i}{\| \mathbf{s} - \mathbf{r}_i \|}$$

Go downhill

$$\mathbf{r}^{(n+1)} = \mathbf{r}^{(n)} - \gamma \nabla(e)$$

Perhaps better yet, use Newton-Raphson

$$\mathbf{r}^{(n+1)} = \mathbf{r}^{(n)} - H(e)^{-1} \nabla(e)$$

where $H(e)$ is the Hessian matrix of second partial derivatives.
Nature of the measurement “noise”

- Non-Gaussian

- Not “stationary”

- Unknown effects of the environment
Google Wifi 5 GHz band, 80 MHz BW, distances 1, 2, and 3 meters
Horizontal: actual distance (meter)
Vertical: measured distance (meter)

red line: slope 1
green line: slope 1.2 (best fit)
blue line: slope 1.6
Relative Permittivity of Building Materials

<table>
<thead>
<tr>
<th>Material</th>
<th>Permittivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plasterboard</td>
<td>2.02</td>
</tr>
<tr>
<td>Gypsum</td>
<td>2.41 – 2.60</td>
</tr>
<tr>
<td>Plywood</td>
<td>3.67 – 3.81</td>
</tr>
<tr>
<td>Brick</td>
<td>3.88 – 4.62</td>
</tr>
<tr>
<td>Wood</td>
<td>3.92 – 5.89</td>
</tr>
<tr>
<td>Glass</td>
<td>6.06</td>
</tr>
<tr>
<td>Concrete</td>
<td>7.63 – 9.54</td>
</tr>
<tr>
<td>Tissue</td>
<td>28 – 50</td>
</tr>
</tbody>
</table>


Horizontal: actual distance (meter). Vertical: measured distance (meter)
Red line: slope 1, Green line: slope 1.2 (best fit), Blue line: slope 1.6
Dot color code based on actual RSSI minus predicted RSSI
blue = -10dB, green = 0 dB, red = +10 dB
Where RSSI prediction is based on actual distance
Horizontal: actual distance (meter). Vertical: measured distance (meter)
Red line: slope 1, Green line: slope 1.2 (best fit), Blue line: slope 1.6
Dot color code based on actual RSSI minus predicted RSSI
blue = -10dB, green = 0 dB, red = +10 dB
Where RSSI prediction is based on measured distance
Horizontal axis: ratio of true distance to measured distance
Green triangle: observation model for Bayesian update
Bayesian Grid Update

At each time step, measure distances and:

- Apply transition model (random walk), and

- Apply observation model (use Baye’s rule)
Bayesian Grid Update

At each time step, measure distances and:

- Apply transition model (random walk), and
- Apply observation model (use Baye’s rule)

For single position output, compute:

- Maximum likelihood (peak), or
- Expected value (centroid)
Dilution of Precision (noise gain): $\frac{1}{\sin(\theta)}$
Dilution of Precision (noise gain): \( 1/\sin(\theta) \)

Close up (non linear) case
Is the location accuracy high enough?

- 10 m – 20 m  ❌
- 1 m – 2 m  ❓
- 0.1 m – 0.2 m  ✔
Will it “scale”?

• Hundreds at Honolulu Symphony trying to find their seat

• Knock out Google Wifi mesh with FTM RTT “DOS attack”

• Need “passive” “GPS-like” system

• Can be done if APs communicate and broadcast results.

• Unclear if clock synchronization can be accurate enough.
Privacy

• User needs to give app permission
• User needs to enable location services on device
• STA (phone) need not be connected to AP (WiFi)
• AP need not be connected to WLAN (internet)
• MAC address is randomized
• AP cannot determine RTT
• FTM RTT disabled when app is in background
• But: Neighbour Awareness Networking (NAN)?
What is the competition?

- BLE beacons + phased array direction measurement.
- Low cost, low power, small size.
- Not tied into Wifi AP infrastructure
- Will it work?
- Will it work accurately enough?
18,008 WiFi APs (unique global MAC addresses) in Back Bay
<table>
<thead>
<tr>
<th>No RTT responses from 99 APs</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:19:be:29:07:ff</td>
</tr>
<tr>
<td>12:19:be:29:07:ff</td>
</tr>
<tr>
<td>94:91:7f:48:3c:b3</td>
</tr>
<tr>
<td>00:19:be:29:08:07</td>
</tr>
<tr>
<td>12:19:be:29:08:07</td>
</tr>
<tr>
<td>GPS 21.282213 -157.828692</td>
</tr>
</tbody>
</table>
- Broadcom 802.11ac Acculocate Access Point
- Intel® Dual Band Wireless-AC 8260
- Marvell AP-8964 802.11ac 4x4 Wave2 Concurrent Dual Band Access Point
- Mediatek MT663X 802.11abgn/ac Ref. STA
- Qualcomm IPQ4018 802.11ac 2-stream Dual-band, Dual-concurrent Router
- Qualcomm IPQ8065 802.11ac 4-stream Dual-band, Dual-concurrent Router
- Qualcomm Snapdragon™ 820 Development Kit
- Realtek RTL8812BU
236 FTM RTT (802.11mc) responders in Back Bay
WiFi Mesh Systems

