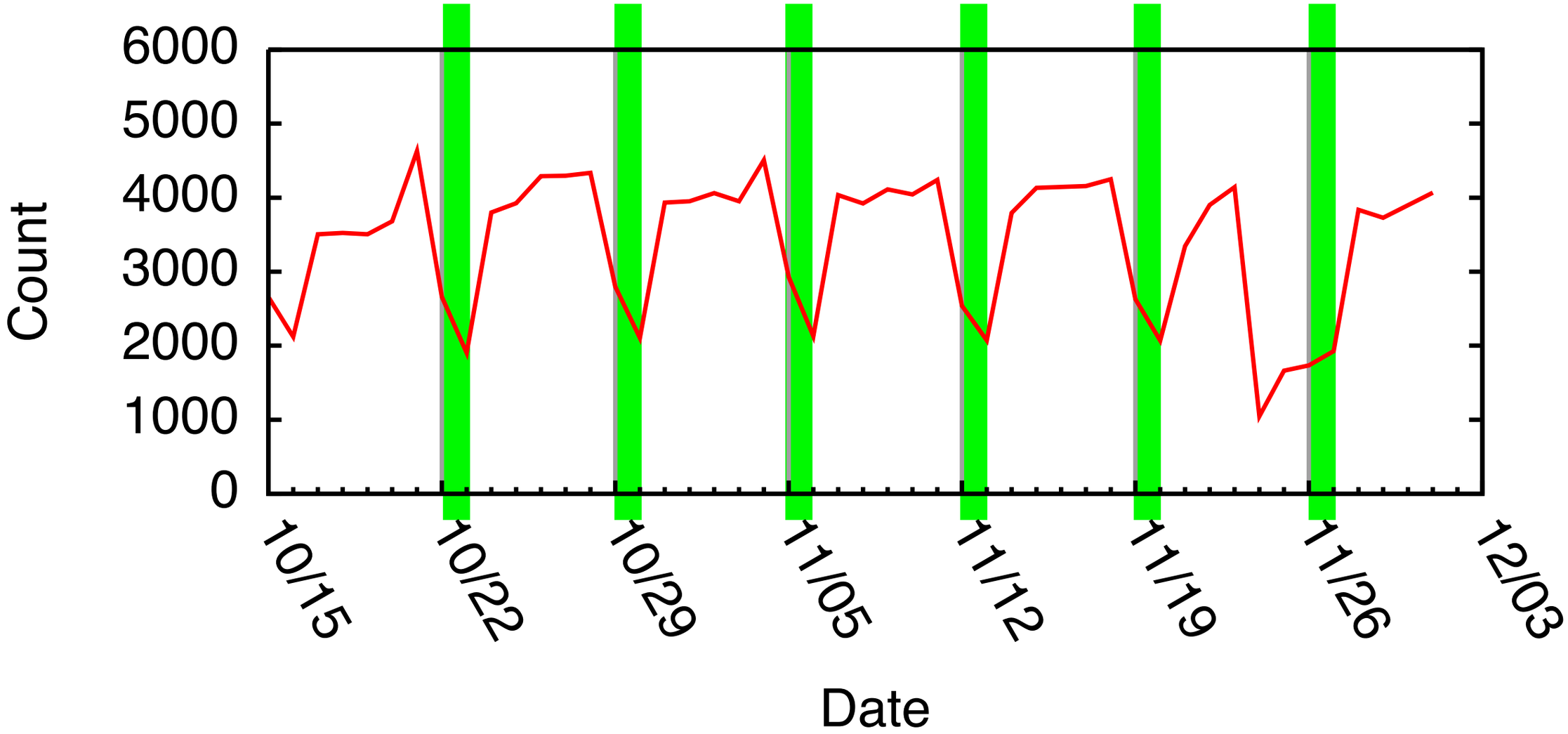
Tracking Unmodified Smartphones Using Wi-Fi Monitors

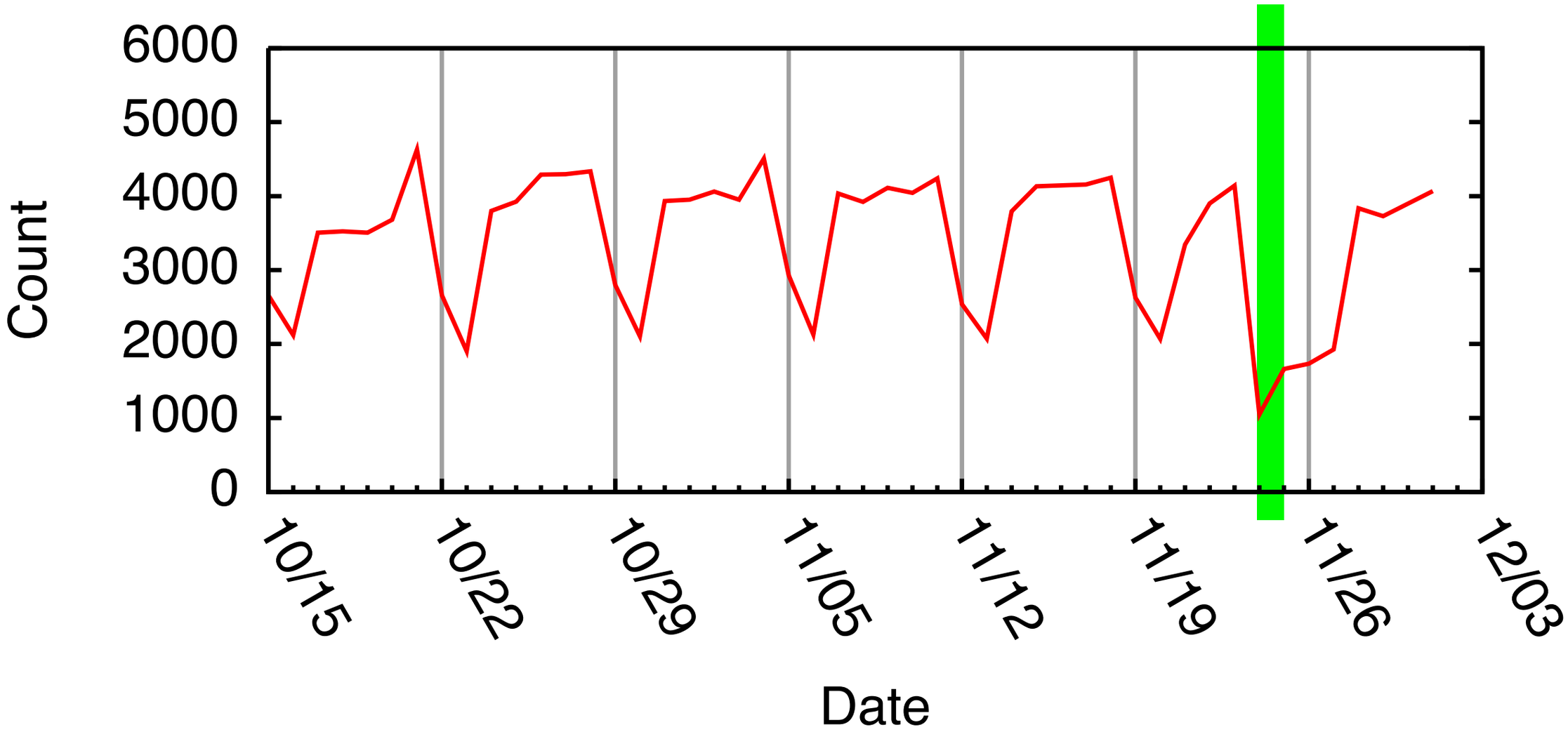
A.B.M. Musa, Jakob Eriksson

UIC UNIVERSITY OF ILLINOIS AT CHICAGO
Bits Networked Systems Laboratory
COLLEGE OF ENGINEERING

A curious pattern...



A curious pattern...

