Time-based Location Techniques Using Inexpensive, Unsynchronized Clocks in 802.11 Wireless Cards
PinPoint Location System

Matthew Mah
Ashok Agrawala

University of Maryland, College Park

March 25, 2010
Goals for PinPoint Location System

- Meter-level location accuracy for mobile devices
  - 1 \( \mu s \approx 300\text{m} \)
  - 1 ns \( \approx 0.3\text{m} \) (1 ft.)
- Locate both system participants and nonparticipants
- Use inexpensive, off-the-shelf hardware
- Require no synchronization infrastructure
### Location Methods For Wireless Signals

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angle</td>
<td>Triangulation</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>Radio Map</td>
</tr>
<tr>
<td>Time</td>
<td>Trilateration, Hyperbolic Location</td>
</tr>
</tbody>
</table>

- Hybrid systems combine data sources
- Measuring angle of arrival requires special antennas
- Radio maps require extensive calibration

#### Data Source Process

<table>
<thead>
<tr>
<th>Angle Triangulation</th>
<th>Signal Strength Radio Map</th>
<th>Time Trilateration, Hyperbolic Location</th>
</tr>
</thead>
</table>

#### Challenges

- Existing Location Systems
  - Clocks
    - Clock Drift
    - Round Trip Time
    - Time and Clock Offset
    - Nonlinear Clock Behavior

#### PinPoint

- TOA
- TDOA Variants
- Card Delays
- Error Analysis
- Filtering

#### Experimental Results

#### Future Work

#### Questions?
Goals
- Measure time accurately
- Convert times to distance: \( D = c \Delta t \). To simplify notation, use time version of distance \( d = D/c \)
  - Time of Arrival (TOA): \( d(a, b), d(a, q), d(b, q) \)
  - Time Difference of Arrival (TDOA): \( d(b, q) - d(a, q) \)

Challenges
- Existing Location Systems
  - Clocks
    - Clock Drift
    - Round Trip Time and Clock Offset
    - Nonlinear Clock Behavior

PinPoint
- TOA
- TDOA Variants
  - Card Delays
  - Error Analysis
  - Filtering

Experimental Results

Future Work

Questions?

Distances for PinPoint TOA, TDOA

- Solve optimization problem for location
Time Notation

- Distinguish between idealized global time and measured local times
  
  \( t \)  global time
  
  \( \tau \)  local clock time

- Describe send and receive times for network messages
  
  \( t^S(i) \)  Send time of message \( i \) sent by \( s \)
  
  \( t^r_S(i) \)  Receive time of message \( i \) sent by \( s \) and received at \( r \)
  
  \( \tau^S_s(i) \)  Send time measured at \( s \) of message \( i \) sent by \( s \)
  
  \( \tau^r_r(i) \)  Receive time measured at \( r \) of message \( i \) sent by \( s \) and received at \( r \)
Time of Arrival (TOA)

1. Timestamped message sent from \( a \)
Time of Arrival (TOA)

1. Timestamped message sent from $a$
2. Reception is timestamped at $q$:
3. $d(a, q) = t_q^a - t^a$ Location is ambiguous within sphere solution set
Trilateration

- TOA measurements
- Solution is intersection of spheres
- Non-linear optimization problem to minimize
Message sent by $q$
Time Difference of Arrival (TDOA)

1. Message sent by \( q \)
2. Message received by \( a \) at \( t_a^q \)

\[\text{Solution set is hyperboloid with foci at } A, B \text{ satisfying } d(b, q) - d(a, q) = t_{b} - t_{a}^q\]
Time Difference of Arrival (TDOA)

1. Message sent by \(q\)
2. Message received by \(a\) at \(t^q_a\)
3. Message received by \(b\) at \(t^q_b\)

\[
\text{Solution set is hyperboloid with foci at } A, B \text{ satisfying } d(b, q) - d(a, q) = t^q_b - t^q_a
\]
Time Difference of Arrival (TDOA)

1. Message sent by $q$
2. Message received by $a$ at $t^q_a$
3. Message received by $b$ at $t^q_b$
4. Solution set is hyperboloid with foci at $A$, $B$ satisfying $d(b, q) - d(a, q) = t^q_b - t^q_a$
Hyperbolic Location

- TDOA measurements
- Solution is intersection of hyperboloids
- Non-linear optimization problem to minimize difference of differences of distances
Challenges

