PowerSpy Upgraded: Location Tracking using Mobile Device Power Analysis

By Shengtuo Hu and Shibo Chen
University of Michigan - Ann Arbor

EECS588 Project Presentation
April. 17th, 2018

Introduction - Motivations

Multiple motivations to get location information about someone, i.e. Ads service based on geolocation or espionage etc.

Roadblocks to get those information: more and more restricted access control and permission granting process.

A Stanford team extracted location information through power consumption information (PowerSpy, Y. Michalevsky, USENIX `15).

Introduction - Problems

After three years, new questions arise:

(1) A change in threat model due to Android 6.0 upgrade (Doze execution) and 8.0 upgrade (restriction on background service)

(2) Availability under more conditions: geo-condition and network condition.

(3) A hole in their research: Had both GPS and Cellular on when collecting reference profile but did not discuss which has major effect.

Introduction - Achievements

(1) Reproduced their research in Ann Arbor and re-evaluated the threat model

(2) Extended the attack to add one more scenario based on our findings.

(3) Fixed the hole in their research by providing evidence that network condition have more effect on power consumption changes over GPS.

Threat Model - Requirements

For the attack in general, the following requirements need to be met:

(1) Pre-knowledge about the victim's frequent visit areas or routes. Be able to extract the fingerprints of the targeting routes shortly before or after the attack.

(2) Trick the victim to have the app running in the foreground during the attack. Also, the victim does not have any long-time power consumption disruptive activity.

Threat Model - Outdoor

For outdoor tracking:

Pre-knowledge about victim's carrier. Traveling distance is long (more varieties) and travels in a relatively high speed (more dramatic changes).

We are able to:

(1) Distinguish which route the victim has taken
(2) Real-time tracking or record the power information and recover the location later.

Threat Model - Indoor

For indoor tracking:

Have and only have wifi network on (airplane mode or Android pad)

We are able to:

Distinguish which route the victim has taken

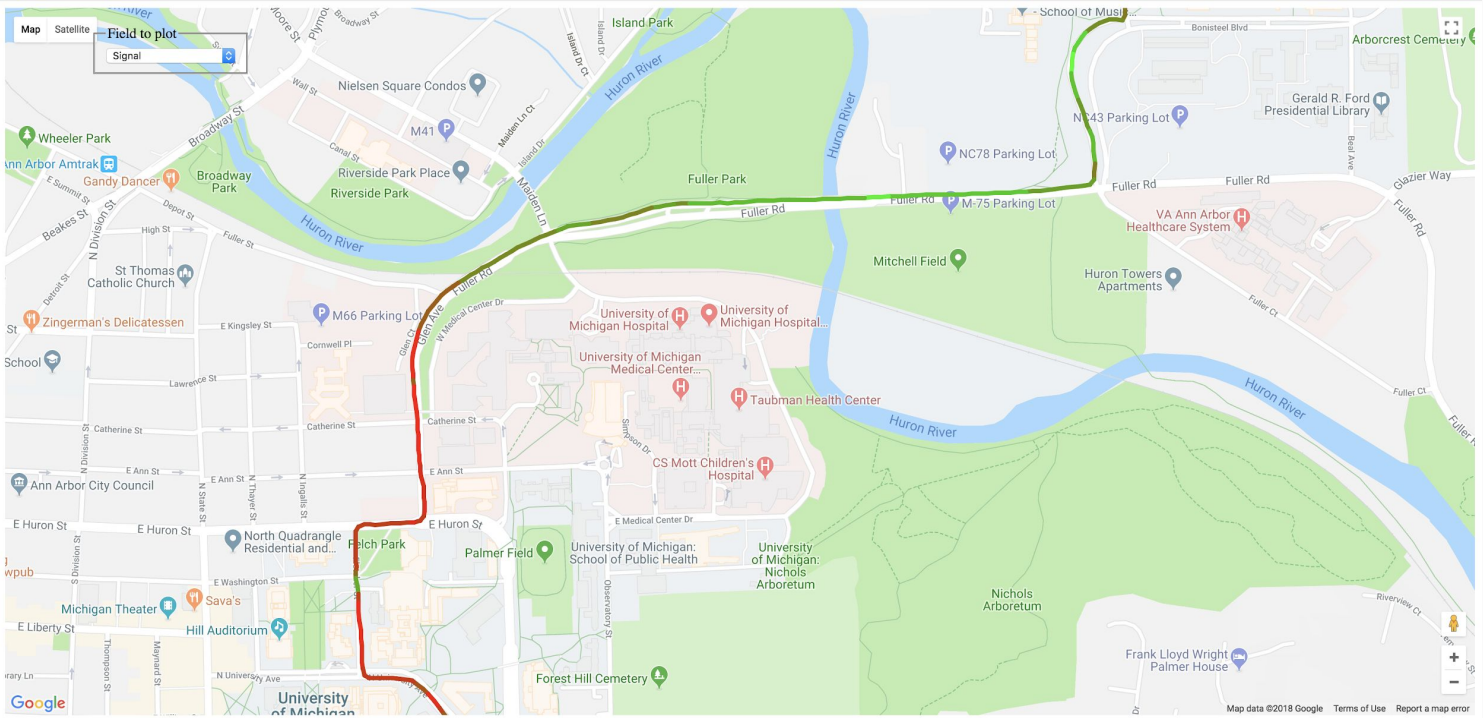
Background

How does location affect signal strength?

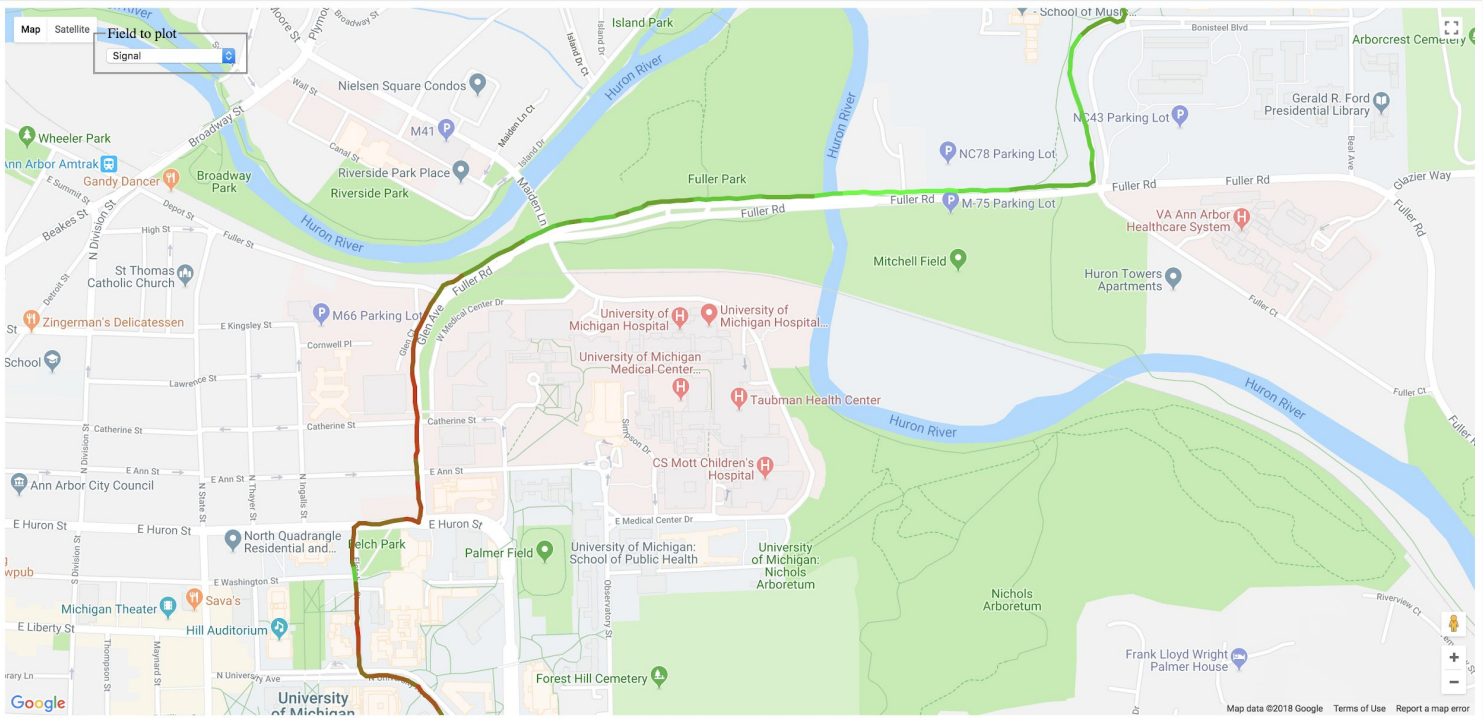
- **Distance** to the base station
- **Signal obstacles**
- **Reflectors**