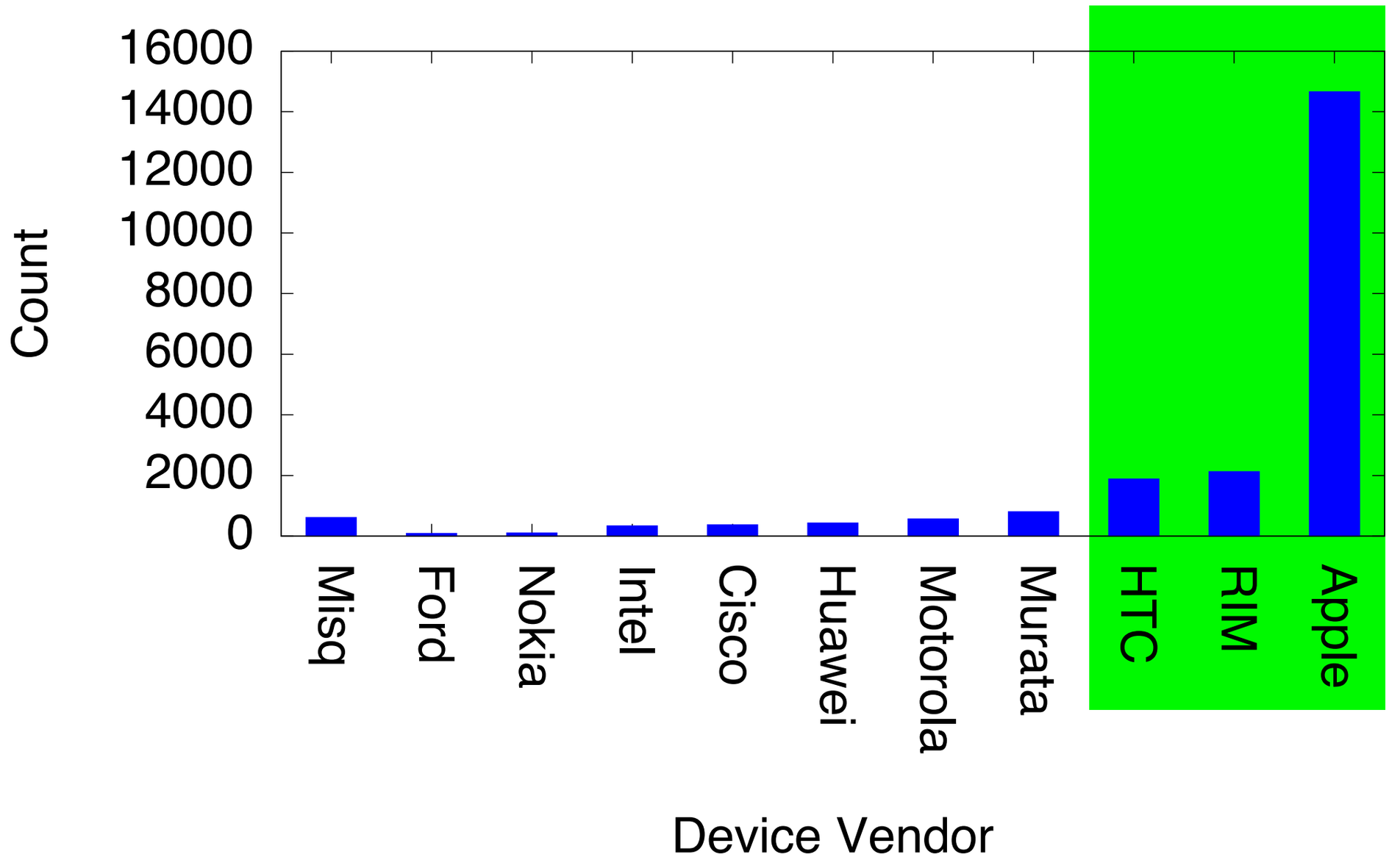


Organizationally Unique Identifier (OUI)

00:0a:27:b7:89:91

Apple Computer, Inc.

00:0a:27:b7:89:91



What could it possibly be?

Could we track them?

Could we track them?

Trajectory estimation from detections

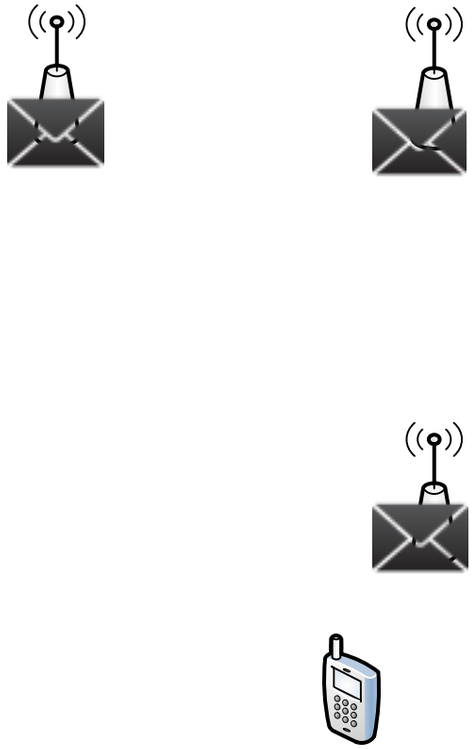
Outline of the talk

- System overview
- Trajectory estimation
- Prompting additional transmissions
- Tracking coverage and accuracy