- Must measure time very precisely and accurately: 1 ns ≈ 0.3m (1 ft.)
- Times from multiple clocks must be translated to common frame of reference
- Clocks drift at variable relative rates
- For 802.11, clocks are typically accurate to 10 ppm. Manufacturing specification is 100 ppm.
### Existing Location Systems

<table>
<thead>
<tr>
<th></th>
<th>Mobile Unit Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
</tr>
<tr>
<td><strong>TOA</strong></td>
<td>PinPoint TOA</td>
</tr>
<tr>
<td></td>
<td>Goodtry</td>
</tr>
<tr>
<td></td>
<td>Pseudolite</td>
</tr>
<tr>
<td><strong>TDOA</strong></td>
<td>GSM UL-TOA</td>
</tr>
<tr>
<td></td>
<td>PinPoint TDOA</td>
</tr>
<tr>
<td></td>
<td>LORAN</td>
</tr>
</tbody>
</table>

**Location System Classification**

- For user privacy, passive mobile units are preferred.
- Nonparticipant targets must be active.
Clock Model

\[ \tau^q_a = \beta_a(t^q + \alpha_a) + r + e^q_a \quad \text{receive} \]
\[ \tau^a = \beta_a(t^a + \alpha_a) + s + e^a \quad \text{send} \]

- Each clock runs independently at separate rate \( \beta \)
- Each clock started at different time \( \alpha \)
- Real time \( t \) is not directly measurable
- Time measured with receive delay \( r \) or send delay \( s \) in local time
Pairwise Clock Drift

\[
\frac{\beta_b}{\beta_a} = \frac{\tau^a_b(i) - \tau^a_b(i - k)}{\tau^a_a(i) - \tau^a_a(i - k)}
\]

- From 802.11 standard, drift < 100ppm
- Apply exponential filter to repeated measurements to reduce error
Average Clock Drift: Fully Connected

- Pairwise clock drift estimated from set $\Omega = \{a, b, \ldots\}$
- Define $\beta_* = \frac{1}{|\Omega|} \sum_{\omega \in \Omega} \beta_\omega$
- For the matrix

$$B = \frac{1}{|\Omega|} \begin{bmatrix} 1 & \beta_b & \beta_c & \ldots \\ \beta_a & 1 & \beta_c & \ldots \\ \beta_a & \beta_b & 1 & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

- Eigenvector for the greatest eigenvalue ($\lambda = 1$) contains conversions from local clocks to virtual global clock
Round Trip Time and Clock Offset

- Timestamped messages passed between two nodes to determine round trip time and clock offset as in SNTP

\[
\delta = \left( \tau^b_a - \tau^a_a \right) - \left( \tau^b_b - \tau^a_b \right)
\]

- Clock offset \( \theta_{a \rightarrow b} \):

\[
\theta_{a \rightarrow b} = \frac{1}{2} (\tau^b_b - \tau^a_a + \tau^a_b - \tau^b_a)
\]
Nonlinear Behavior of $\theta_{a\rightarrow b}$

- $\theta_{a\rightarrow b}$ over a 80 second interval
- $\theta_{a\rightarrow b}$ Deviation from Linear over 80 second interval

- Clocks behave nonlinearly even over short 80 second time periods
- Nonlinear behavior of approximately 0.01 ppm is within specified precision of 100 ppm
- Must model time to handle nonlinear behavior
PinPoint Variants

Goals
Location
Methods
TOA
TDOA
Challenges
Existing
Location
Systems
Clocks
Clock Drift
Round Trip
Time and Clock
Offset
Nonlinear Clock
Behavior
PinPoint
TOA
TDOA Variants
Card Delays
Error Analysis
Filtering
Experimental
Results
Future Work
Questions?

TOA

TDOA
1 Active Target
2 No Send Times
3 Low Traffic

Hyperbolic Location

Trilateration

\( d(a, q) \)
\( d(b, q) \)
\( d(c, q) \)
PinPoint Approach

- Frequently exchange messages to implicitly track nonlinearity of clock offset $\theta_{a\rightarrow b}(\tau)$ with period $P$
- Assume piecewise linear model
- Filter and combine many samples to statistically improve distance estimate
- Solve nonlinear optimization problem to find location

\[
\frac{\Delta \theta_{a\rightarrow b}}{\Delta \tau_a} = \frac{\beta_b}{\beta_a}
\]

Piecewise Linear Approach
Goals
- Use messages passed between anchors to translate times
- Assume locally linear behavior

