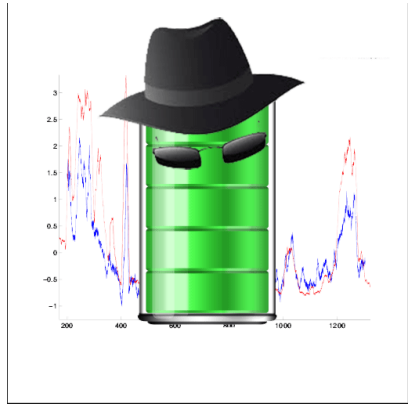
PowerSpy

Location Tracking using Mobile Device Power Analysis



Yan Michalevsky[(1)], Gabi Nakibly[(2)], Aaron Schulman[(1)],
Gunaa Arumugam Veerapandian[(1)] and Dan Boneh[(1)]

[(1)] Stanford University, [(2)] National Research and Simulation Center, Rafael Ltd.

Smartphones have many sensors

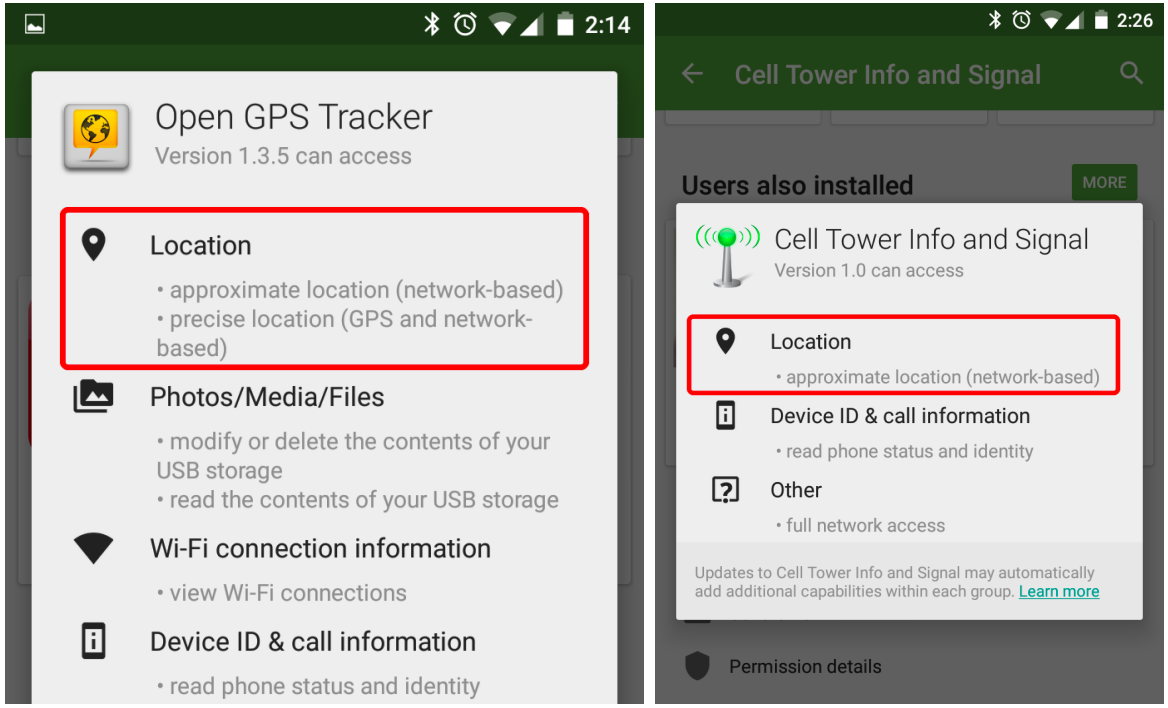


- accelerometer
- gyroscope
- magnetometer
- front and rear cameras
- NFC
- barometer
- speaker
- microphone
- proximity
- light sensor
- Bluetooth
- GPS
- WiFi + cellular
- humidity
- temperature

Related Work on Information Leakage Through Sensors

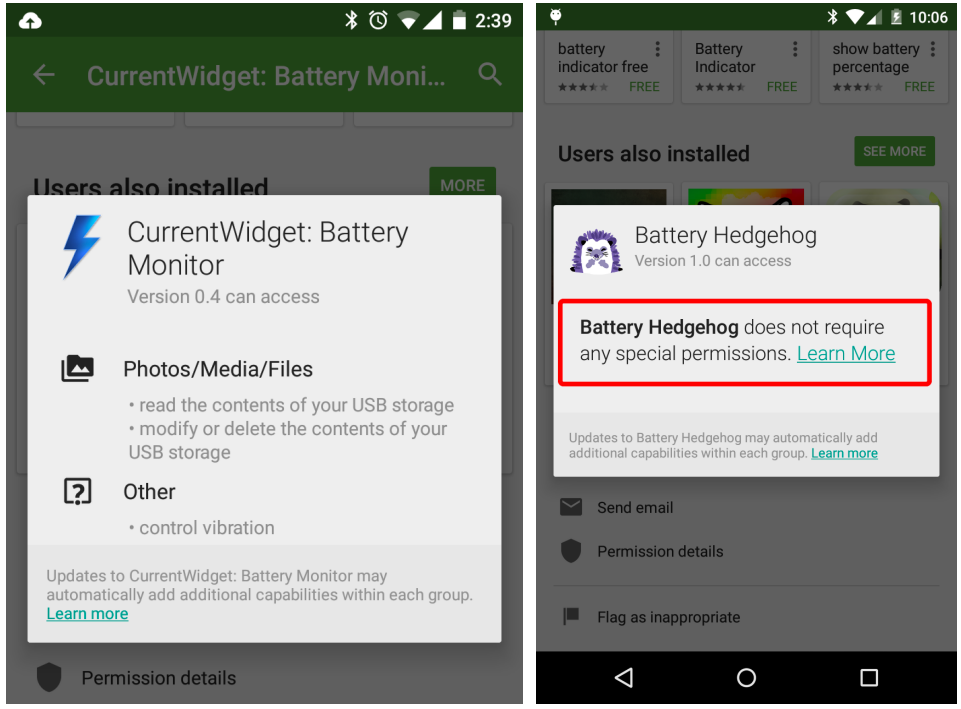
- Speaker on/off status [Zhou et al. '13]
- Accelerometers [Hua et al. '15, Han et al. '12]
- Microphone [Schlegel at al. '11]
- and many more...

Accessing Location Requires Permissions



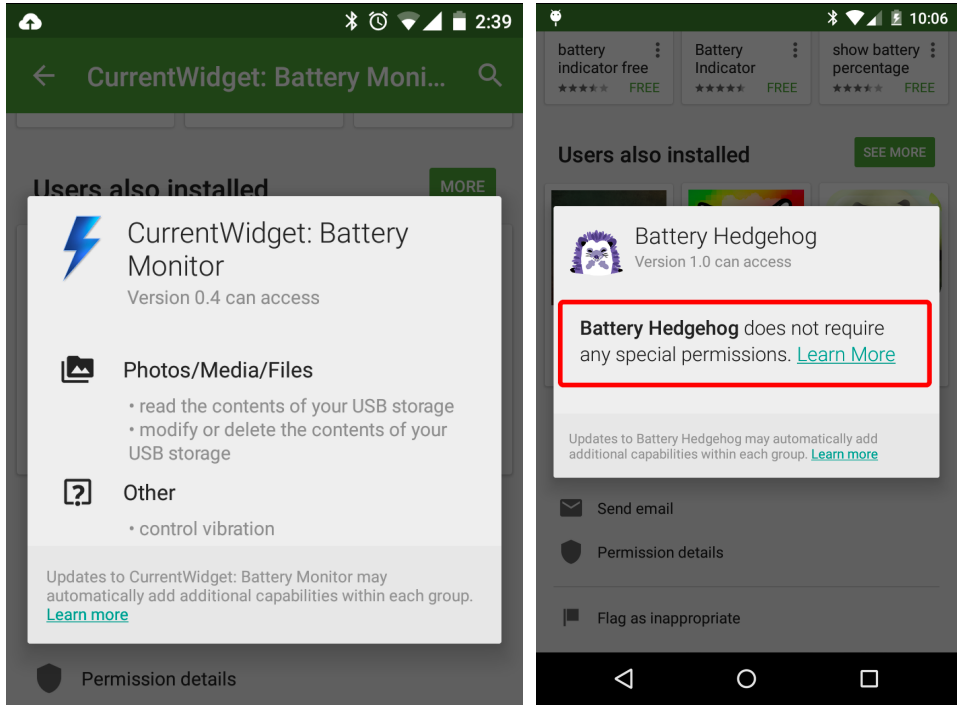
Even coarse location based on cellular network information