In one particular location, signal strength is almost unchanged because base stations, signal obstacles, and reflectors remain **stationary**

Background


Map
Satellite
Field to plot
Signal
Island Park
Huron River
Nielsen Square Condos
M41
Wheeler Park
Broadway Park
Riverside Park Place
Riverside Park
Fuller Park
NC78 Parking Lot
M-75 Parking Lot
Fuller Rd
Gerald R. Ford Presidential Library
Arborcrest Cemetery
VA Ann Arbor Healthcare System
Mitchell Field
Huron Towers Apartments
St Thomas Catholic Church
Zingerman's Delicatessen
M66 Parking Lot
University of Michigan Hospital
University of Michigan Medical Center...
Taubman Health Center
CS Mott Children's Hospital
Ann Arbor City Council
North Quadrangle Residential and...
Palmer Field
University of Michigan: School of Public Health
University of Michigan: Nichols Arboretum
Nichols Arboretum
Michigan Theater
Sava's
Hill Auditorium
Forest Hill Cemetery
Frank Lloyd Wright Palmer House
Google
Map data ©2018 Google
Terms of Use
Report a map error
-60
-75
-90

Background


Map
Satellite
Field to plot
Signal
Island Park
Huron River
Nielsen Square Condos
M41
Wheeler Park
Broadway Park
Riverside Park Place
Riverside Park
Fuller Park
NC78 Parking Lot
NC43 Parking Lot
Gerald R. Ford Presidential Library
Arborcrest Cemetery
Fuller Rd
M-75 Parking Lot
VA Ann Arbor Healthcare System
Mitchell Field
Huron Towers Apartments
St Thomas Catholic Church
Zingerman's Delicatessen
M66 Parking Lot
University of Michigan Hospital
University of Michigan Medical Center...
Taubman Health Center
CS Mott Children's Hospital
Ann Arbor City Council
North Quadrangle Residential and...
Palmer Field
University of Michigan: School of Public Health
University of Michigan: Nichols Arboretum
Nichols Arboretum
Michigan Theater
Sava's
Hill Auditorium
Forest Hill Cemetery
Frank Lloyd Wright Palmer House
Google
Map data ©2018 Google
Terms of Use
Report a map error


-72
-84
-96

Background

- Communication at a **poor signal** location can lead to **the increase of power consumption**, compared to a good signal location
- Power consumption information along one road is influenced by the **direction of movement** as well
  - Hysteresis

Background

Fix a hole left in the original research:

In order to fingerprint different segments of a route, we need to have both GPS and network on. However, we also need to prove that it is the network that introduces the most varieties.

Background

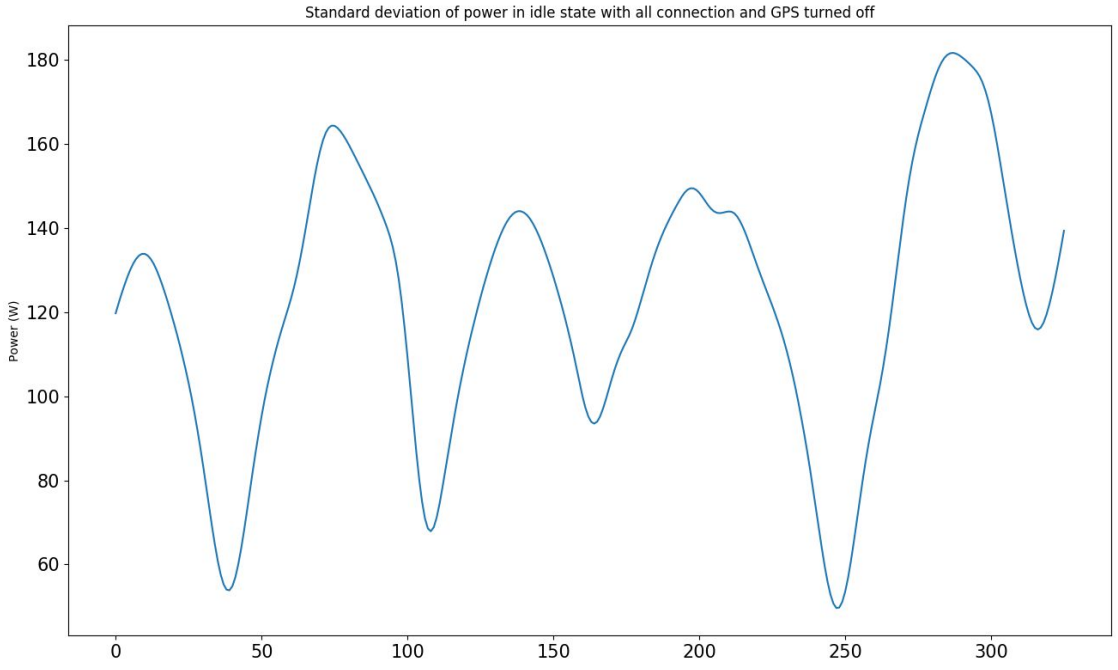
Based on our tests, the phone in idle state with all network connection and GPS off have a standard deviation of about 130 in the power profile.

	Route 1 Sample 1	Route 1 Sample 2	Route 2 Sample 1	Route 2 Sample 2
Cellular Only	231.14	253.96	241.47	239.66
GPS Only	164.16	133.13	150.14	140.66