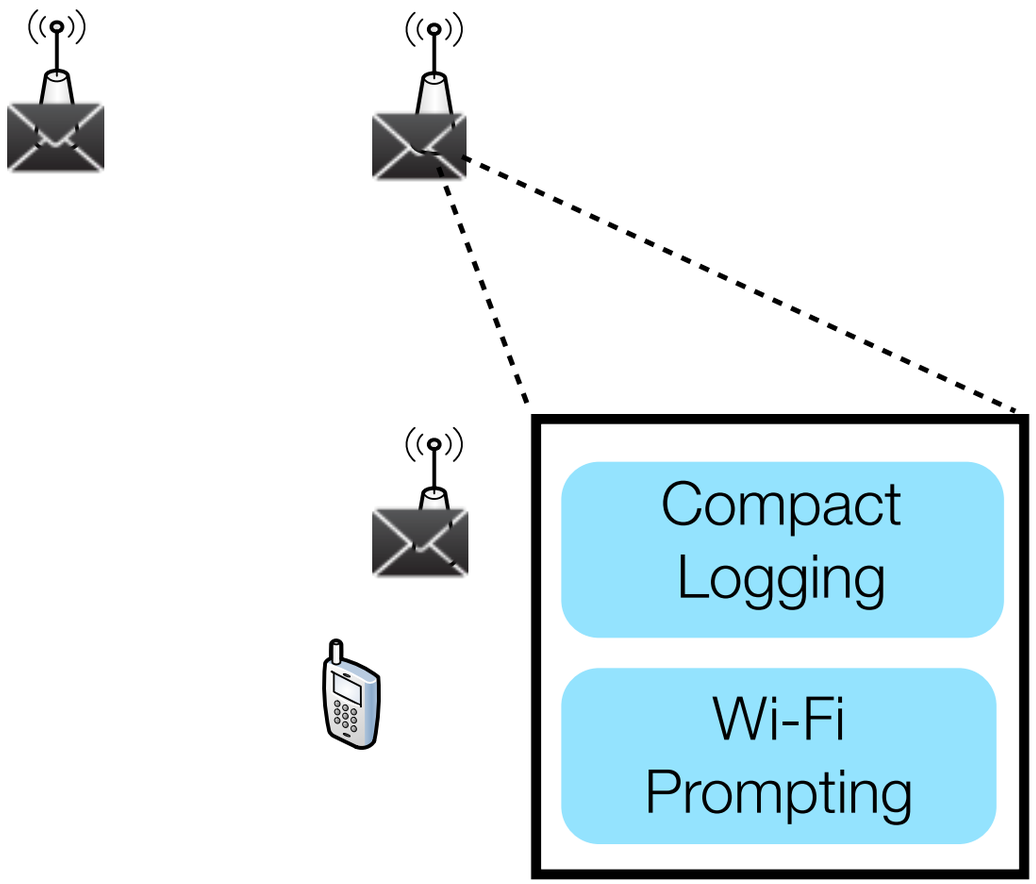
System overview

System overview

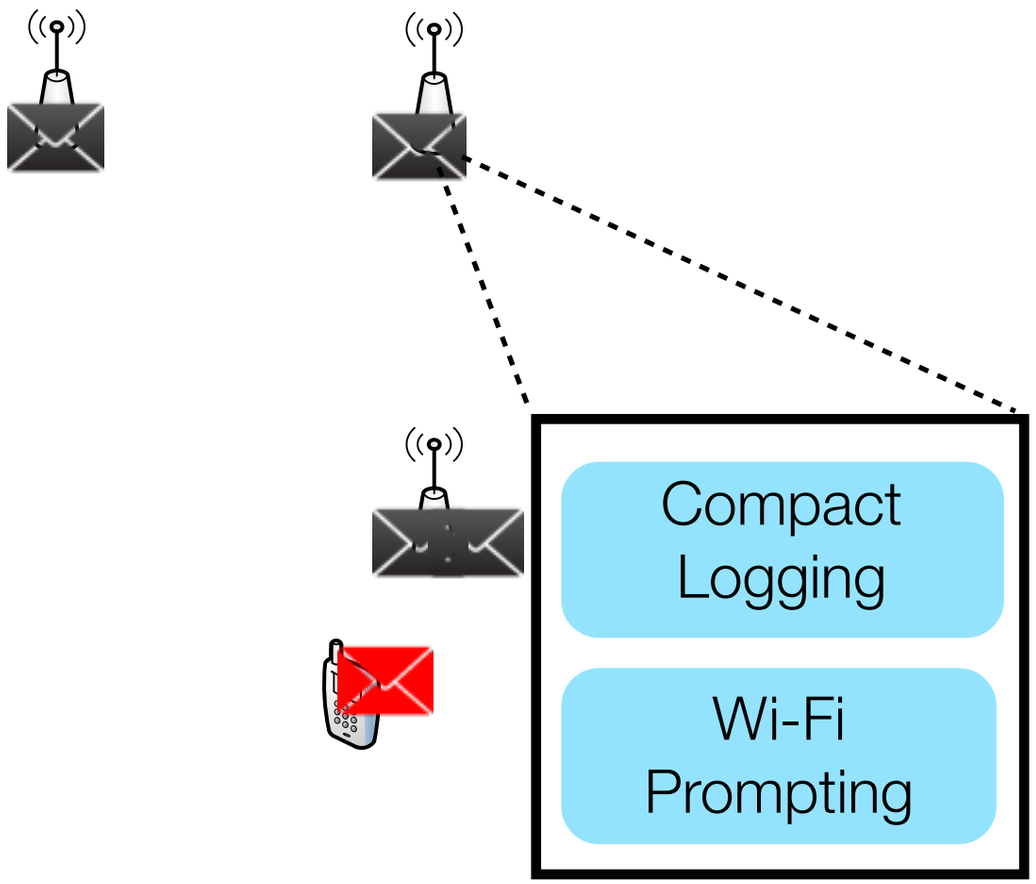
System overview



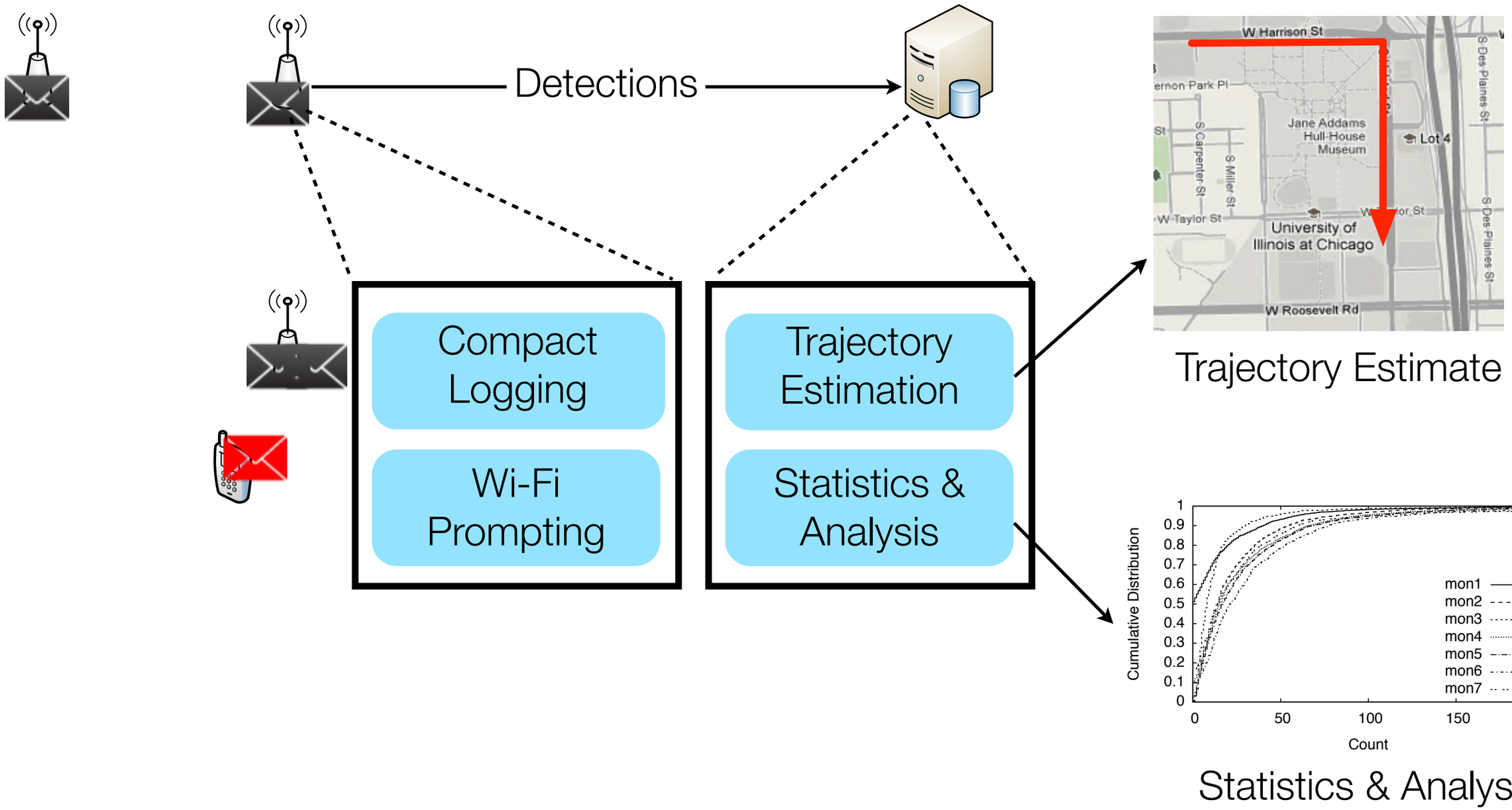
System overview



System overview



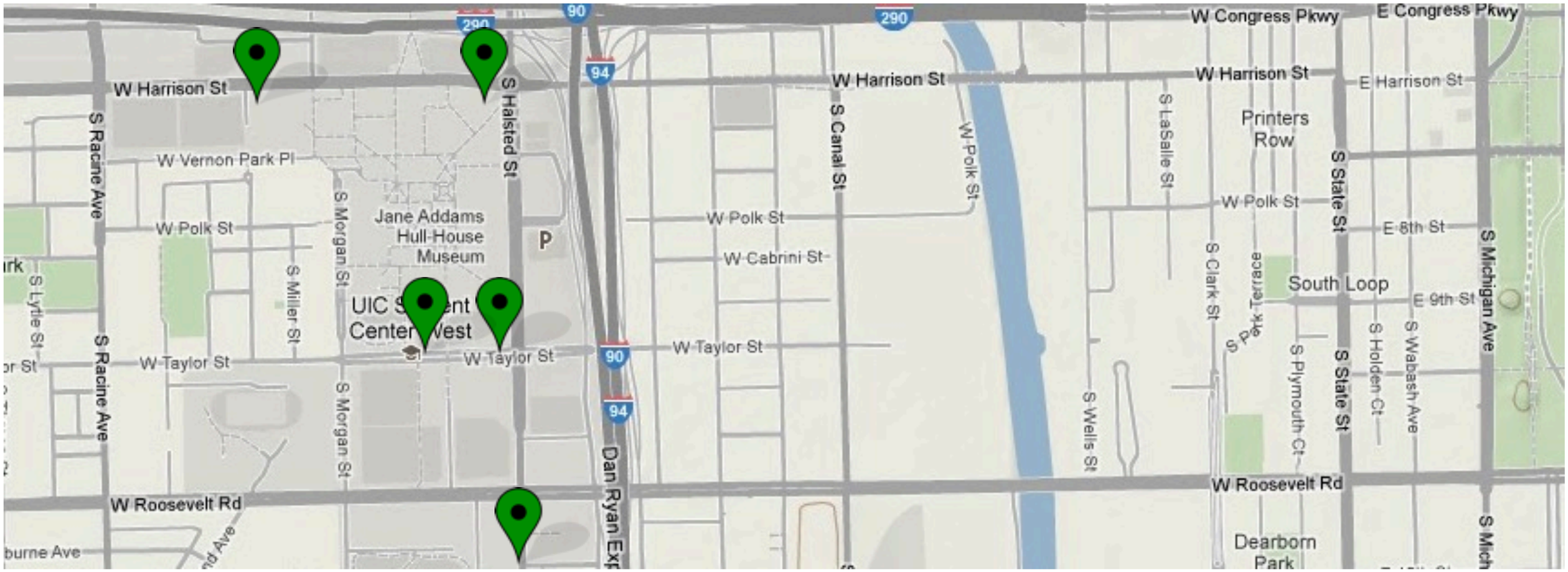
System overview



Trajectory Estimate

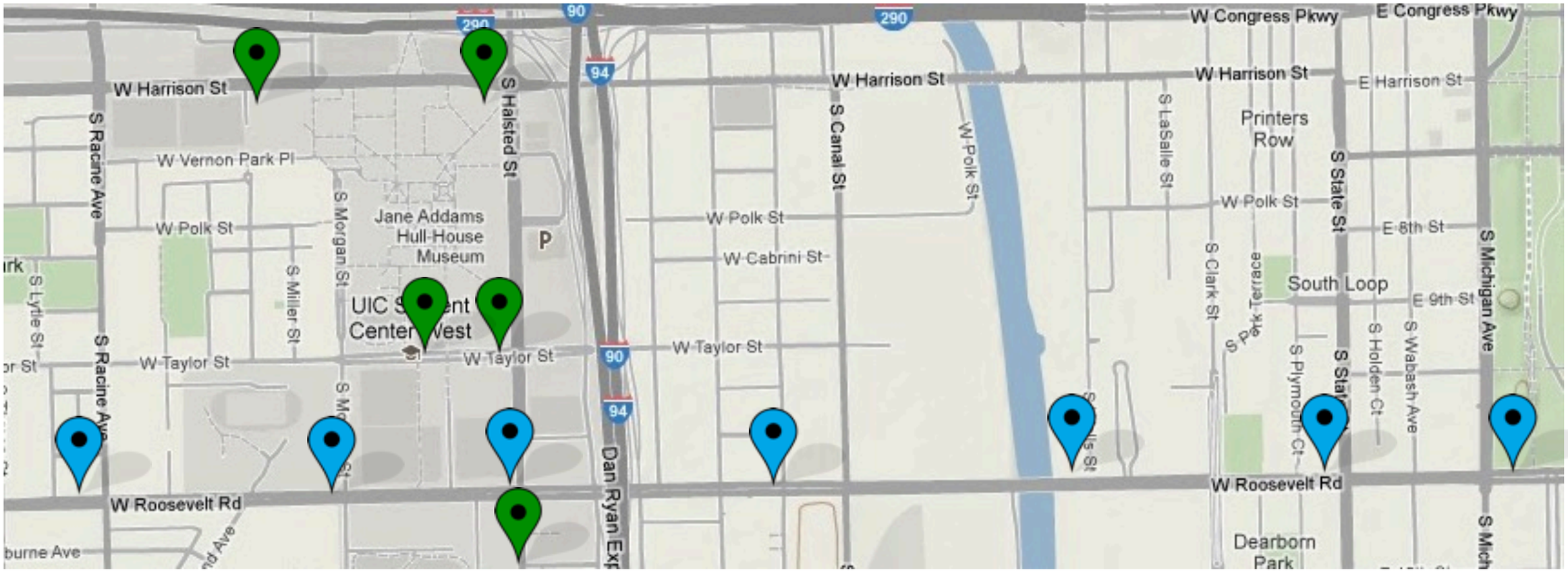