Reading Voltage and Current Requires NO Permissions



/sys/class/power_supply/battery/voltage_now
/sys/class/power_supply/battery/current_now

Reading Voltage and Current Requires NO Permissions



/sys/class/power_supply/battery/voltage_now

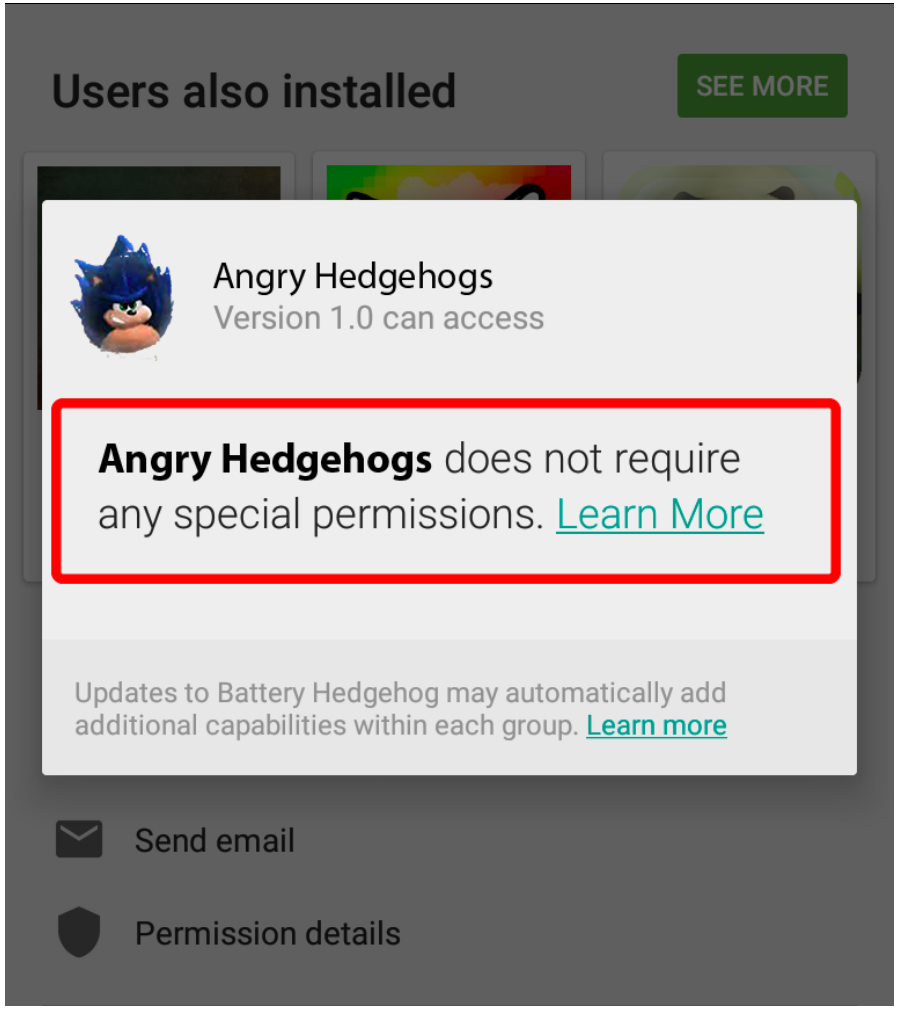
/sys/class/power_supply/battery/current_now

Nexus 4, Nexus 5, HTC Desire, iPhone 6...

