Robust Location Distinction Using Temporal Link Signatures

Neal Patwari

Sneha Kasera

Department of Electrical and Computer Engineering

THE UNIVERSITY OF UTAH

SCHOOL OF COMPUTING
What is location distinction?

- Ability to know when a transmitter has changed position
- Enabled by the physical layer only
- Compared to localization:
  - no coordinates
  - benefits from multipath
  - more sensitive, needs less coverage

Each transmitter \((i_1, i_2, i_3)\) is distinguished at the two receivers \((j_1, j_2)\)

Applications

- Efficient location estimation in WSN
- Physical security, management of objects
- Prevent impersonation in wireless networks
Location Estimation in WSNs

• Network self-localization expensive
  - Ranging energy, bandwidth
  - Communication

• Only re-localize when sensor moves
  How do you know? Collaboration?

• WSN low-energy location distinction: detect movement w/o collaboration
Real-Time Location Service

• Applications in Logistics
  - Healthcare, distribution, manufacturing, mining, military, ...

• Idea: Detect Movement of Objects
  - most assets should be stationary
  - focus resources on rare moving assets

• However, existing methods are costly!
  - Accelerometers: add $3 to each tag
  - Doppler: require continuous transmission
  - both: energy, cost, communication inefficient

• Localization Issues: Coverage, Accuracy, Security
Wireless LAN Security

- Impersonation
- **MAC-address spoofing** [1]
- Traditional crypto methods subject to node compromise

Goals & Challenges

• Develop link signatures with key properties
  - uniqueness: as function of tx, rx locations
  - non-measurement: can’t read from another place
  - spoof-proof: can’t create from another place

• Efficiency: receivers, time

• Do not change transmitter

• Validate with real measurements
Outline

• Temporal link signatures
• Related work
• Methodology
• Measurement apparatus
• Quantitative evaluation
• Summary
Physical Layer Filter

Wireless channel from $i$ to $j$ is a filter $h_{i;j}(\xi)\,$

$$h_{i;j}(\xi) = \sum_{l=1}^{\infty} e^{j\xi l}$$

Sum of attenuated, delayed impulse functions
Received Signal

• The signal is filtered by the channel

\[ r(t) = s(t) \ast h_{i,j}(t) \]

\[ R(f) = S(f)H_{i,j}(f) \]
Calculation in Receiver

• Further convolve with known tx signal

\[ r(t) \quad s_{\alpha}(t) \quad h_{i;j}^{(n)}(t) = s(t) \star h_{i;j}(t) \star s_{\alpha}(t) \]

\[ R(f) \quad S_{\alpha}(f) \quad H_{i;j}^{(n)}(f) = jS(f)j^2H_{i;j}(f) \]
Estimate of the Channel

- Typically $|S(f)|^2$ largely flat in-band, very low out of band. (spectral efficiency)

$$H_{i;j}^{(n)}(f) = jS(f)j^2H_{i;j}(f)$$

$$H_{i;j}^{(n)}(f) \approx \frac{1}{4} H_{i;j}(f)$$

*Figure: Spectral characteristic of an OFDM signal*
**Temporal Link Signature**

- **In time domain**, temporal link signature

\[ h_{i;j}^{(n)}(t) = \frac{1}{4} h_{i;j}(t) \]

*Figure: Multipath are approximated in the measurement (t) h_{i;j}(t)*
Related Work

- Use RSS only (multiple receivers) [1]
  - Power in received signal $r(t)$

- Use frequency-domain estimate [2]
  - Equivalent to $H_{i,j}^{(n)}(f)$ at selected frequencies $\{f\}$


Temporal Link Sig. Methodology

- Sampled temporal link signature

\[ h_{i;j}^{(n)} = [h_{i;j}^{(n)}(0); \ldots; h_{i;j}^{(n)}(\cdot T_r)]^T \]

- Normalized link signature (NLS)

\[ h_{i;j}^{(n)} = \frac{h_{i;j}^{(n)}}{kh_{i;j}^{(n)}k} \]
**Distance Between Signatures**

- **History for** \( f h^{(n)}_{i,j} \ g_n=1;\ldots;N \ i \ j \)

- **Size of history** \( \gamma_{i,j} : \) avg. distance between points

- **New measurement** \( h^{(N)}_{i,j} \)

- **Distance:** normalized Euclidean \( (l_2) \) to closest point
  \[
  d_{i,j} = \frac{1}{3}\sqrt[3]{4} \ \min \ h_{i,j}^{(N)} k
  \]
Detection of Different Location

• Want to test two cases

  \( H_0 \): New Meas’t at same location
  \( H_1 \): New Meas’t at different location

• Two conditional densities for distance \( d \)

  \[ f_{d|H_0}, f_{d|H_1} \]

  \( P_{FA} \) = Probability of false alarm
  \( P_D \) = Probability of detection

• Choose a threshold ?
Measurement Experiment

- Meas’t set from Motorola office area
- Using 40 MHz direct sequence spread-spectrum (DSSS) Tx and Rx
Measurement Experiment

- 13 by 15 m area, and 44 devices
- 5 meas’ts per link (over 30 sec)
- 44 x 43 x 5 = 9460 measurements
- ‘Manual’ procedure, Mostly stationary

Leave-one-out Comparison

Temporal Differences:
- Compare $N = 5$ measurements from same link $(i,j)$ to History for $(i,j)$

Spatial Differences:
- Compare $N = 5$ measurements from different link $(k,j)$ to History for $(i,j)$
Example Link Signatures

- Each plot: 5 meas’ts
  \[ h^{(n)}_{i,j} \quad n = 1; \ldots; 5 \]
- How different are they?
  - Temporal Differences: 0.18, 0.76
  - Spatial Differences: 3.6, 10.0

Link Signatures: Worst Case

- Temporal channel changes can cause changes
  - most widely varying set
Comparing Results

• Three methods
  - RSS [Faria 2006]
  - Link Signature
  - Amplitude-Normalized Link Signature
Performance with one Rx

- Adjustable results based on threshold

Heavy Tail on Worst Links

- Worst 5% of links cause 46% of missed detections
  - System could disable link signatures for highly varying links
Multiple Receivers

- Can employ more than one receiver (access point)
Performance with Three Rx

- Significantly higher reliability compared to one Rx
Multiple RX Summary

- Table 1: False Alarm Rates for Constant 95% Detection Rate

<table>
<thead>
<tr>
<th>Method</th>
<th>1 RX</th>
<th>3 RX</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS</td>
<td>0.0655</td>
<td>0.0019</td>
</tr>
<tr>
<td>RSS</td>
<td>0.5164</td>
<td>0.0295</td>
</tr>
</tbody>
</table>
Summary

• Robust location distinction can be achieved using temporal link signatures

• Significant improvement over RSS-only signature methods

• Future work
  - Comparison w/ freq-domain link signatures [Li '06]
  - Study other link characteristics, metrics
  - Real-time Implementation
Measurement Data Access

• SPAN Website
  - http://span.ece.utah.edu/
  - Under “Data & Tools”

• To appear in CRAWDAD
Threat Model

- **Attacker can**
  - listen to all wireless traffic
  - compromise encryption
  - use attenuators, amplifiers, directional antennas, software radios

- **Attacker cannot**
  - be at location of user
  - be at location of access points

- **System deployment must have multiple coverage**