Statistics & Analysis

Deployment



Permanent 9 months

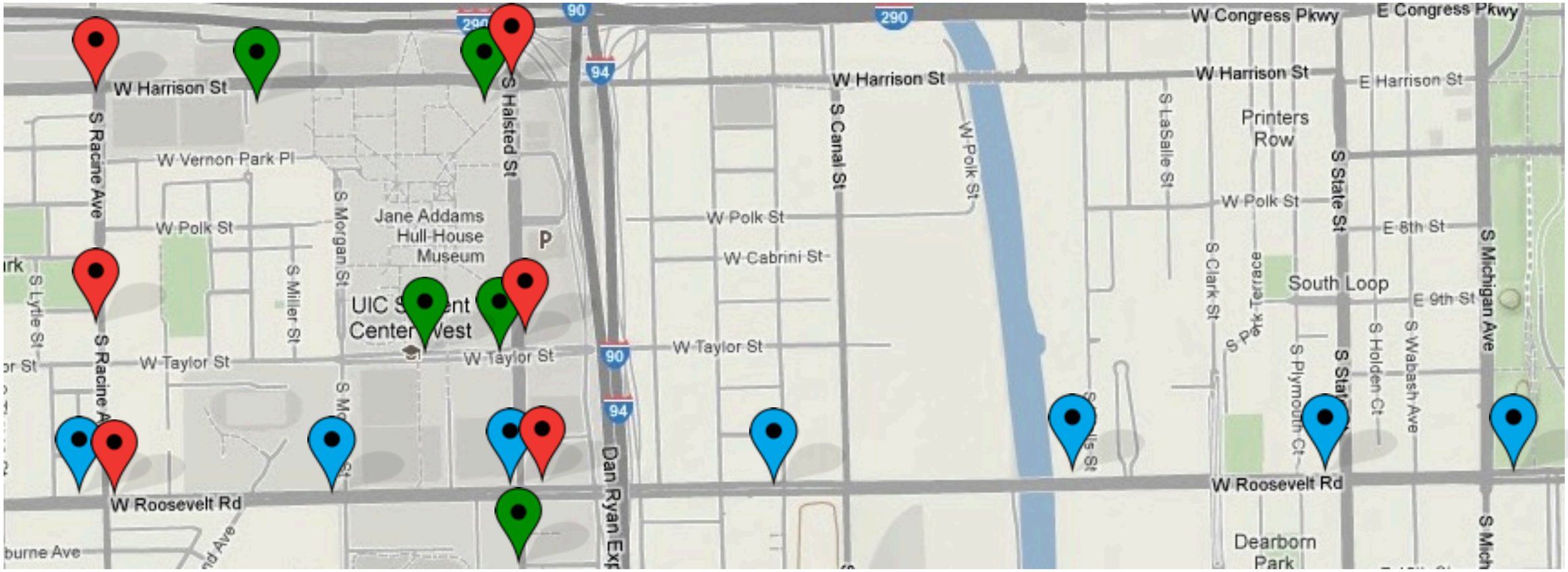
Deployment



Permanent 9 months

2.8 km straight

Deployment



Permanent 9 months

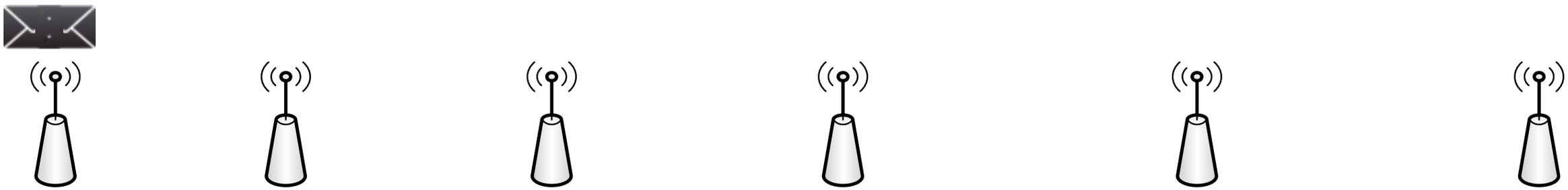
2.8 km straight

3.2 km rectangular

Trajectory Estimation

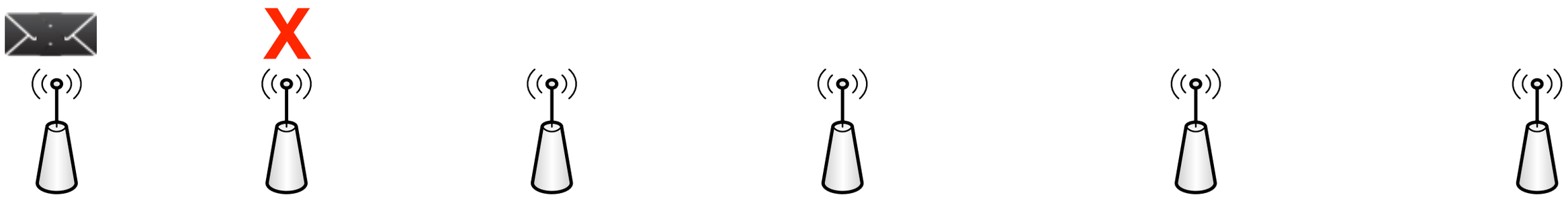
The problem at hand...