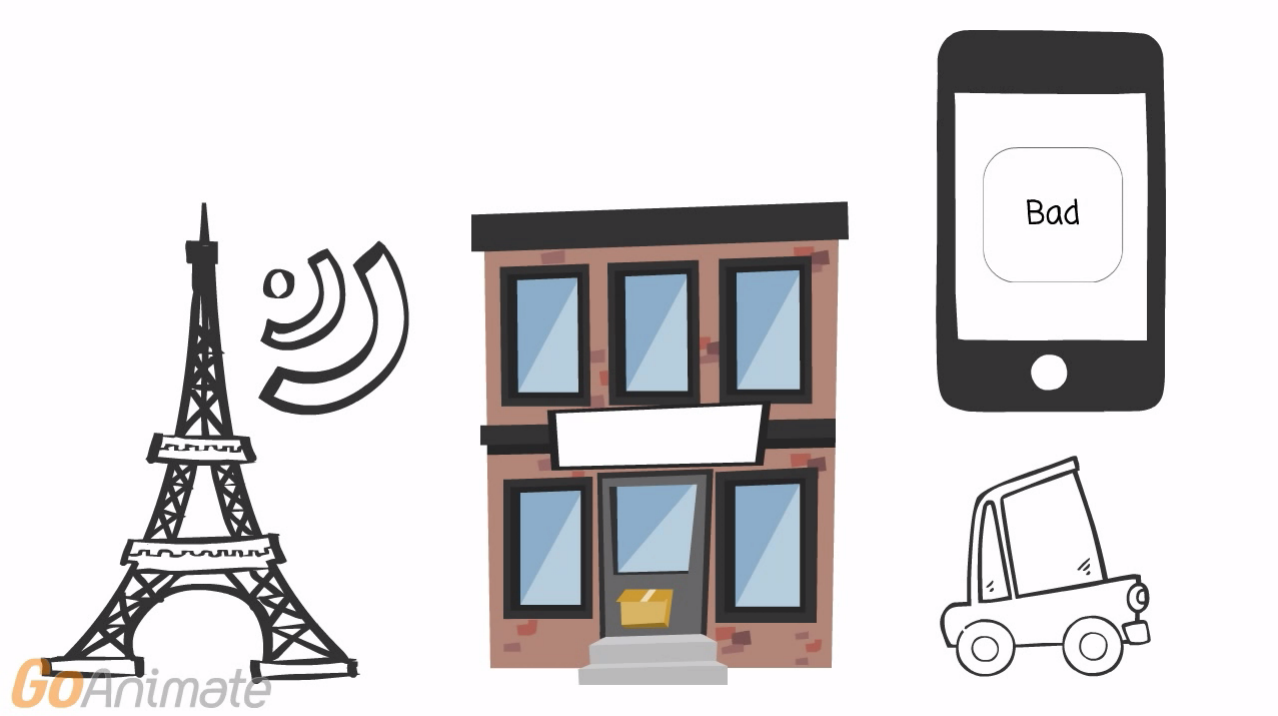
Sampling at order of 100 Hz

Power Meter Reveals Location

A seemingly innocent application can read the power meter

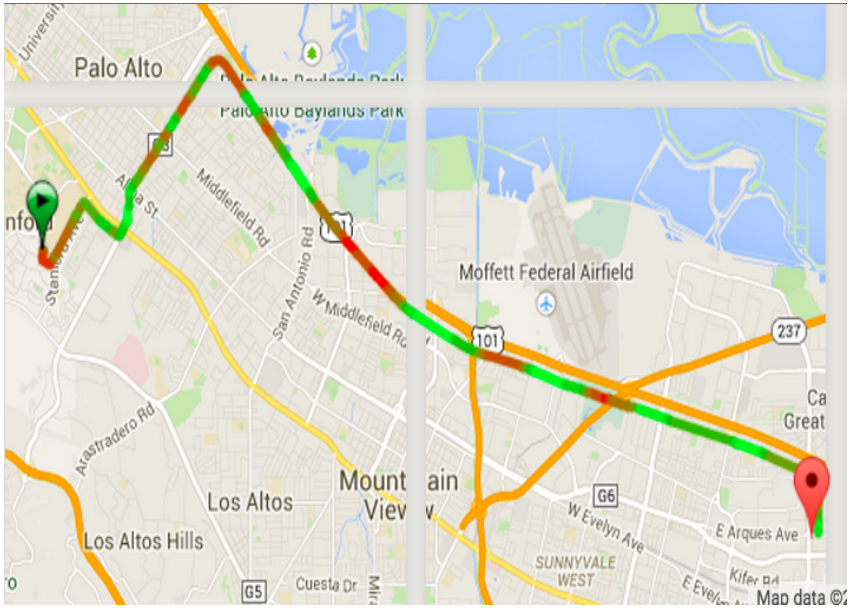


Signal Strength Depends on Location and Environment

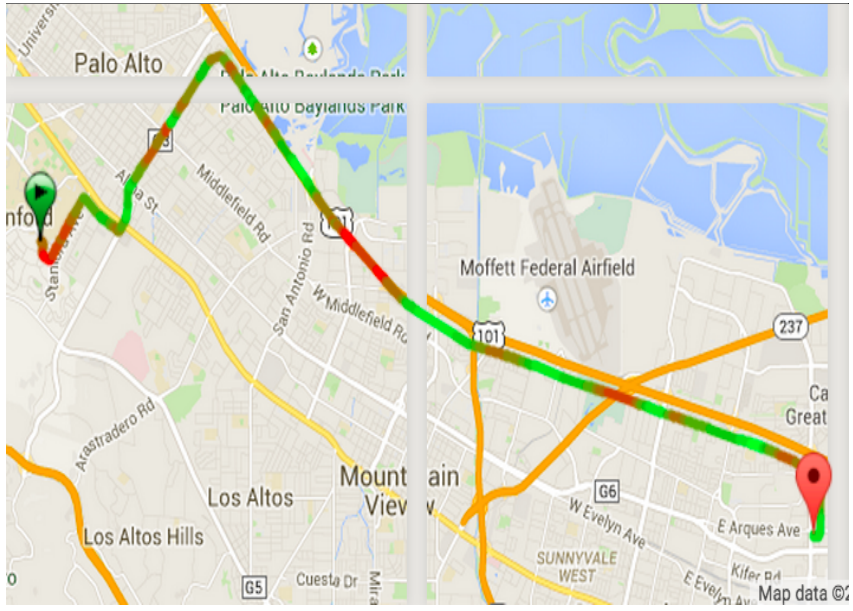


Signal Strength is Stable Across Days

06/23/2014



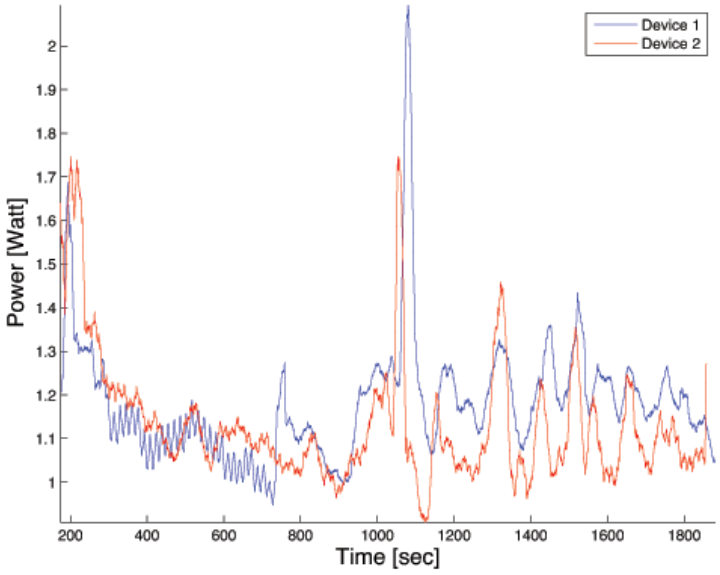
06/24/2014



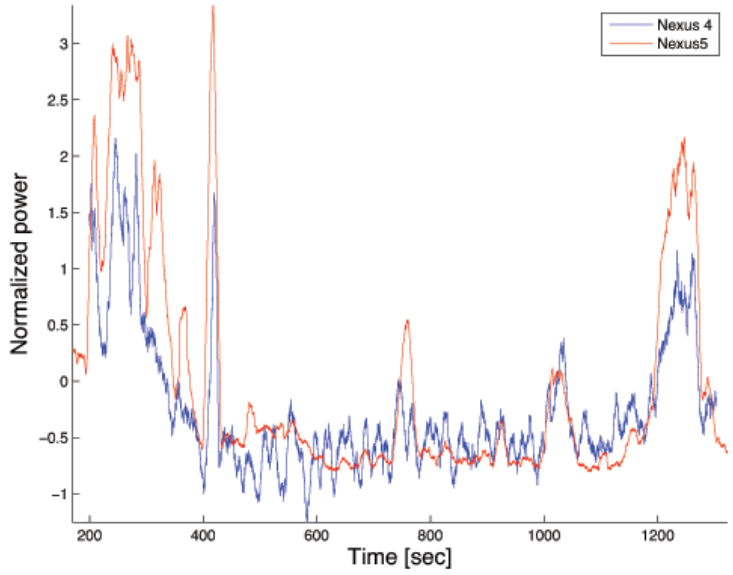
$$Power = f(Signal\ Strength)$$

- More power used upon transmission under low SNR
- Signal amplification, error correction on the receive part
- Verified experimentally in Bartendr [Schulman et al. '10]

Power Profile is Consistent Across Devices



Two phones of same model, same route

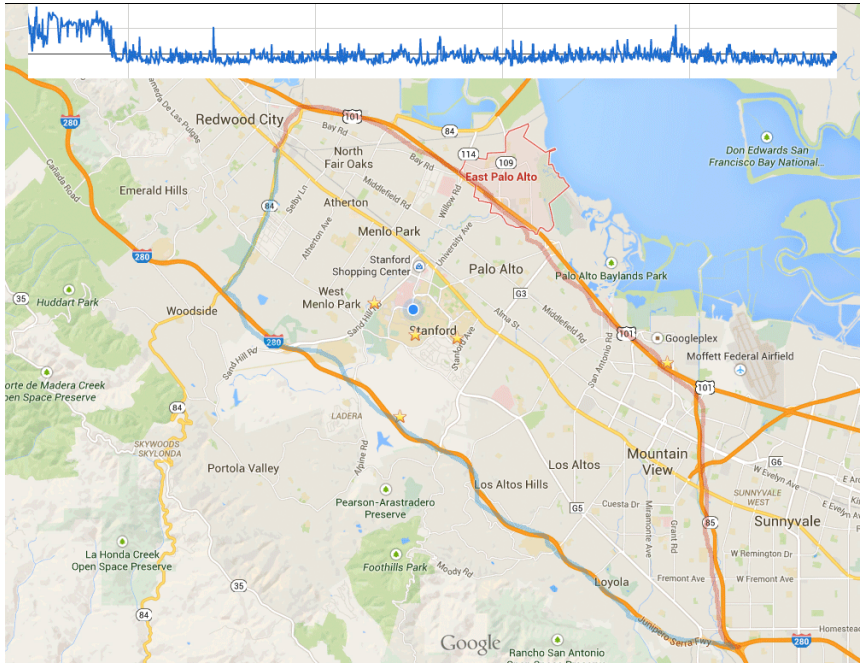


Different models, same route

What can we achieve with that?