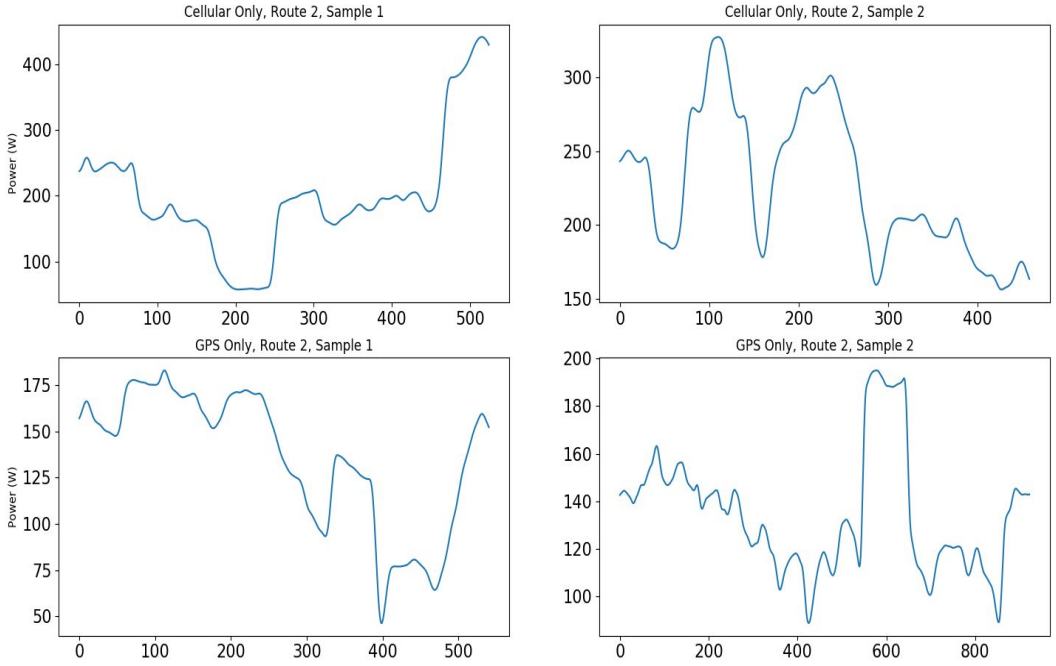
	Route 1 Sample 1	Route 1 Sample 2	Route 2 Sample 1	Route 2 Sample 2
Wifi Only	190.39	253.85	290.70	271.84
GPS Only	160.62	104.63	120.61	101.45

Standard deviation of the power profile under different conditions

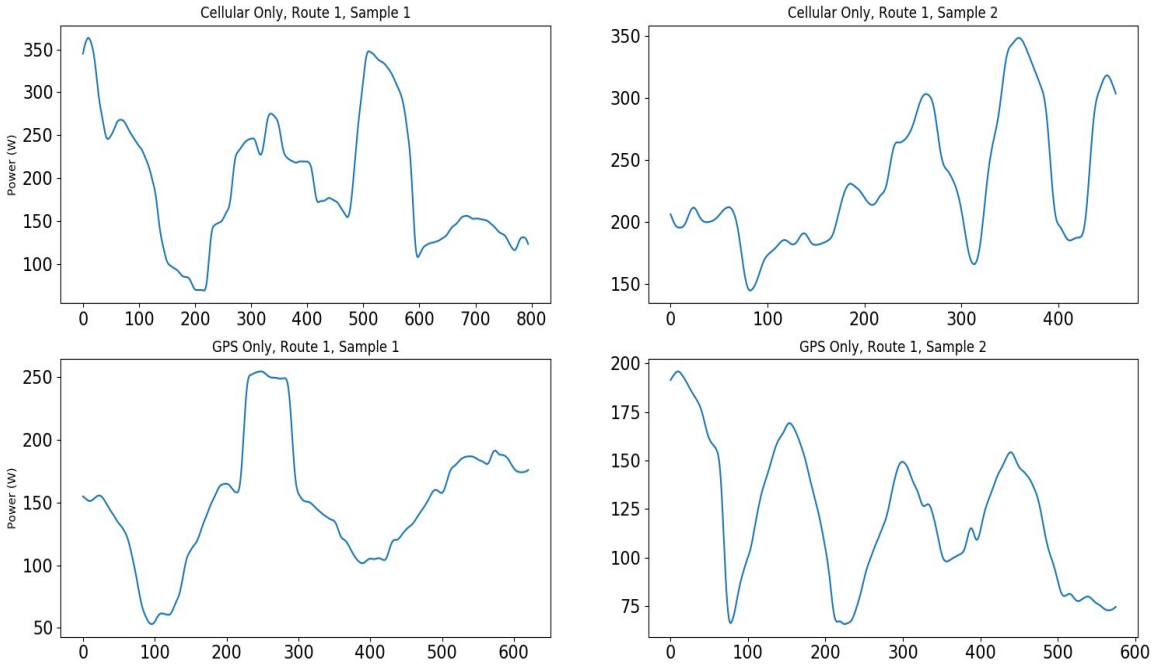
Background


Standard deviation of power in idle state with all connection and GPS turned off
Power (W)
180
160
140
120
100
80
60
0
50
100
150
200
250
300

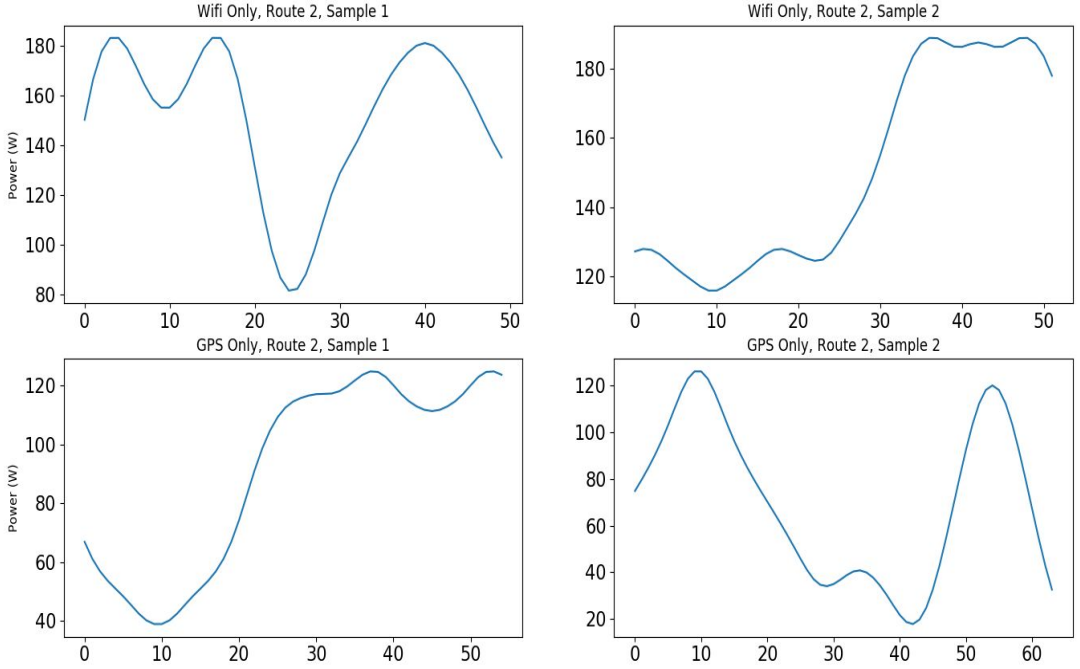
Background


Cellular Only, Route 2, Sample 1
Power (W)
400
300
200
100
0
100
200
300
400
500
Cellular Only, Route 2, Sample 2
300
250
200
150
0
100
200
300
400
GPS Only, Route 2, Sample 1
Power (W)
175
150
125
100
75
50
0
100
200
300
400
500
GPS Only, Route 2, Sample 2
200
180
160
140
120
100
0
200
400
600
800