PinPoint Reference Equations

\[
\tau^a = \beta_a(t^a + \alpha_a) + s_a + e^a
\]

\[
\tau^b = \beta_b(t^a + \alpha_b + d(a, b)) + r_b + e^b
\]

\[
\tau^b = \beta_b(t^b + \alpha_b + s_b + e^b)
\]

\[
\tau^a = \beta_a(t^b + \alpha_a + d(a, b)) + r_a + e^a
\]

\[
\tau^q = \beta_a(t^q + \alpha_a + d(a, q)) + r_a + e^q
\]

\[
\tau^q = \beta_b(t^q + \alpha_b + d(b, q)) + r_b + e^q
\]
No Send Times  Some drivers support receive timestamps but not than send timestamps. A protocol without send times supports more platforms.

**Participant**  Target node must timestamp

**Active**  Target node must send messages frequently

<table>
<thead>
<tr>
<th>Variant</th>
<th>No Send Times</th>
<th>Participant</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TDOA</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>TDOA No Send Times</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>TDOA Participant</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
PinPoint TOA

\[ \beta_\ast d(a, b) = \frac{1}{2} \left[ \frac{\beta_\ast}{\beta_a} \left( \tau_b^a - \tau^a_a \right) - \left( r_a - s_a \right) \right] - \frac{\beta_\ast}{\beta_b} \left[ \left( \tau^b - \tau_b^a \right) - \left( s_b - r_b \right) \right] \]
PinPoint TDOA: Active Target

\[
\beta_*(d(b, q) - d(a, q)) = \frac{\beta_*(q)}{\beta_b} \left( \tau^q_b - \frac{1}{2}(\tau^b_a + \tau^a_b) - (r_b - s_b) \right) \\
- \frac{\beta_*(q)}{\beta_a} \left( \tau^q_a - \frac{1}{2}(\tau^a_a + \tau^b_a) - (r_a - s_a) \right)
\]
PinPoint TDOA: No Send Times

- Requires geometry for $a$, $b$, $l$, which may be known beforehand or computed with TOA.

$$\beta_* [d(b, q) - d(a, q)] = \beta_* [d(b, l) - d(a, l)] + \frac{\beta_*}{\beta_b} (\tau^q_b - \tau^l_b) - \frac{\beta_*}{\beta_a} (\tau^q_a - \tau^l_a)$$
PinPoint TDOA: Low Traffic

• \( m \) must timestamp and estimate clock drift, but is not required to send messages for each distance estimate

\[
\beta_* \left( d(b, m) - d(a, m) \right) = \frac{\beta_*}{\beta_m} \left( \tau^b_m - \tau^a_m \right) - \frac{1}{2} \frac{\beta_*}{\beta_b} \left( \left( \tau^b - \tau^a_b \right) - (r_b - s_b) \right) + \frac{1}{2} \frac{\beta_*}{\beta_a} \left( \left( \tau^a - \tau^b_a \right) - (r_a - s_a) \right)
\]
Card Delay Equations

- Times reported by wireless cards are consistently biased.
- Anecdotally stable for 20+ minutes
- Measured with anchor nodes colocated such that \( d(a, b) = d(b, q) - d(a, q) \).
- Requires 3 nodes to measure

\[
\begin{align*}
    r_b - s_b &= \tau_b^q - \tau_b^b + \frac{\beta_b}{\beta_a} \left( \tau_a^b - \tau_a^q \right) \\
    r_a - s_a &= \frac{\beta_a}{\beta_b} \left( -\tau_b^q + \tau_b^a \right) + \tau_a^q - \tau_a^a
\end{align*}
\]
## Card Delay Results

<table>
<thead>
<tr>
<th>Beacon Interval (k ticks)</th>
<th>Clock Speed (MHz)</th>
<th>Sample Size</th>
<th>$r - s$ clock ticks</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>20</td>
<td>48000</td>
<td>22422.65 -54377.87</td>
</tr>
<tr>
<td>500</td>
<td>20</td>
<td>11000</td>
<td>22423.20 -361577.38</td>
</tr>
<tr>
<td>1000</td>
<td>20</td>
<td>6000</td>
<td>22423.02 -745577.91</td>
</tr>
<tr>
<td>1000</td>
<td>40</td>
<td>8000</td>
<td>45230.69 -722771.39</td>
</tr>
</tbody>
</table>