Goal 1: Route Distinguishability

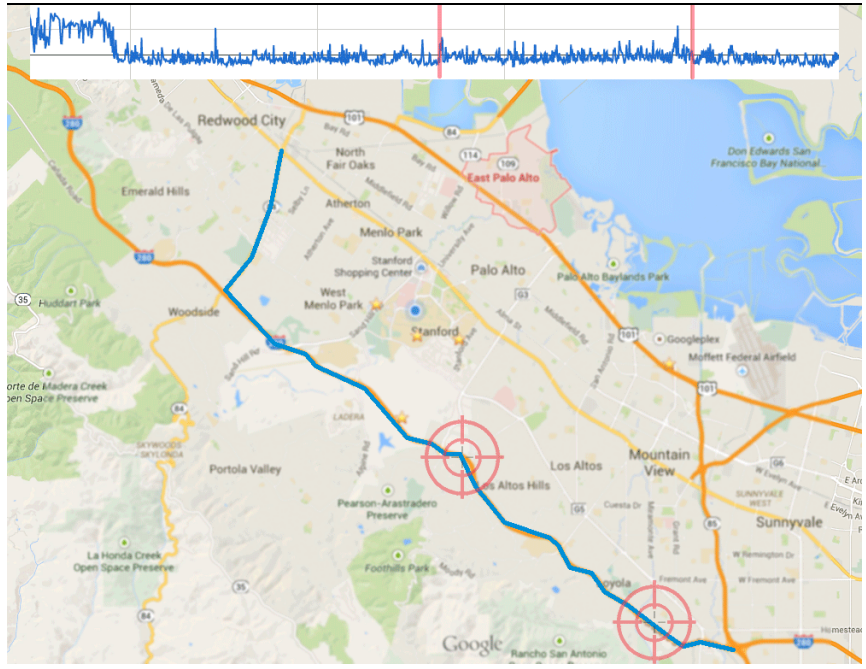
- Determine the route taken by the user from a given set
- Learn past locations
- Application: advertisement, etc.



Goal 2: Real-Time Tracking

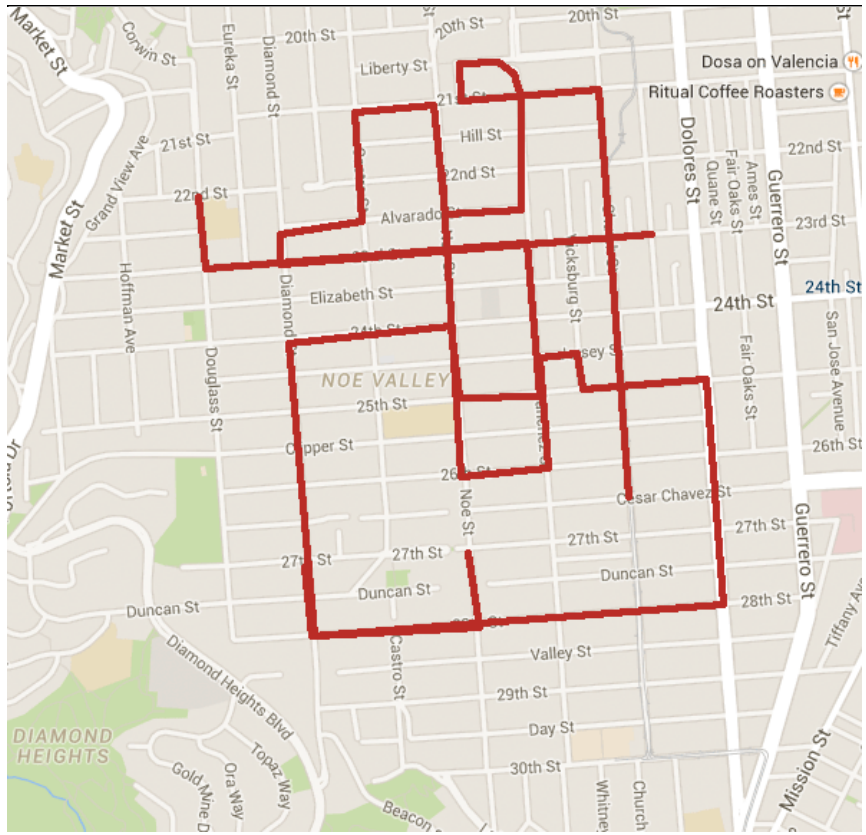
along a known (or assumed) route

Perform tracking of the user's current location on a given route



Goal 3: New Route Inference

Learn the route using previously measured power profiles of many short road segments

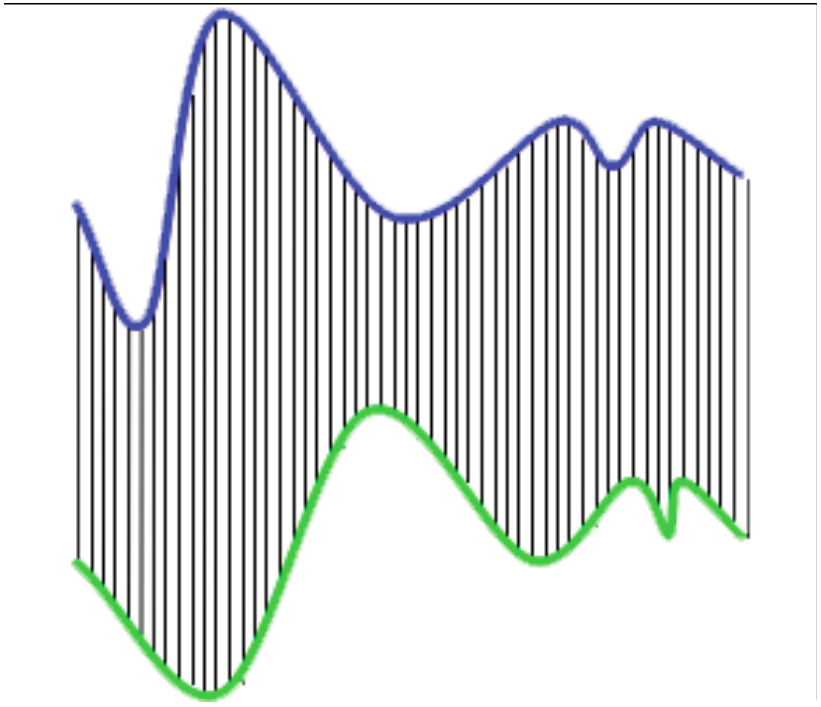


Distinguishing Routes

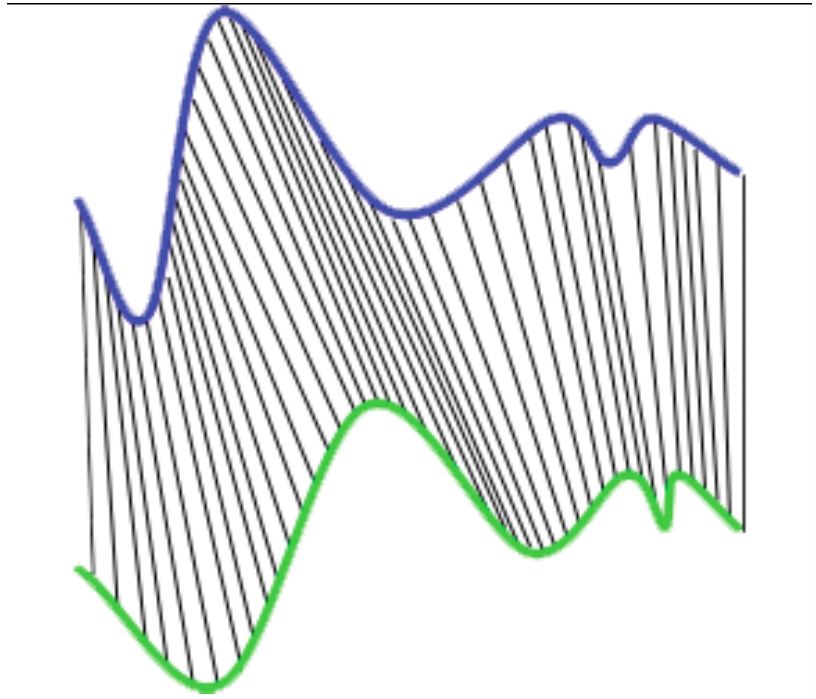
Each power profile is a time-series

Classifier based on time series comparison using Dynamic Time Warping (DTW) [Sakoe and Chiba 1978]