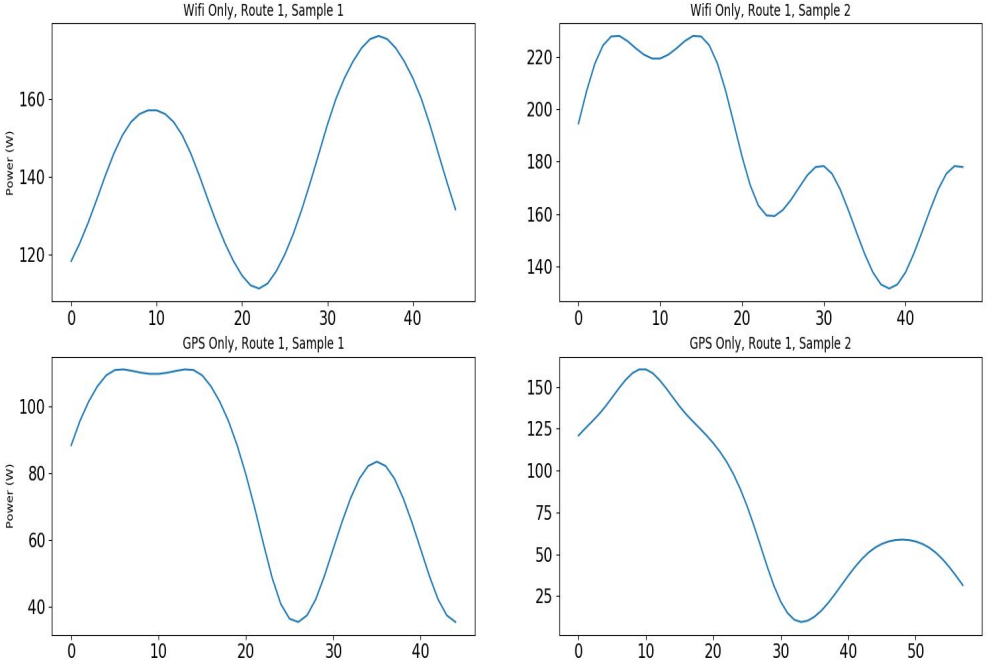
Background


Cellular Only, Route 1, Sample 1
Power (W)
350
300
250
200
150
100
0
100
200
300
400
500
600
700
800
Cellular Only, Route 1, Sample 2
350
300
250
200
150
0
100
200
300
400
GPS Only, Route 1, Sample 1
Power (W)
250
200
150
100
50
0
100
200
300
400
500
600
GPS Only, Route 1, Sample 2
200
175
150
125
100
75
0
100
200
300
400
500
600

Background


Wifi Only, Route 2, Sample 1
Power (W)
Wifi Only, Route 2, Sample 2
GPS Only, Route 2, Sample 1
Power (W)
GPS Only, Route 2, Sample 2

Background


Wifi Only, Route 1, Sample 1
Power (W)
160
140
120
0
10
20
30
40
Wifi Only, Route 1, Sample 2
220
200
180
160
140
0
10
20
30
40
GPS Only, Route 1, Sample 1
Power (W)
100
80
60
40
0
10
20
30
40
GPS Only, Route 1, Sample 2
150
125
100
75
50
25
0
10
20
30
40
50

Background

- There are significantly more varieties introduced by the network connection than those introduced by GPS, if GPS has any effect on power profile varieties.

Background

- Stable signal strength in one particular location
- Poor signal => the increase of power consumption
- Hysteresis & the direction of movement
- Cellular/Wi-Fi module v.s. GPS module

Conclusion:

- Power consumption may reveal location information

Methodology

Two tasks:

- Route distinguishability
  - Classification
  - Identify the route along which a user is traveling
- Real-time tracking

Route Distinguishability

- Feature selection: power traces (time series)
- Classification algorithm: k-NN (k=1)

Route Distinguishability

- Feature selection: power traces (time series)
  - Length
  - Time
- Classification algorithm: k-NN (k=1)

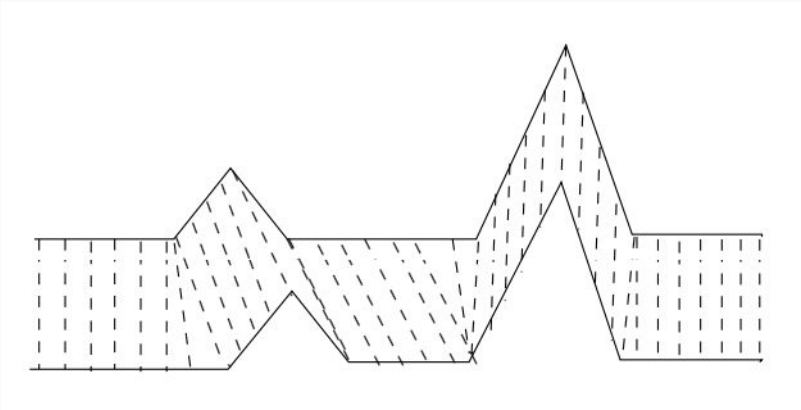
How to measure the **similarity/distance** between any two power traces?

Route Distinguishability

- Dynamic Time Warping (DTW)
  - Tolerate misalignment of power traces
  - Handle time or speed variants
- Normalization before classification
  - Handle issues like different power baselines and variability

$$X_i = \frac{X_i - mean(X_i)}{std(X_i)}$$

$$i = \underset{i \in [1,n]}{\arg\min}\, \mathrm{DTW}(Y, X_i)$$



Real-time Tracking

- Tracking via Dynamic Time Warping
  - Use **Subsequence DTW** algorithm

Algorithm 1 Tracking algorithm

```
locked ← false
while target moving do
    loc[i], score ← estimateLocation()
    d ← getDistance(loc[i], loc[i − 1])
    if locked and d > MAX_DISP then
        loc[i] ← loc[i − 1]
    end if
    if score > THRESHOLD then
        locked ← true
    end if
end while
```

Real-time Tracking

- Tracking via Dynamic Time Warping
  - Use **Subsequence DTW** algorithm
- Tracking via Optimal Subsequence Bijection

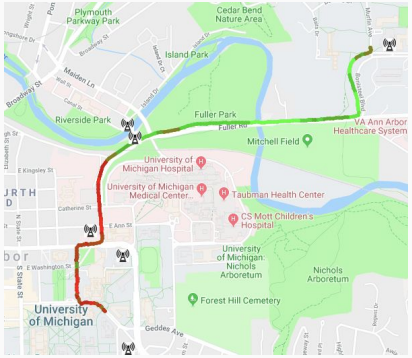
Algorithm 1 Tracking algorithm

```
locked ← false
while target moving do
  loc[i], score ← estimateLocation()
  d ← getDistance(loc[i], loc[i − 1])
  if locked and d > MAX_DISP then
    loc[i] ← loc[i − 1]
  end if
  if score > THRESHOLD then
    locked ← true
  end if
end while
```

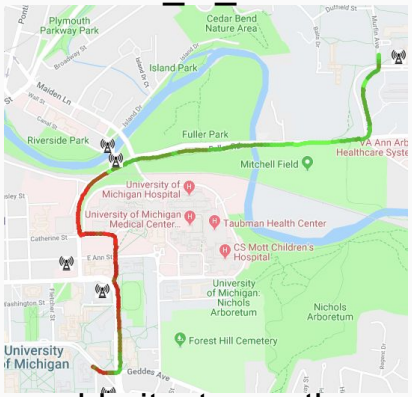
Experiments - Data Collection

- Device: Moto X4
- OS: Android 8.0
- Carrier: Google
- Environment:
  - Outdoor, taking bus
  - Outdoor, walking
  - Indoor, walking