The problem at hand...



ideal
case

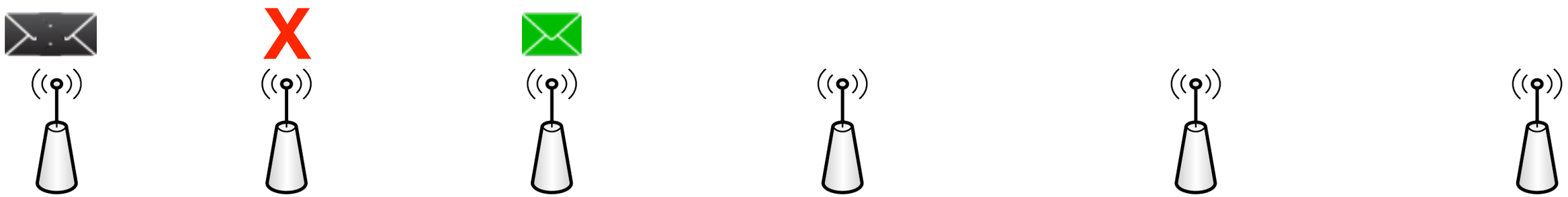
The problem at hand...



ideal case

nothing received

The problem at hand...

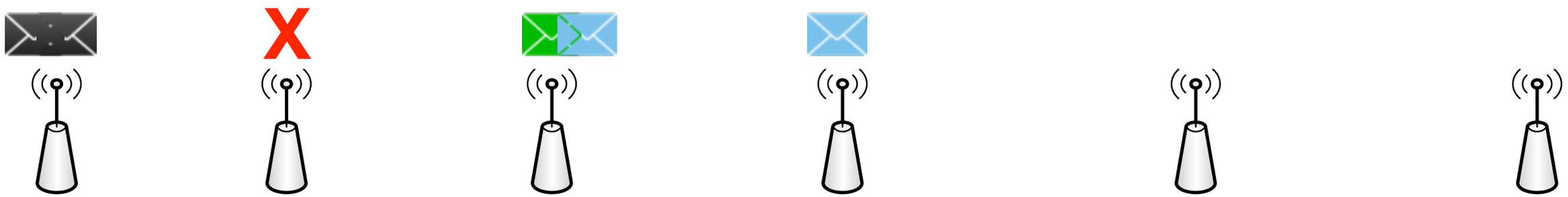


ideal case

nothing received

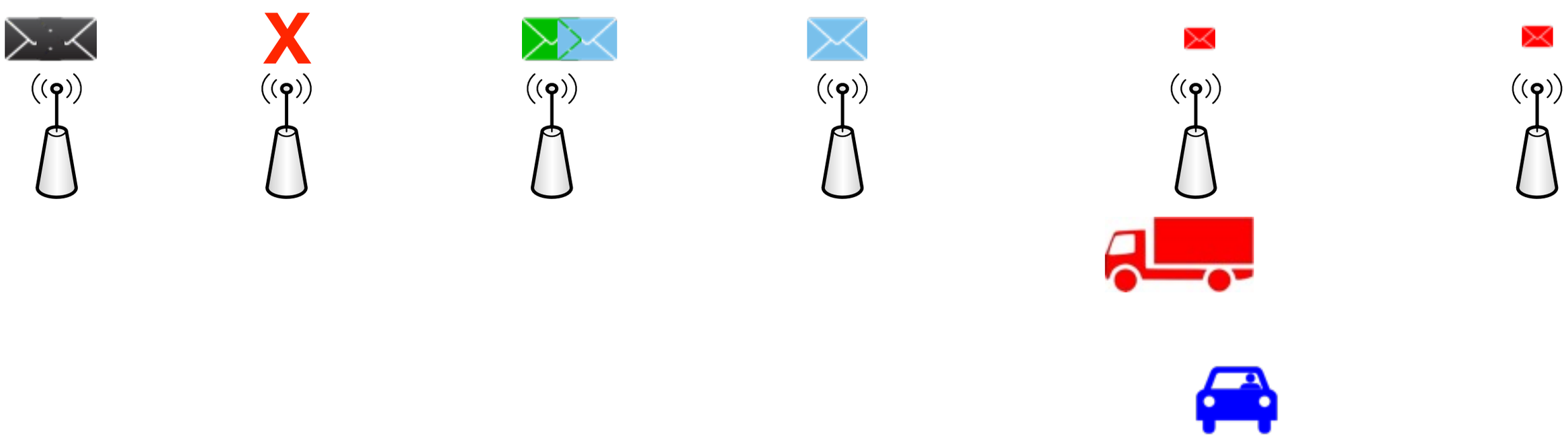
single packet

The problem at hand...



ideal case	nothing received	single packet	ambiguous reception

The problem at hand...