Dynamic Time Warping

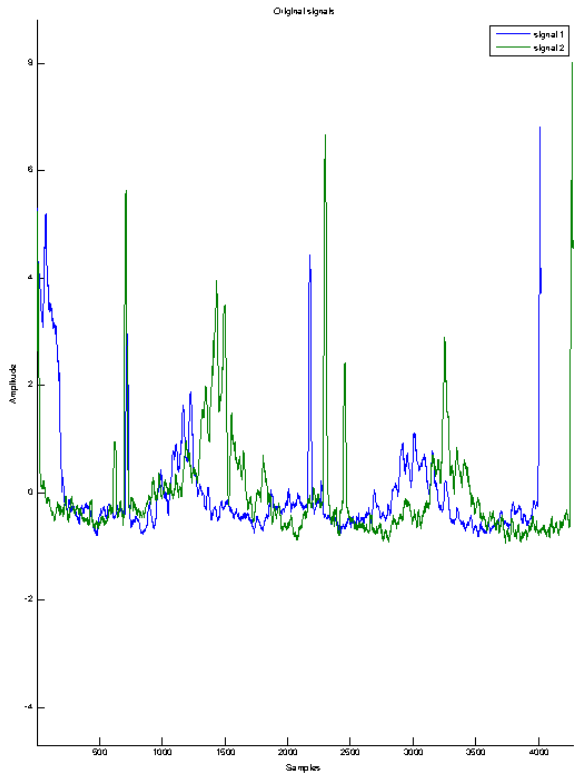


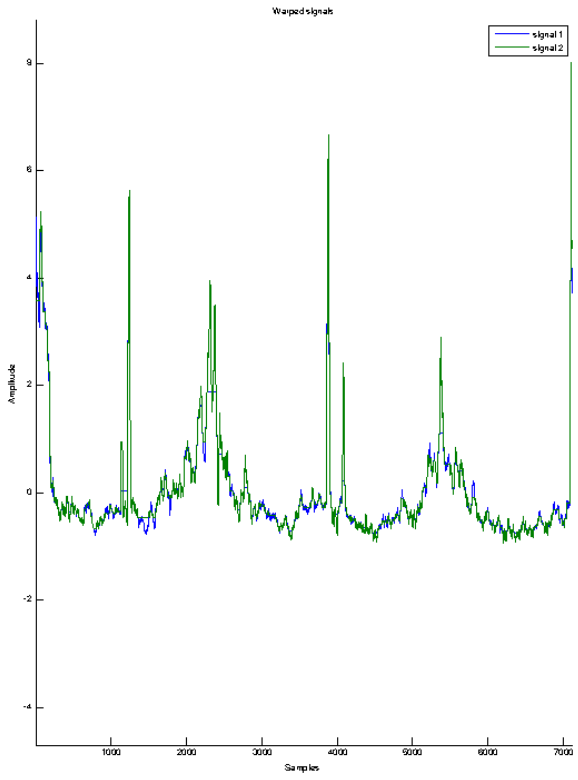
Euclidean distance



DTW distance

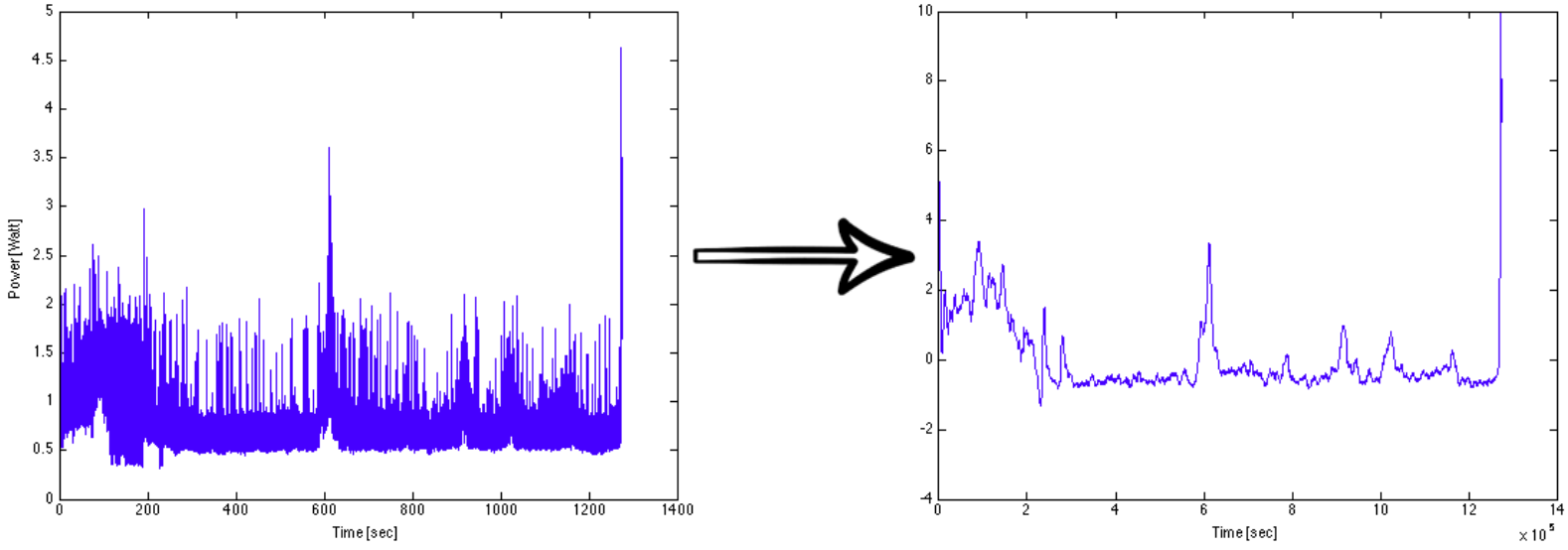
DTW Alignment





Data Processing

- DC offset removal and normalization
  - Compensate for background appications introducing a constant offset
  - Compensate for gain differences
- Smoothing: Moving Average filter (obtain general trends)
- Downsampling (important for computation reduction)




Evaluation

Goal 1: We can Distinguish between Routes

Unique Routes	# Ref. Profiles/Route	# Test Routes	Success %	Random Guess %
8	10	55	85	13
17	5	119	71	6
17	4	136	68	6
21	3	157	61	5
25	2	182	53	4
29	1	211	40	3