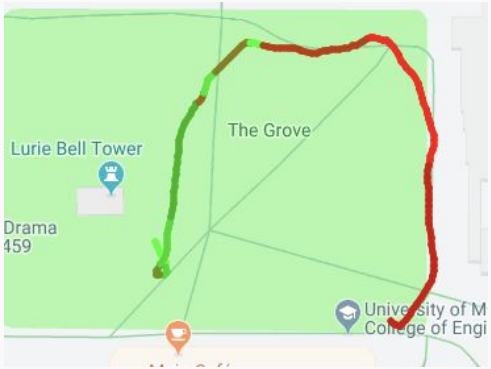
Experiments - Data Collection



bbaits_to_central

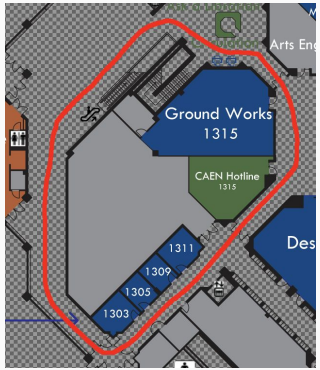


bbaits_to_north

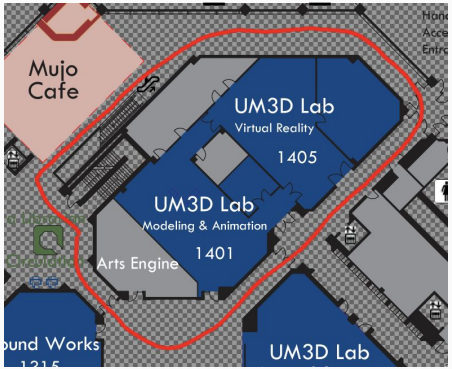


north_route_1

north_route_2



indoor_route_1



indoor_route_2

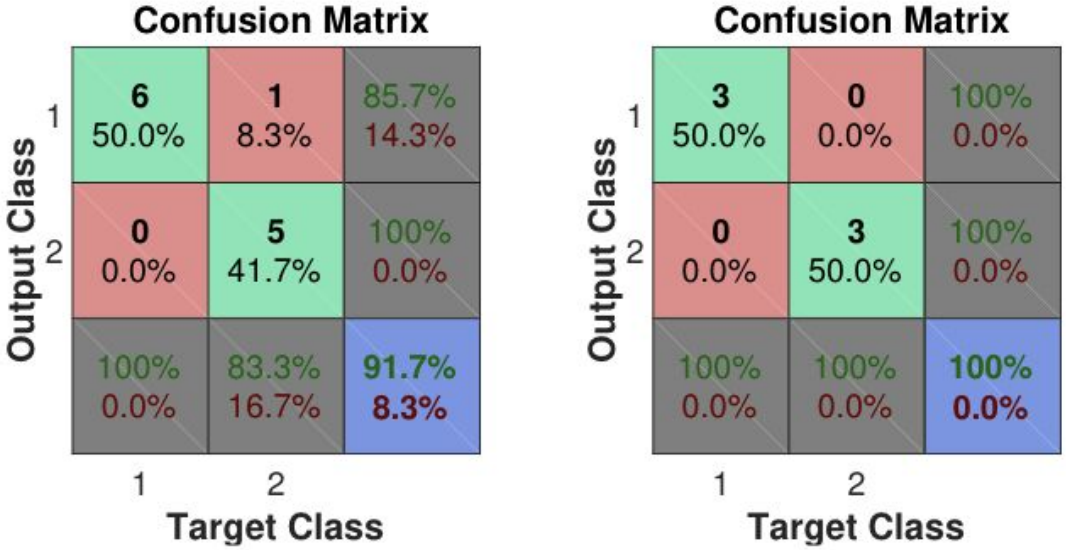
Experiments - Data Collection

- Device: Moto X4
- OS: Android 8.0
- Carrier: Google
- Environment:
  - Outdoor, taking bus
  - Outdoor, walking
  - Indoor, walking
- Network:
  - Cellular only
  - Wi-Fi only
  - Mixed (cellular + Wi-Fi)

Table 2: Sample number of each combination

Route	Cellular Only	Wifi Only	Mixed
bbaits_to_central	6	Not Applicable	3
bbaits_to_north	6	Not Applicable	3
north_route_1	6	6	6
north_route_2	6	6	6
indoor_route_1	6	6	6
indoor_route_2	6	6	6

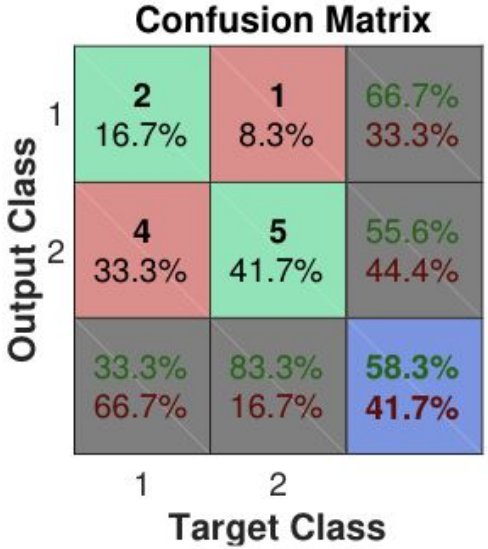
Experiments - Route Distinguishability



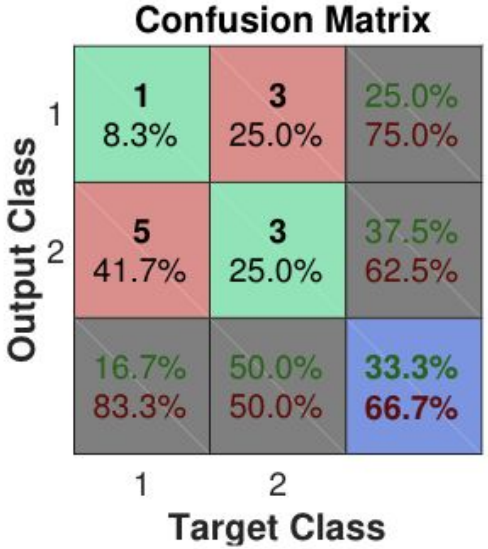
(a) Cellular network (b) Mixed network

Figure 5: Outdoor + Bus. Class 1 stands for `bbaits_to_central`, and class 2 for `bbaits_to_north`.