- eero home WiFi system (Tri-band mesh WiFi)
- Google Wifi – AC1200
- Netgear Orbi – AC2200 (Tri-band mesh WiFi)
- TP-Link Deco M5 Whole Home Mesh WiFi System?
- Linksys Velop – AC2200 (Tri-band Wifi Mesh System)?
- Ubiquiti AmpliFi HD WiFi System?
- Luma Whole Home Wifi (2 pack)?
- ASUS Lyra Trio – AC1750 (Mesh WiFi System)?
- HTC Managed Wi-Fi Service with Mesh Wifi?
- ...
No RTT responses from 55 APs

Use Wi-Fi

{34:fc:d9:74:59:e1=2402,-66,4s}
{34:fc:b9:77:0e:
81=2437,-57,4s};(11)max=-65,
{34:fc:b9:73:d6:f1=5300,-87,10s}
{40:e3:d6:19:e0:b1=5660,-89,5s}
{34:fc:b9:77:0e:

UHM

[(3)
{34:fc:b9:73:d6:e0=2437,-86,9s}
{34:fc:b9:74:59:e0=2462,-66,4s}
{34:fc:b9:77:0e:
80=2437,-58,4s};(9)max=-68,
{40:e3:d6:19:e0:b0=5660,-89,5s}
{34:fc:b9:76:aa:

DIRECT-CB-HP OfficeJet
Pro 8710

No RTT responses from 55 APs
suo sponte

suo motu
How far along are we?

- Boston Back Bay (July 2018) 236/18008 ≈ 1.3%

- Waikiki (January 2019) 37/1275 ≈ 2.9%

- Google WiFi (January 2019) turned on RTT bit in beacon frame
Everything looks good and 3 Wifi points are online.

Your Google Wifi just got better

Google Wifi installed an update at 1/14/2019, 1:12 PM HST. Here's what's new:
- IPv6: Support for devices on the guest network.
- IPv6 port opening.
- General stability & performance improvements.
Indoor navigation using WiFi round-trip time

Berthold K.P. Horn

- Fine Time Measurement (FTM) Round Trip Time (RTT)
- IEEE 802.11mc
- Background: Timing Advance (TA) in GSM and LTE
- Recovering initiator position from distances to responders
- Dilution of Precision (DOP)
- Non-Gaussian, non-stationary error
- Best spatial arrangement for responders
- Some issues, problems, and current limitations
- When will it happen?
Linear Equations for Four Transponders

With 4 responders we get 6 linear equations. We can chose 3 that are linearly independent:

\[
\begin{pmatrix}
(r_0 - r_1)^T \\
(r_1 - r_2)^T \\
(r_2 - r_3)^T
\end{pmatrix}
\begin{pmatrix}
s_1 \\
s_2 \\
s_3
\end{pmatrix} =
\begin{pmatrix}
t_1 \\
t_2 \\
t_3
\end{pmatrix}
\]

where \( t = (t_{0,1}, t_{1,2}, t_{2,3})^T \) and \( t_{i,j} = ((d_i^2 - d_j^2) - (R_j^2 - R_i^2))/2 \).

Can solve 3 linear equations in 3 unknown components of \( s \) (provided \( r_0, r_1, r_2, \) and \( r_3 \) are not coplanar).
Linear Equations for Four Transponders

With 4 responders we get 6 linear equations. We can choose 3 that are linearly independent:

\[
\begin{pmatrix}
(r_0 - r_1)^T \\
(r_1 - r_2)^T \\
(r_2 - r_3)^T
\end{pmatrix}
s = t
\]

where \( t = (t_{0,1}, t_{1,2}, t_{2,3})^T \) and \( t_{i,j} = ((d_j^2 - d_i^2) - (R_j^2 - R_i^2))/2 \).

Can solve 3 linear equations in 3 unknown components of \( s \). (provided \( r_0, r_1, r_2, \) and \( r_3 \) are not coplanar).

BUT: huge noise gain!
Horizontal axis: actual distance (m)
Vertical axis: measured distance (m)
Open office setting - cubicles
Green line slope 1.2
Blue line slope 1.4
Horizontal axis: reported distance (meter)
Vertical axis: signal strength (dBm)

Green line: linear fit -50 - 3.4 * R dBm
Red curve: expected -50 - 20 * log(R) dBm

Use RSSI?
ASUS RT-ACRH13 BW 80 Mhz PREAMBLE_VHT