### Card Delays

- Delays vary with card, beacon interval and clock speed
- Send delays appear to increase linearly with beacon interval
- Error from neglecting $r - s$ is $(\frac{\beta_b}{\beta_a} - 1) \times (r - s)$. For $(\frac{\beta_b}{\beta_a} - 1) = 10 \times 10^{-6}$ and $r - s = 45000$, this is 0.45 clock ticks, or roughly 4 m at 40 MHz clock speed.
Error for PinPoint TOA and TDOA

- Assumptions
  1. Anchor messages send periodically roughly every $P$ clock ticks
  2. Send and receive errors are independent with standard deviation $\sigma$
  3. $r - s$ can be determined accurately using prior data
  4. There is a value of $\frac{\beta_\omega}{\beta_\star}$ within $\epsilon$ of real clock drift values for entire time period
  5. We can estimate $\frac{\beta_\omega}{\beta_\star}$ within $\epsilon$

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Std Dev</th>
<th>Bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOA</td>
<td>$\sigma$</td>
<td>$\epsilon[(r_a - s_a) + (r_b - s_b) + P]$</td>
</tr>
<tr>
<td>Active Target</td>
<td>$\sqrt{3}\sigma$</td>
<td>$\epsilon(\frac{1}{2}((r_b - s_b) + (r_a - s_a)) + 2P)$</td>
</tr>
<tr>
<td>No Send Times</td>
<td>$2\sigma$</td>
<td>$2\epsilon P$</td>
</tr>
<tr>
<td>Low Traffic</td>
<td>$\sqrt{3}\sigma$</td>
<td>$\epsilon(\frac{1}{2}((r_b - s_b) + (r_a - s_a)) + 2P)$</td>
</tr>
</tbody>
</table>

Expected Error for PinPoint Variants
TDOA Filtering

- Filter out all outliers outside \([\text{median} - 10, \text{median} + 10]\)
- Standard deviation 2.83 clock ticks

Histogram of TDOA readings for 15.24 m

QQ Plot shows TDOA distribution has long tails
PinPoint TDOA Test Setup

- 3 Anchor laptops arranged in indoor corridor environment
- Anchors attached using secondary network card to wireless router
- Separate display unit
- All anchor nodes operate with 40 MHz reference clocks and beacon interval of 1000
- All nodes are operating on the same channel
PinPoint TDOA End-to-End Results

Localization Example

Anchor Location

Target Location

Estimated Location

Hyperbola
PinPoint TDOA Location Error

Location estimated within 3.5m for line-of-sight arrangements
Future Work

1. Fusion of TOA and TDOA data
2. Improvement of TOA and TDOA accuracy
3. Semi-definite programming for TOA optimization
4. Implementation for embedded devices
5. Applications for MyeVyu, etc.
Questions?
Hybrid TOA-TDOA Problem

- Fusion of TOA and TDOA data
- Related work approaches are for simulated data and do not consider use of timestamps for both TOA and TDOA
Hybrid $d(b, q) - d(a, q)$

- Examine basic hybrid computation
- Two basic ways to compute $d(b, q) - d(a, q)$
  1. TDOA($a, b, q$)
  2. TOA($b, q$) − TOA($a, q$)
- Also two ways to compute TOA($b, q$) − TOA($a, q$) based on whether messages are reused across nodes

$$\begin{align*}
\text{Time} & \quad a \quad q \quad b \\
\text{reuse} & \quad \text{no reuse}
\end{align*}$$

- Minimize variance of difference for PinPoint computations
  $$k \cdot \text{TDOA}(a, b, q) + (1 - k)(\text{TOA}(b, q) - \text{TOA}(a, q))$$

<table>
<thead>
<tr>
<th>Optimal $k$</th>
<th>Best Hybrid Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>TOA only</td>
</tr>
<tr>
<td>0.25</td>
<td>TOA and TDOA</td>
</tr>
</tbody>
</table>
TOA and TDOA Accuracy

QQ Plot shows TDOA distribution is non-normal

- Error model required to explain non-normal TDOA behavior
- Card delay histogram is unexpectedly asymmetric
- Multipath issues may also need to be explored
Local Coordinate System Integration

- Solved problem in sensor network field, solutions need to be integrated
- Coordinates are relative to PinPoint nodes
- No anchor nodes with known position are required
- Nodes discover their own coordinates
- Combine capability to compute location of stranger nodes
Goodtry

- 802.11 TOA trilateration system
- Exploit fixed interframe spacing between RTS, CTS, data, and ACK frames
- Data traffic between nodes $a$ and $b$ allows all nodes to measure $d(a, b)$
- $O(n^2)$ algorithm to find all pairwise distances