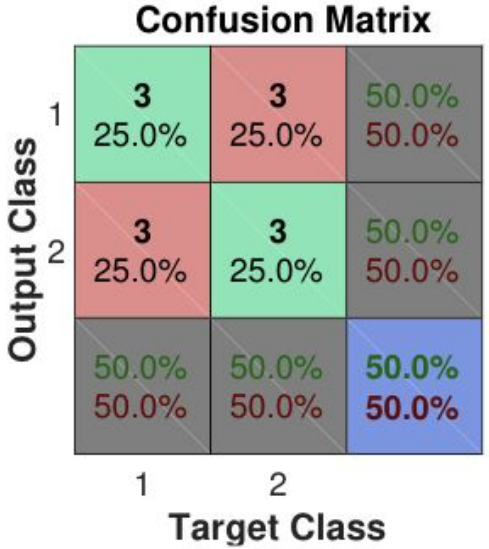
Experiments - Route Distinguishability



(a) Cellular network



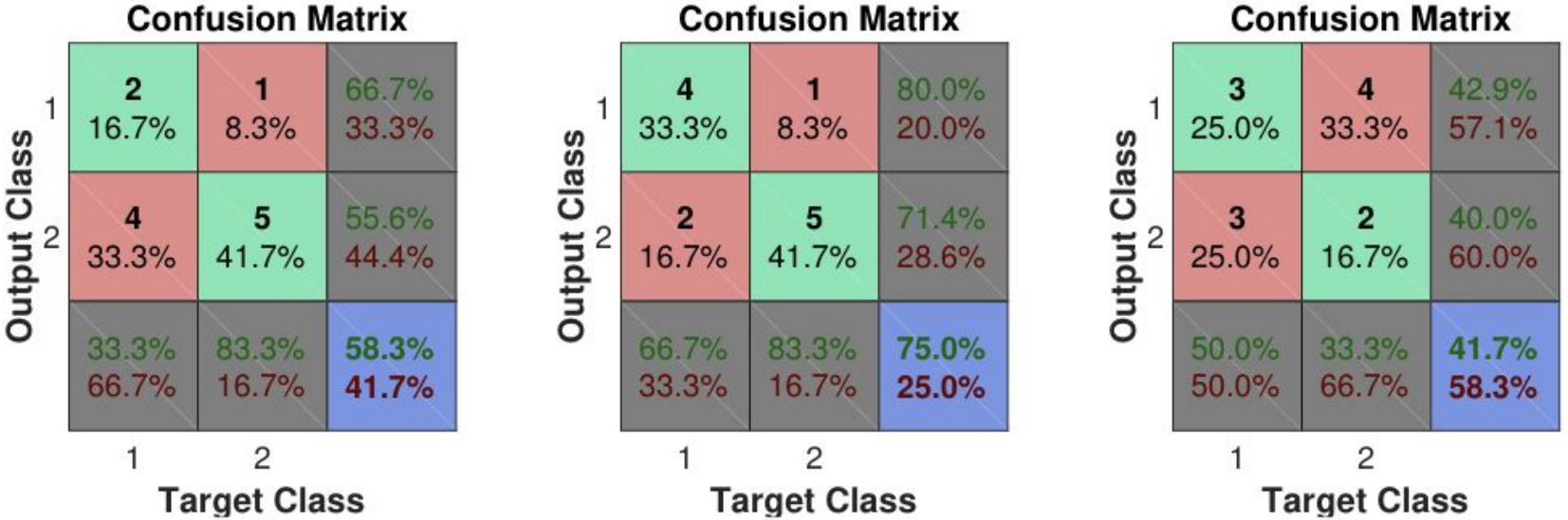
(b) Wi-Fi network



(c) Mixed network

Figure 6: Outdoor + Walk. Class 1 stands for `north_route_1`, and class 2 for `north_route_2`.

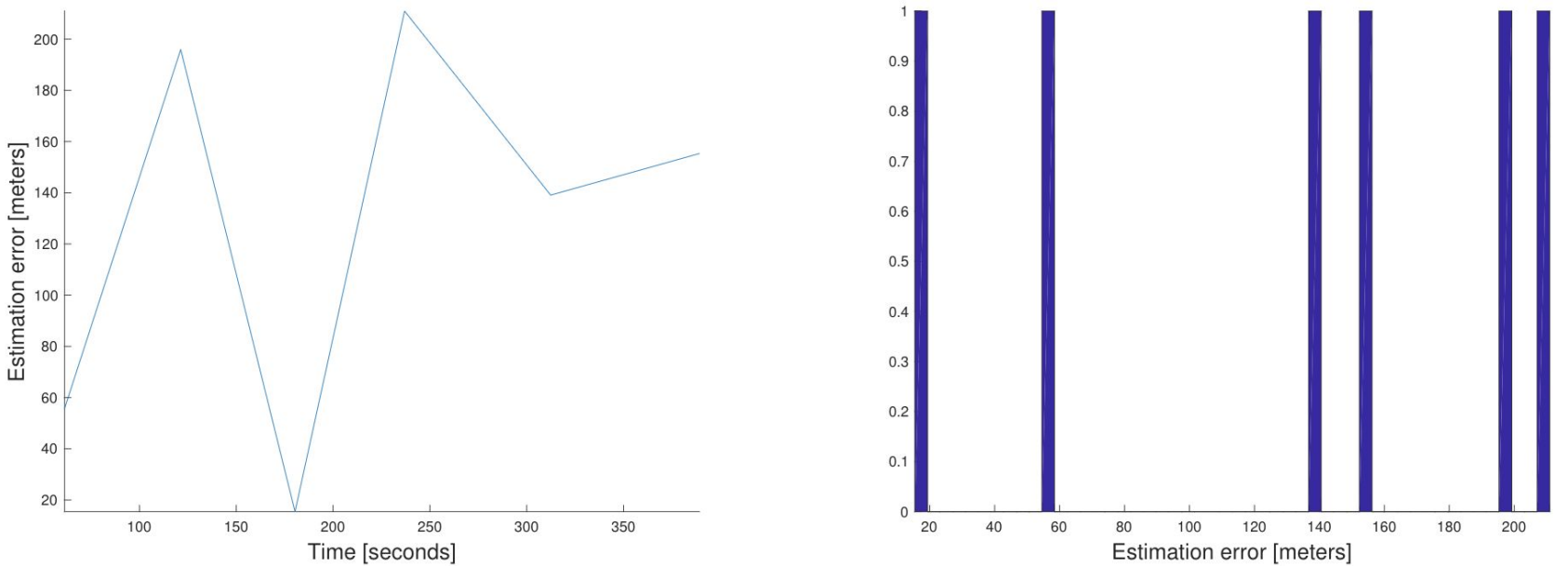
Experiments - Route Distinguishability



(a) Cellular network (b) Wi-Fi network (c) Mixed network

Figure 7: Indoor + Walk. Class 1 stands for `indoor_route_1`, and class 2 for `indoor_route_2`.

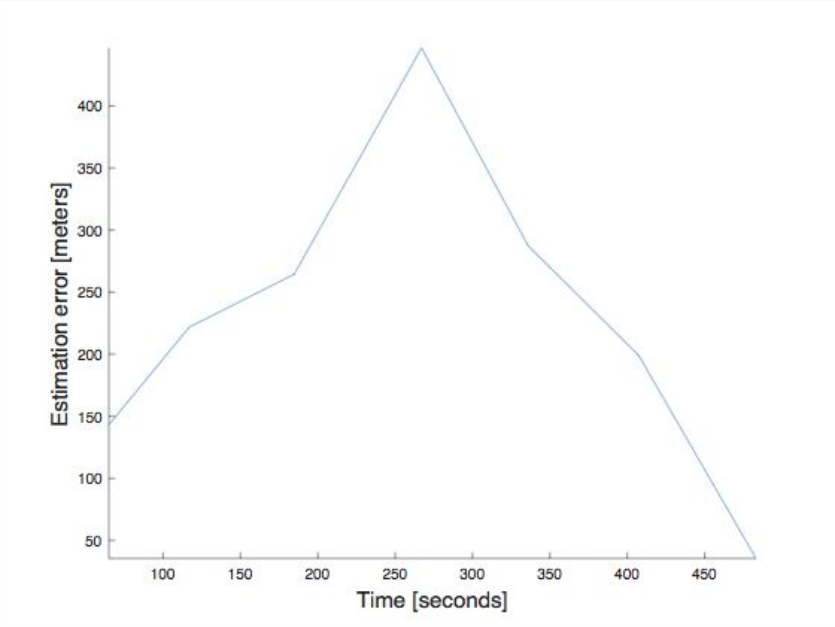
Experiments - Real-Time Tracking

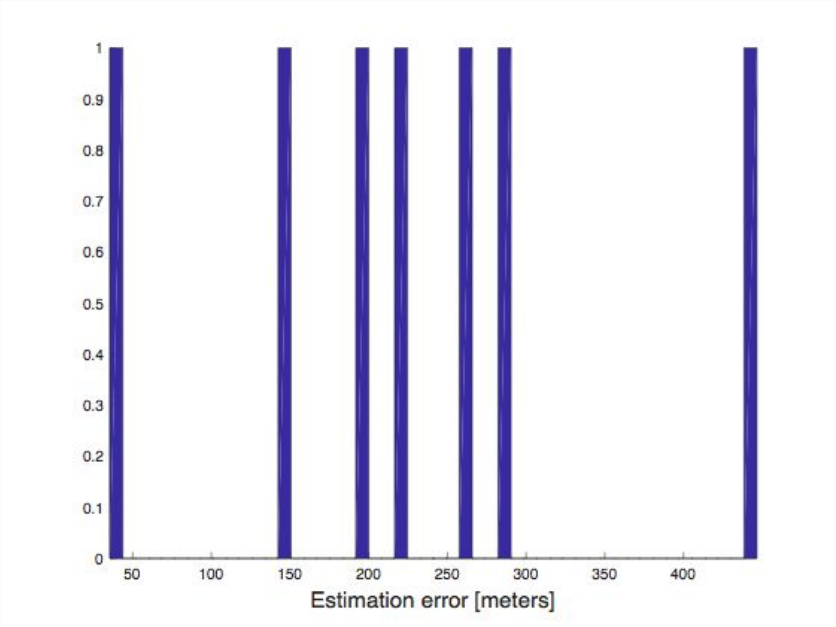


(a) Location estimation error. Route: bbaits-to-central (b) Error histogram.