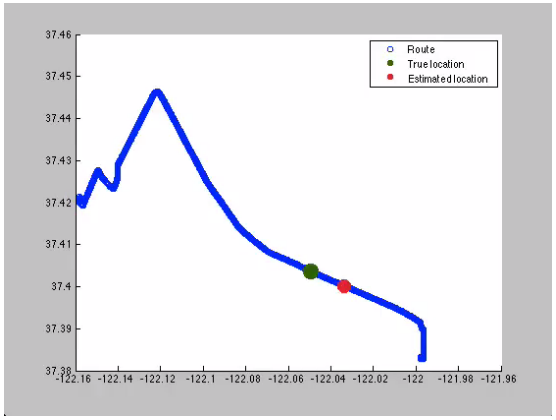
Real-Time Tracking

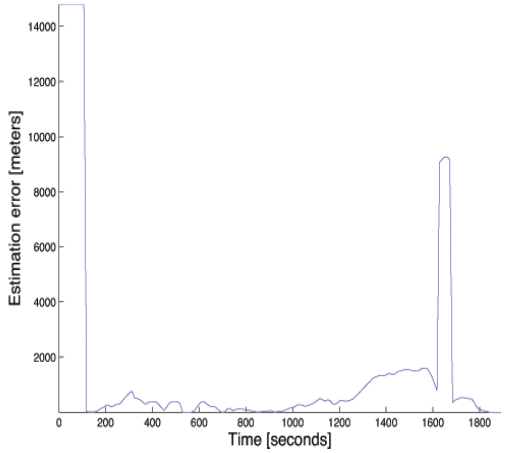
- A window of received samples is a subsequence of the reference power profile
- Using Subsequence-DTW determine the offset of the subsequence
- Infer location from reference profile

Goal 2: We can Track Along a Route

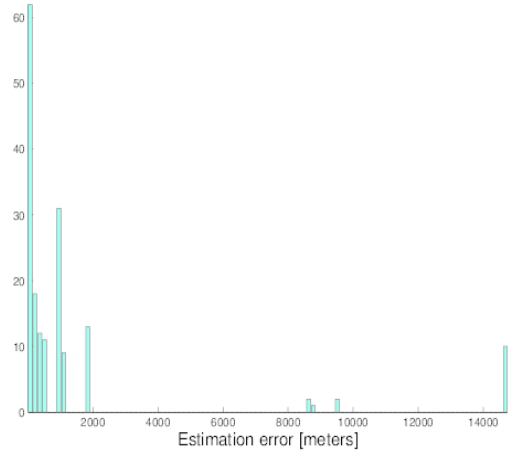


Goal 2: We can Track Along a Route



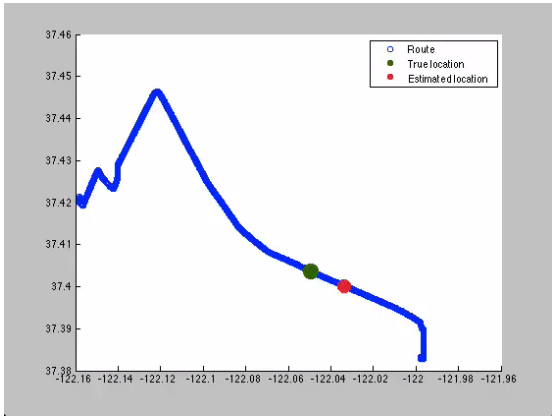


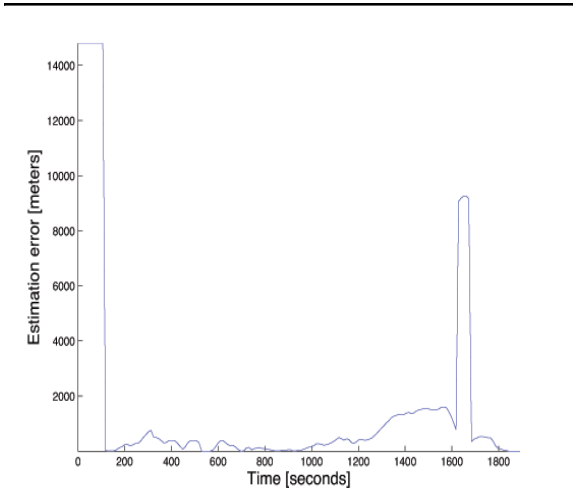
Error(time)



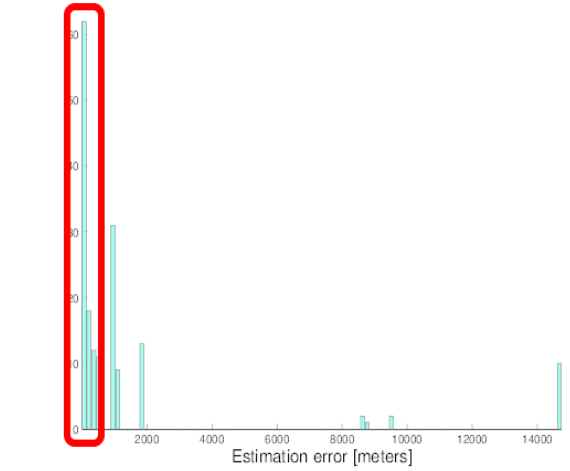
Error histogram

Goal 2: We can Track Along a Route



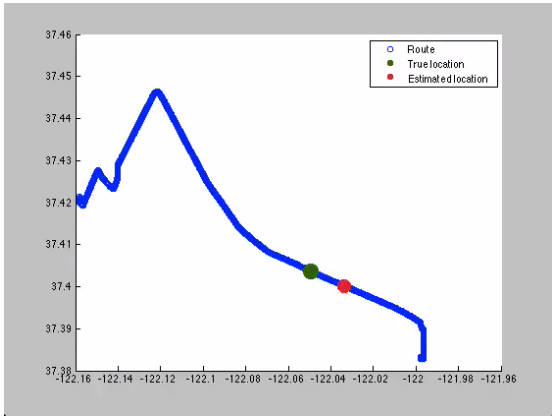


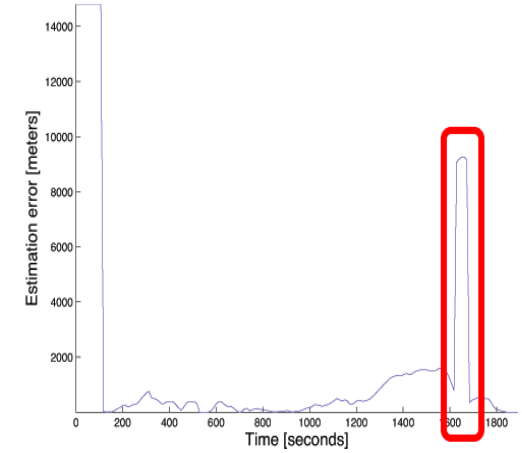
Error(time)