ideal case

nothing received

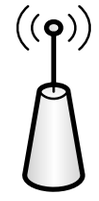
single packet

ambiguous reception

fading and path loss

Straw-man approach

Straw-man approach



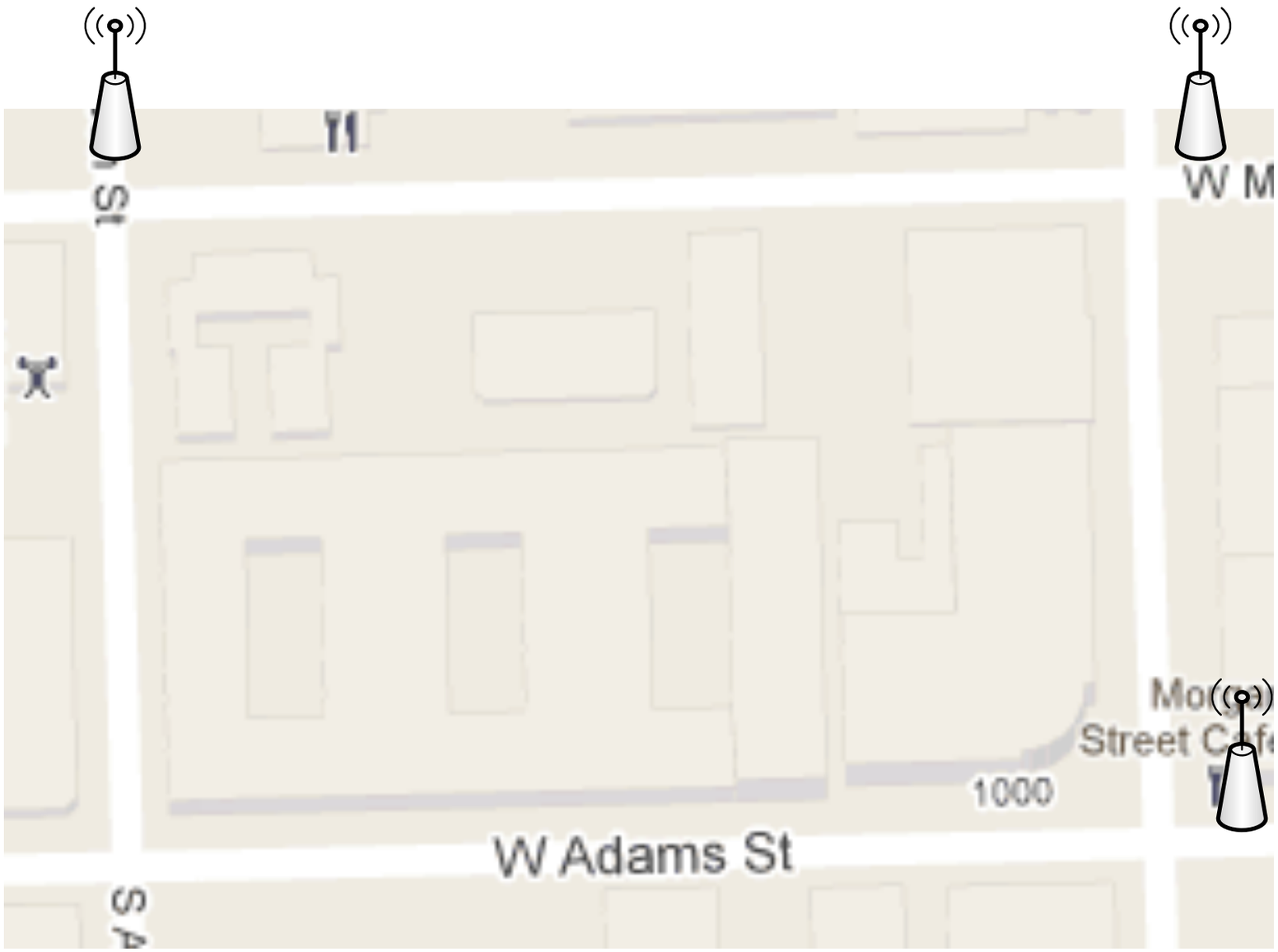
Straw-man approach

Straw-man approach

Straw-man approach

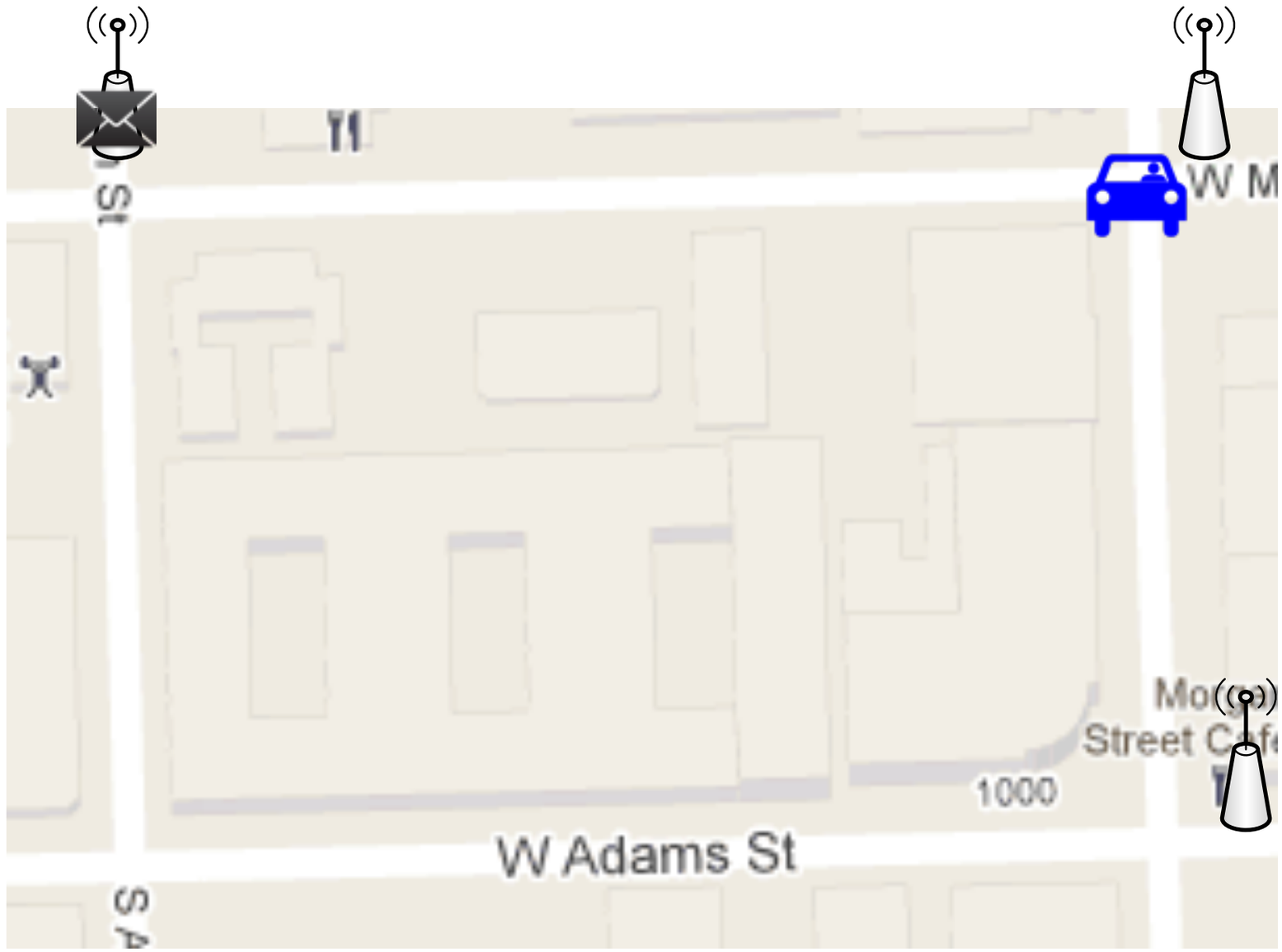
Straw-man approach

Straw-man limitations

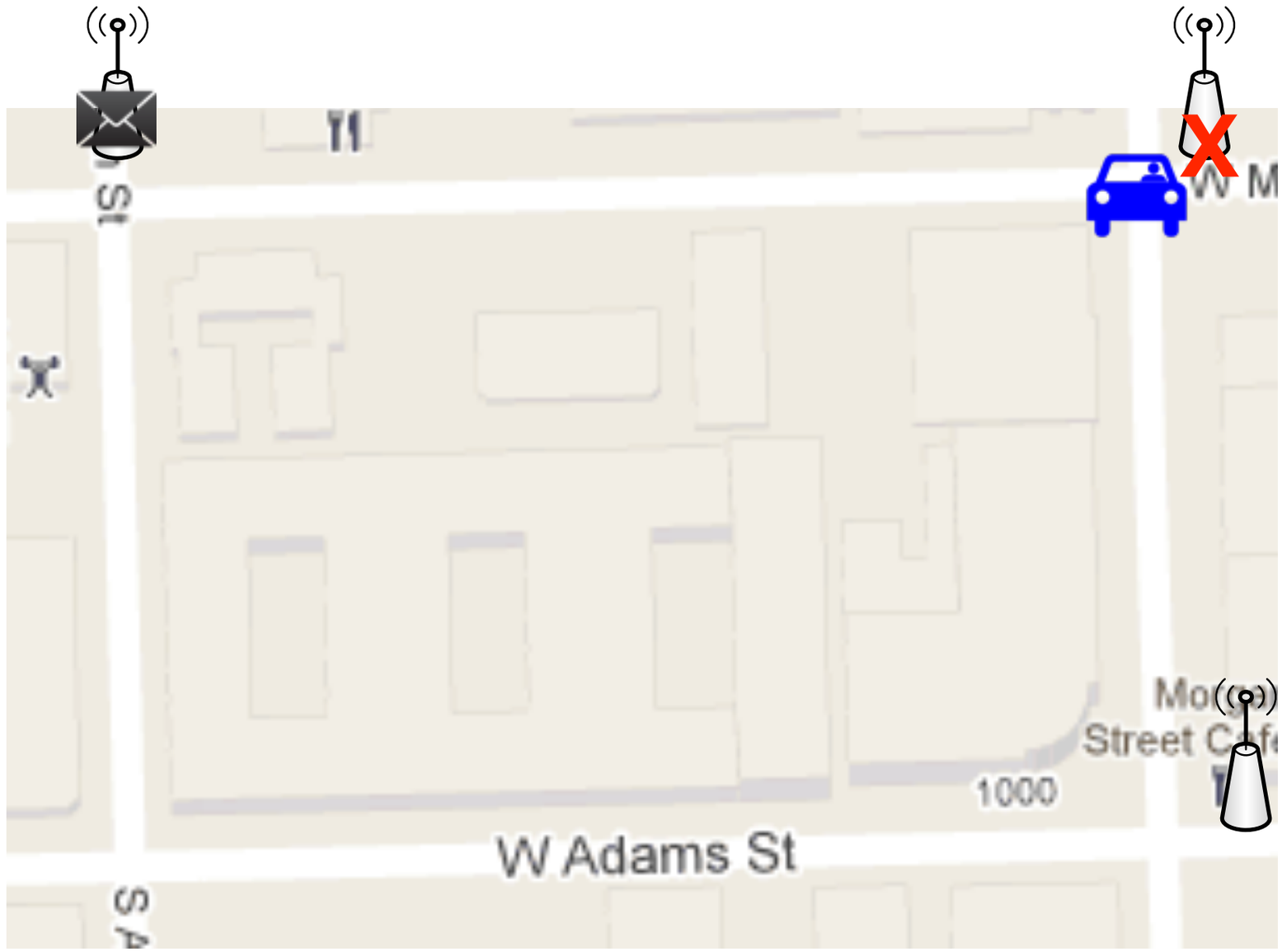


Straw-man limitations

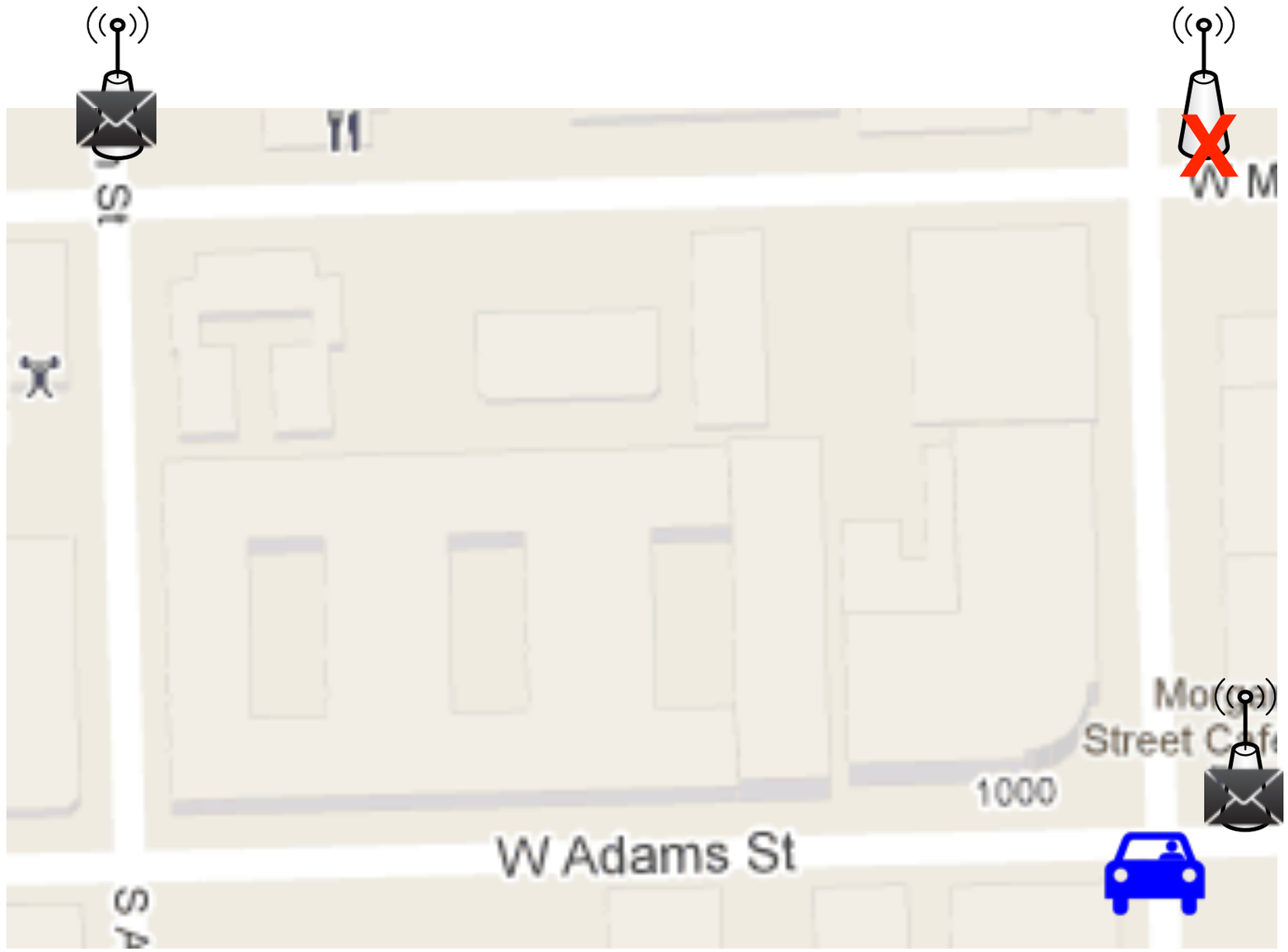
Straw-man limitations



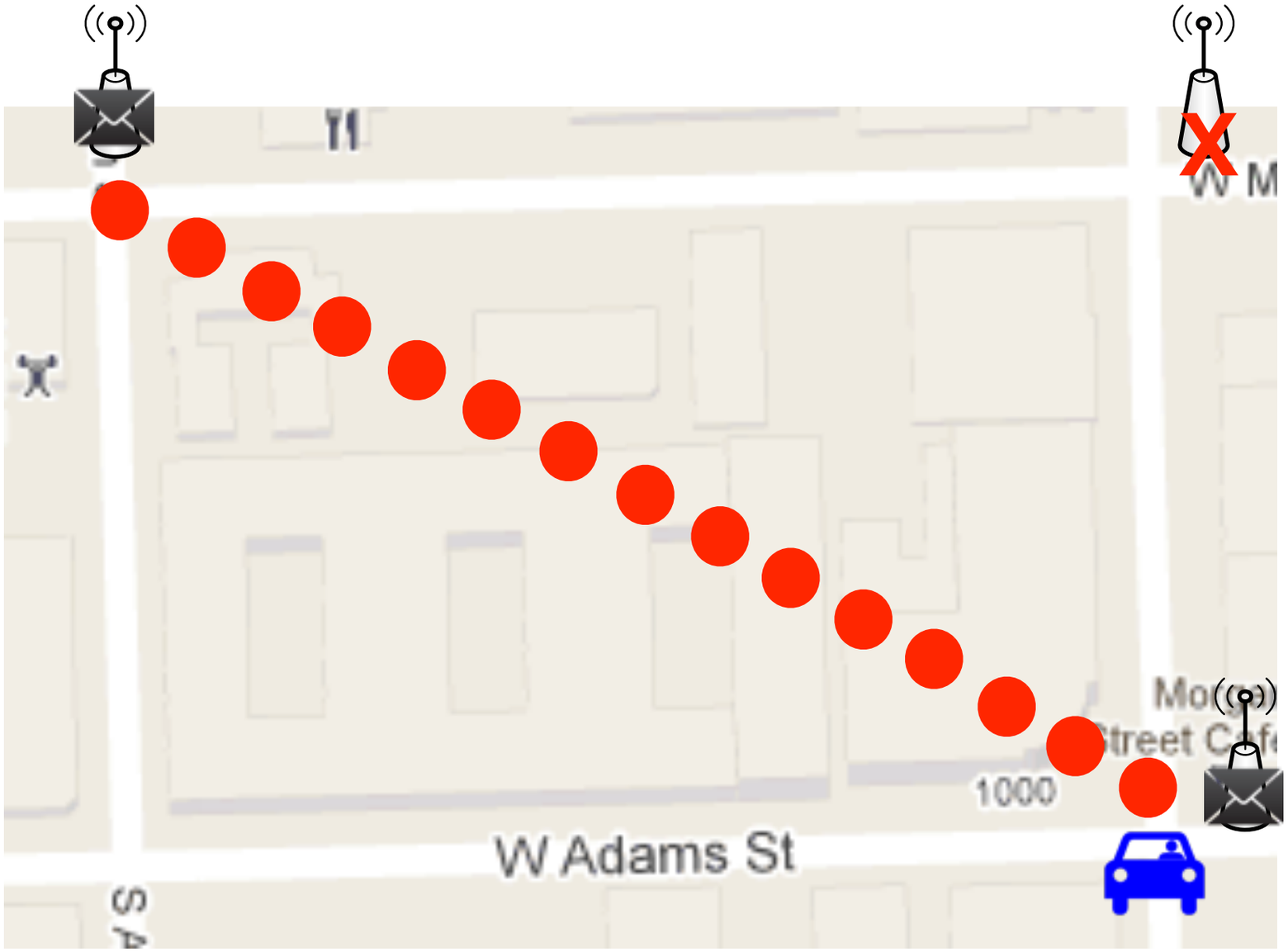
Straw-man limitations