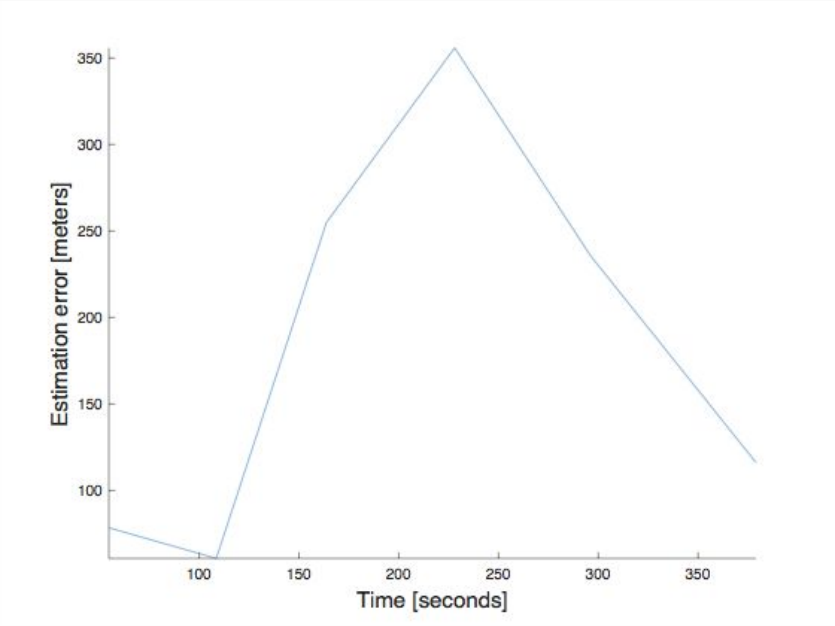
Figure 9: Estimation errors for motion-model tracking.