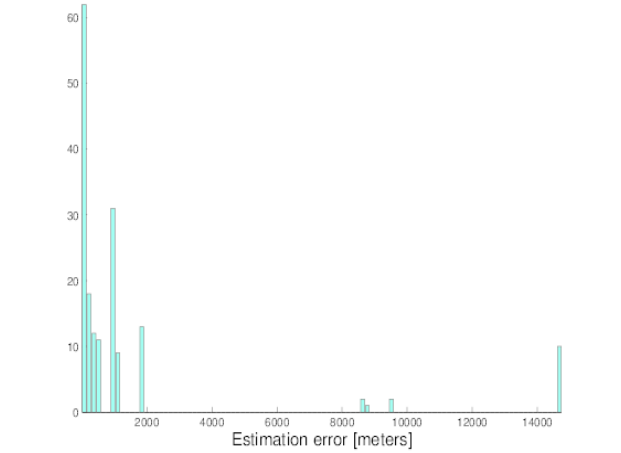
Error histogram

Goal 2: We can Track Along a Route



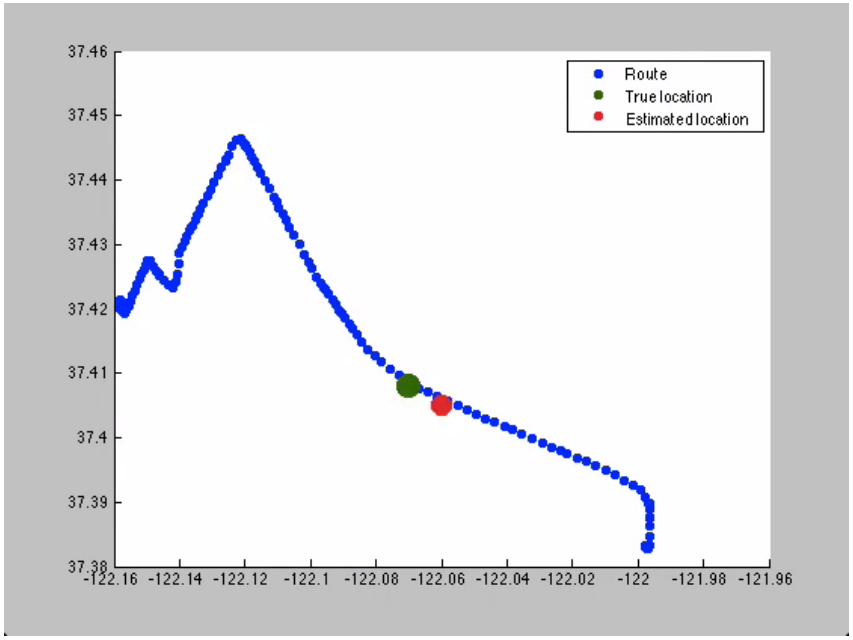


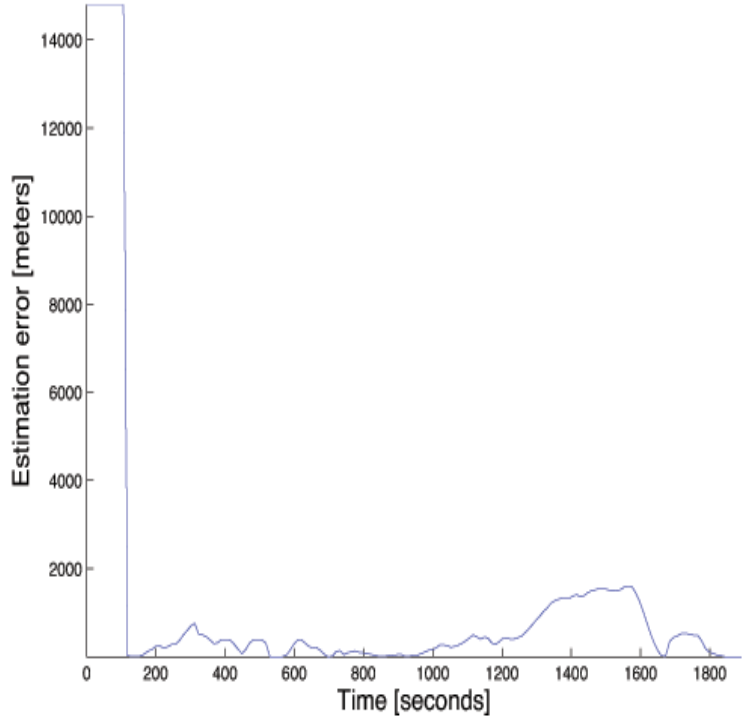
Error(time)



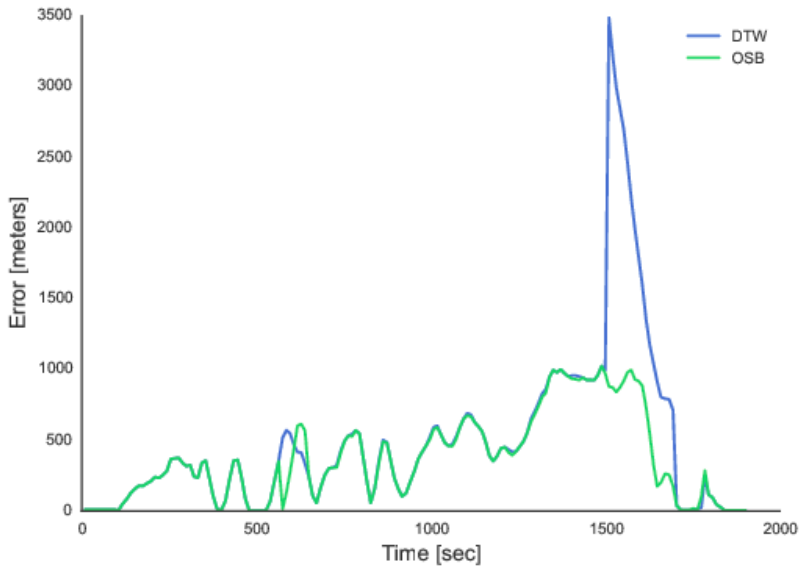
Error histogram

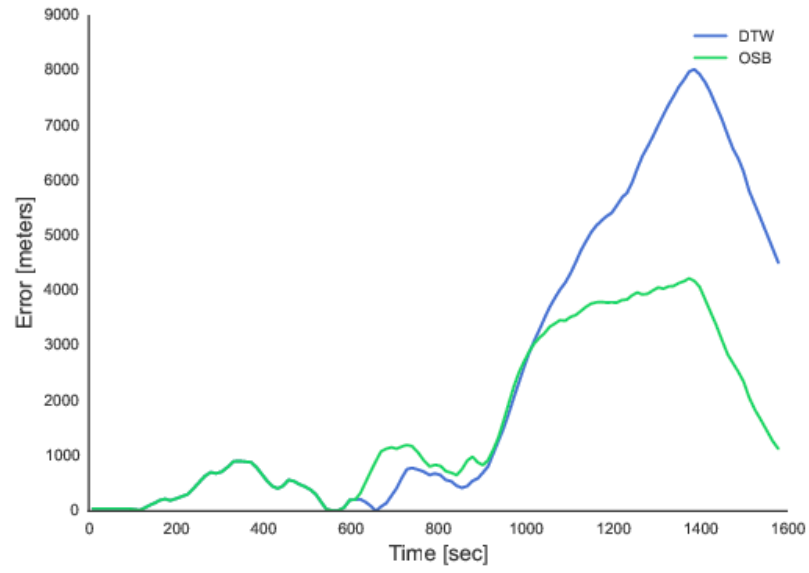
And compensate for obvious errors...





Improved tracking using Optimal Subsequence Bijection (OSB) [Latecki et al. '07]