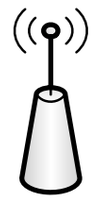
Straw-man limitations



Straw-man limitations

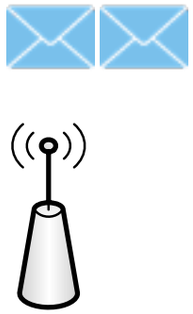


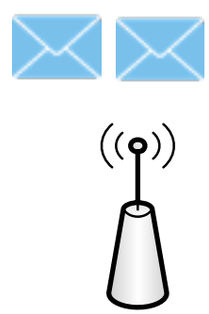
Straw-man's limitations



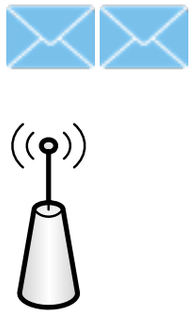
Straw-man's limitations

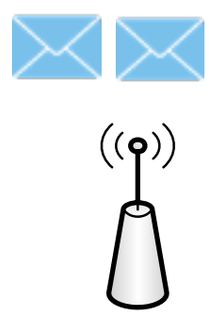
Straw-man's limitations



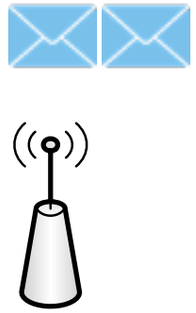


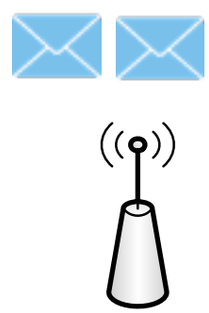
Straw-man's limitations



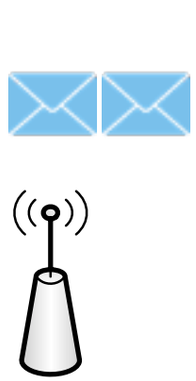


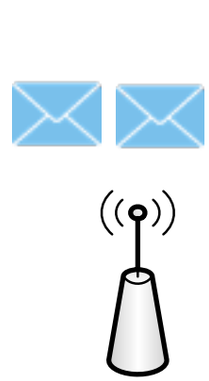