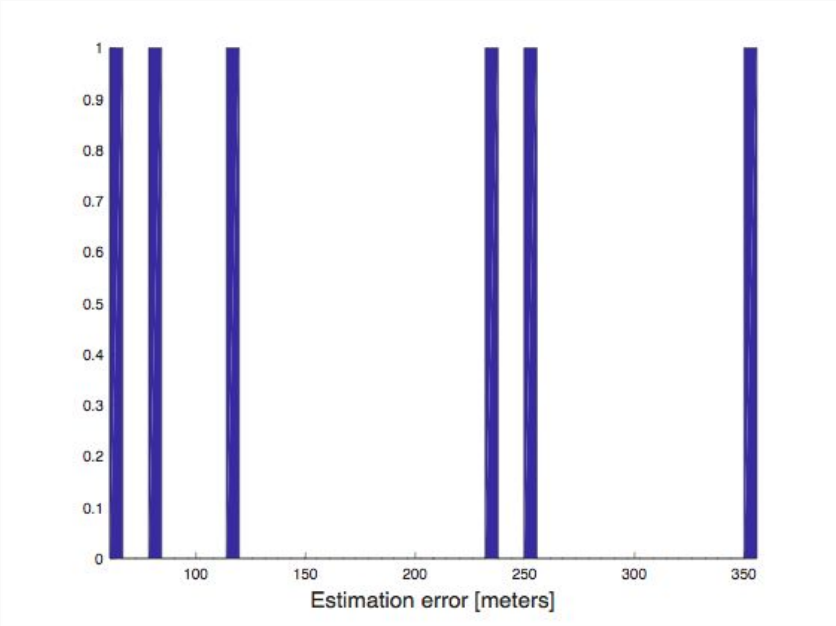
Experiments - Real-Time Tracking



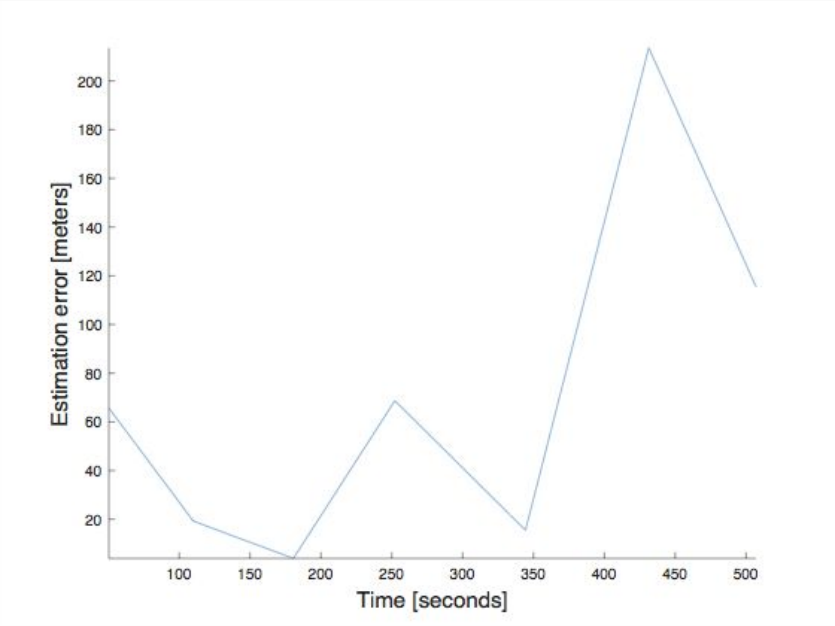


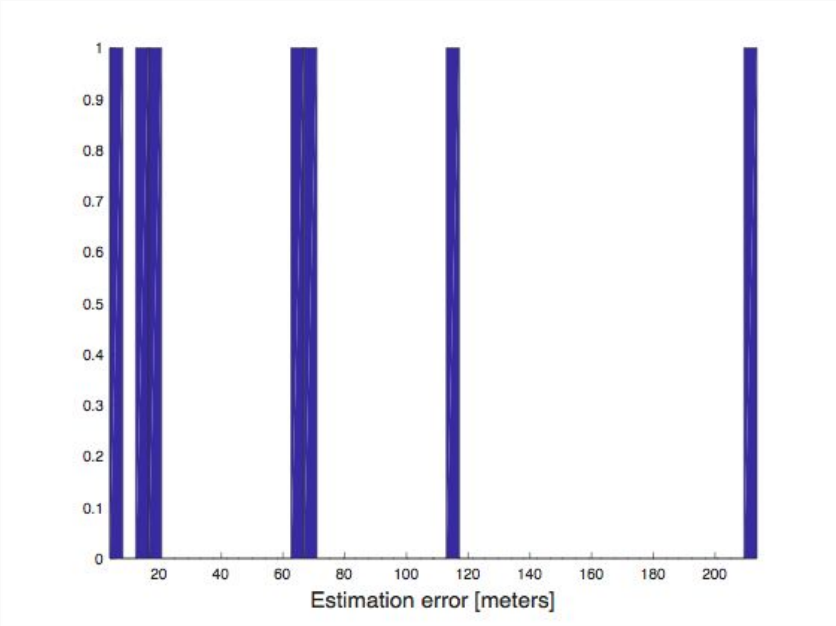
Experiments - Real-Time Tracking



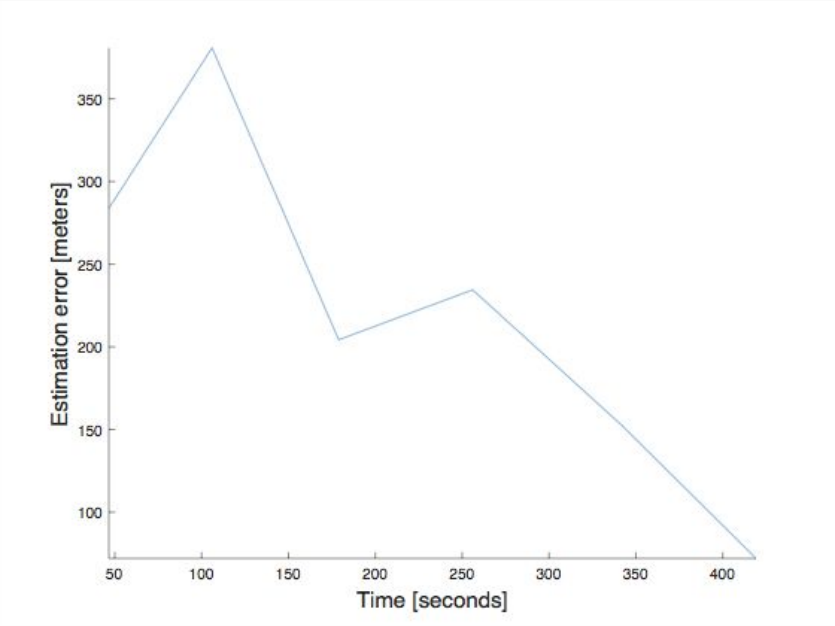


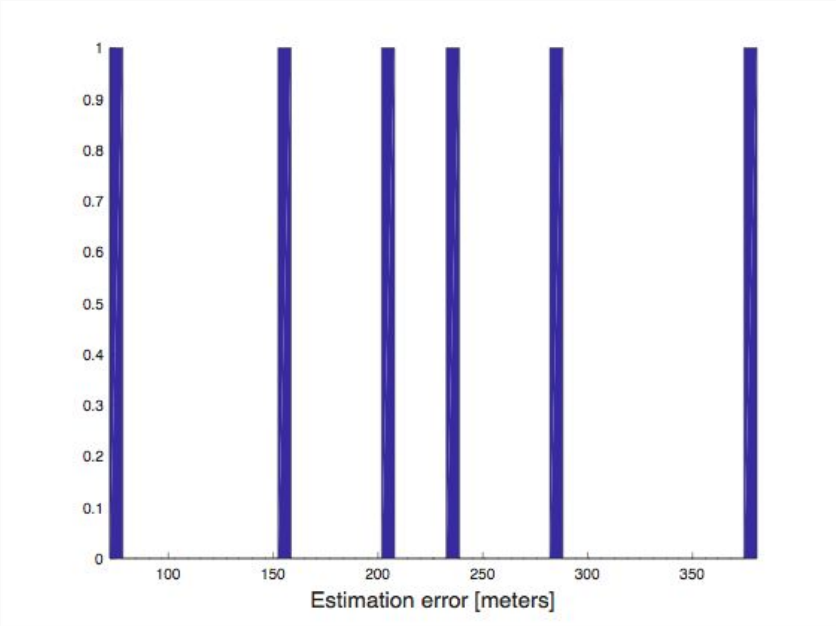
Experiments - Real-Time Tracking



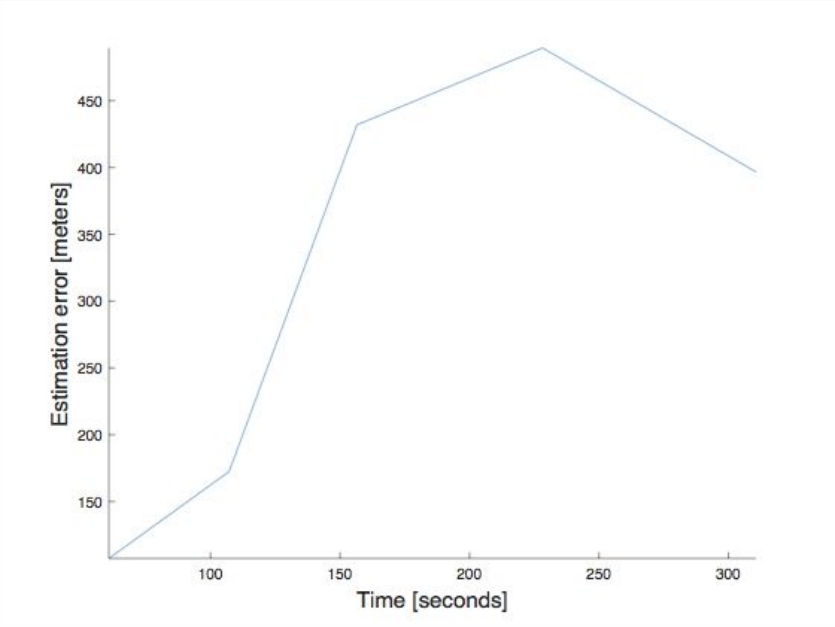


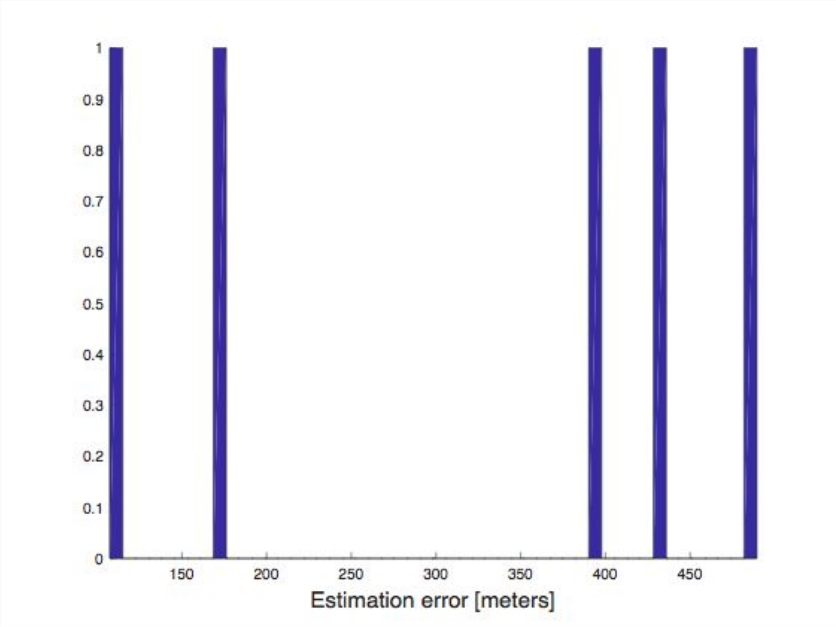
Experiments - Real-Time Tracking





Experiments - Real-Time Tracking





Discussion - Strength and Weakness Comparing to the Original Work

Strength:

(1) Fixed the hole of network vs GPS in their work.
(2) Take power traces once a time.
(3) Extend attack scenarios

Weakness:

(1) Lack of difference devices.
(2) Lack of routes

Discussion - Limitations

(1) Different carriers and change of base station configurations.

(2) Unable to track indoor.

(3) Interference of GPS and other noises.

Conclusion

The threat model has changed significantly. However, information is still leaked out during the reproduction, which implies no defense has been deployed on either hardware level or system level.

Furthermore, we find that such attack is also available under indoor and WiFi-only condition. Such finding does not only extend the threat model but also draws attention to what else may be leaked through power consumption information.

Q&A