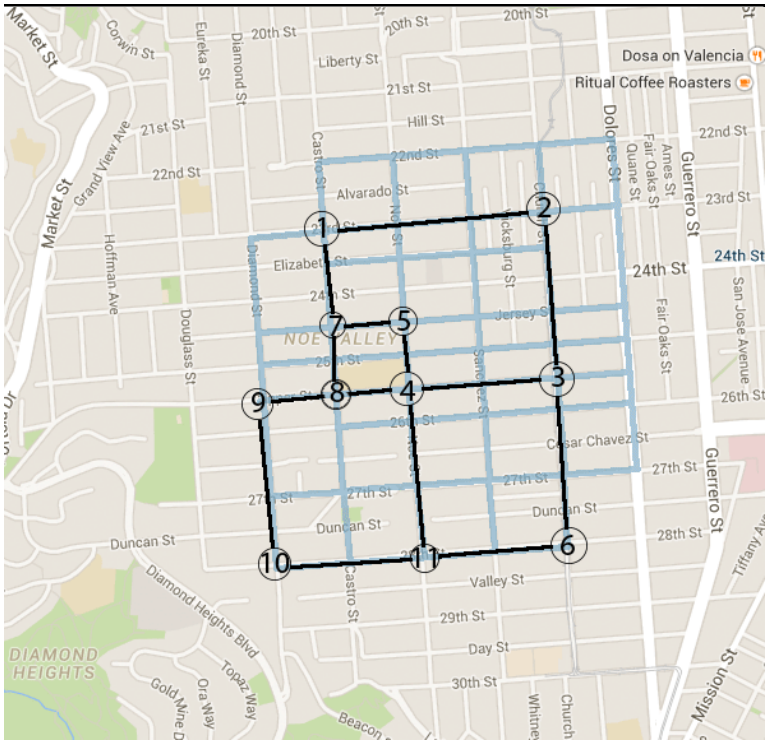




Tracking using OSB

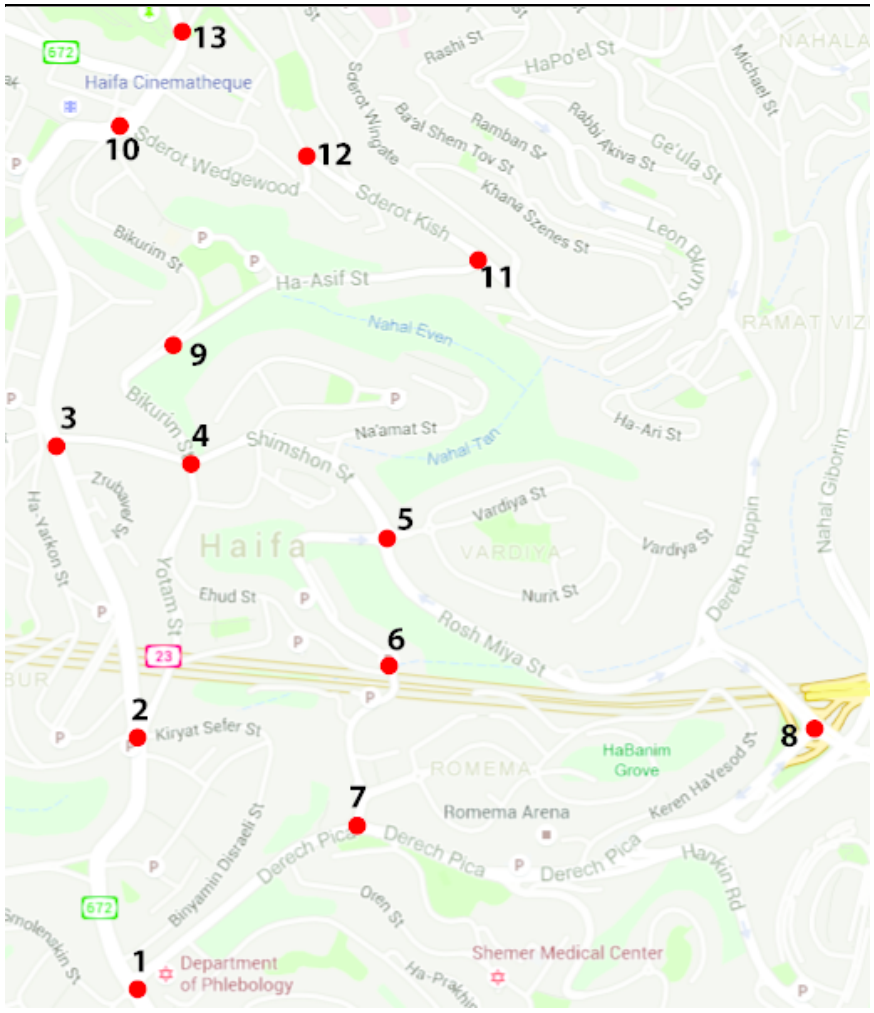


Goal 3: New Route Inference based on Road Segments



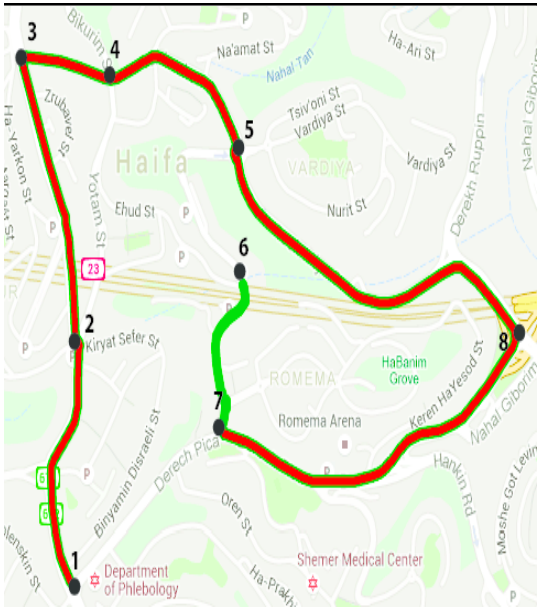
- Points on map represented by nodes
- Connecting road segments represented by edges
- Probabilistic graphical model of location

New Route Inference based on Road Segments: The Area Map

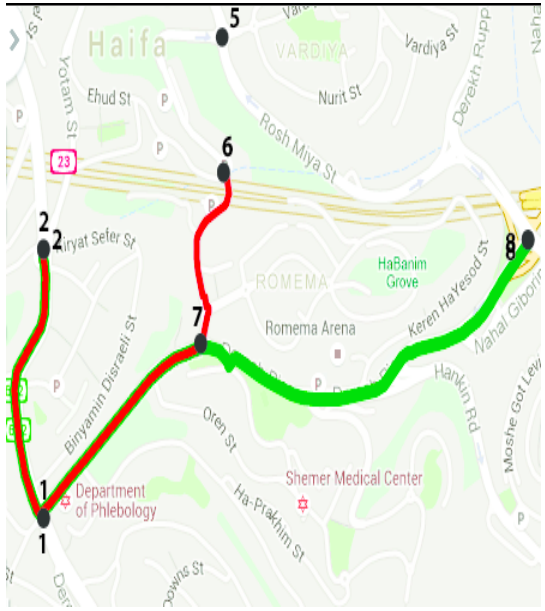


Route Inference based on Road Segments

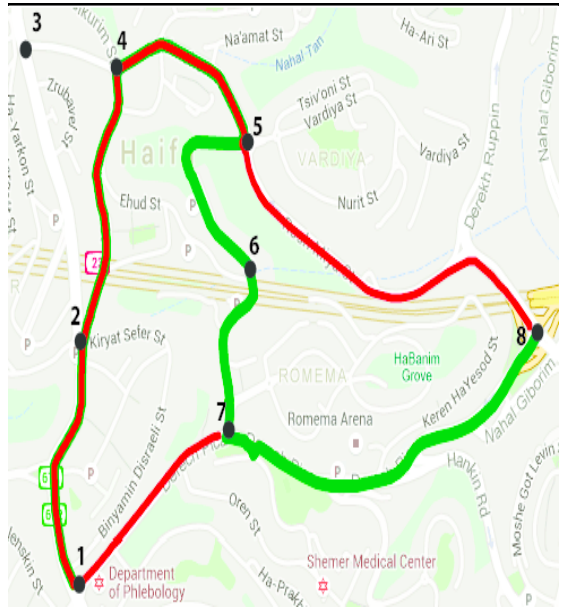
Evaluation metric based on Levenshtein Distance



$d = 0.125$



$d = 0.25$



$d = 0.43$

Future Work

- Build a big dataset of power profiles for US routes
- Improved route inference (Hidden Markov Model, Viterbi...)

Future Warning!

- HTML5 provides battery API that enables receving notifications about changes in battery level.
- The derivative of the battery level is a very coarse power consumption profile.
- Keep power measurement coarse!


Defenses

Non-Defenses

- Adding noise
- Limiting power sampling rate (1 Hz)

Defenses

- Secure hardware design
  - Exclude TX/RX chain from power measurement
- Power consumption as a coarse location indicator
- Provide abstractions, not raw data [Jana et al. '13]

Conclusion

- Sensors can have unintended consequences
- Power meter access should be restricted
- Permissions needed to address sensor access

Thank you for attending

Questions?

yanm2@cs.stanford.edu
www.stanford.edu/~yanm2

Phone Call Profile

A phone call can be easily distinguished and removed from a power profile