Straw-man's limitations





Straw-man's limitations



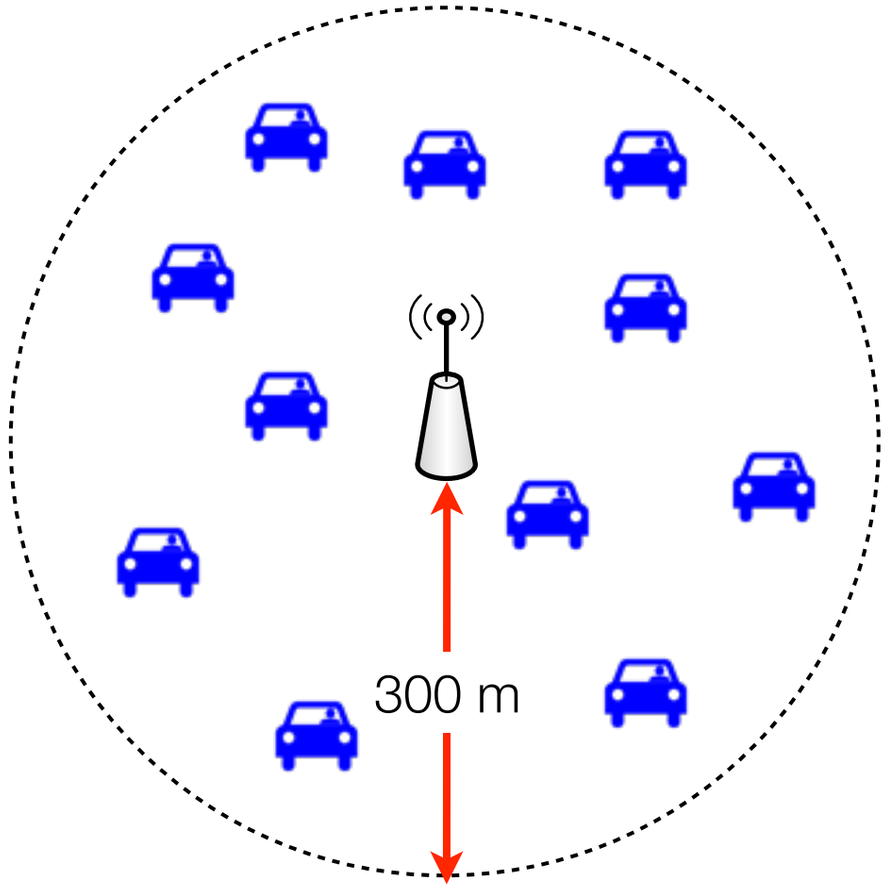


How to fix our straw-man

Impose a graph topology (map) on movements

How to fix our straw-man

Impose a graph topology (map) on movements



Resolve positional ambiguities

The HMM recipe

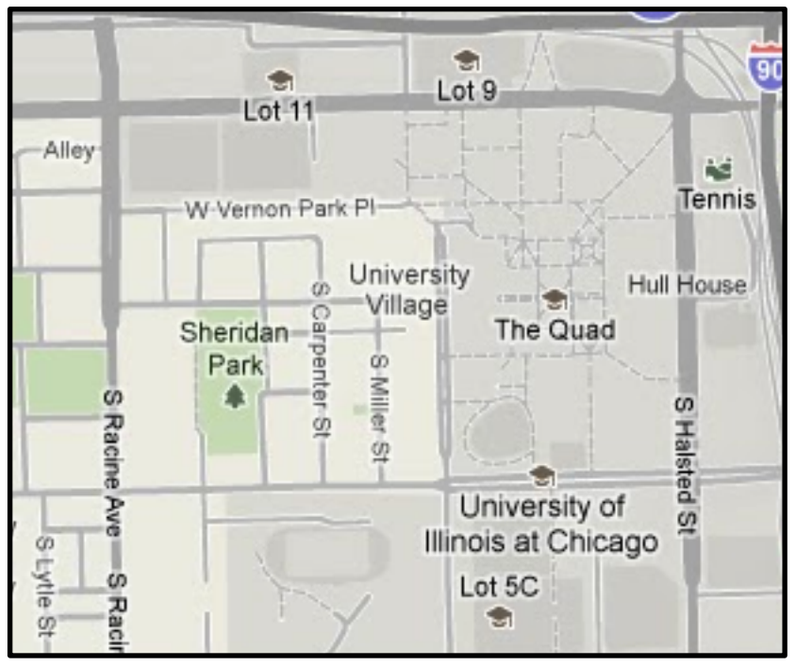
- “hidden” states
- transition probabilities
- emission probabilities

The HMM recipe

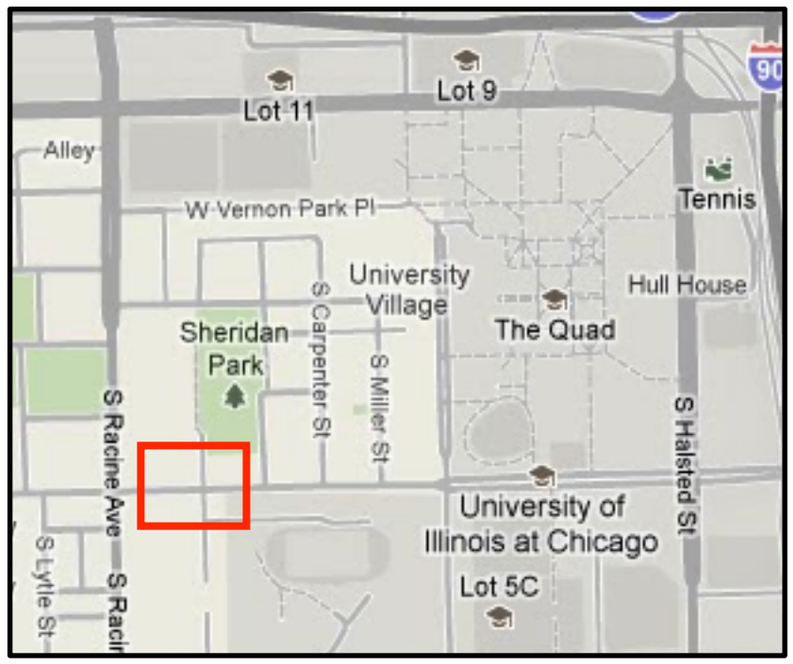
- “hidden” states
- transition probabilities
- emission probabilities

- shaken, not stirred

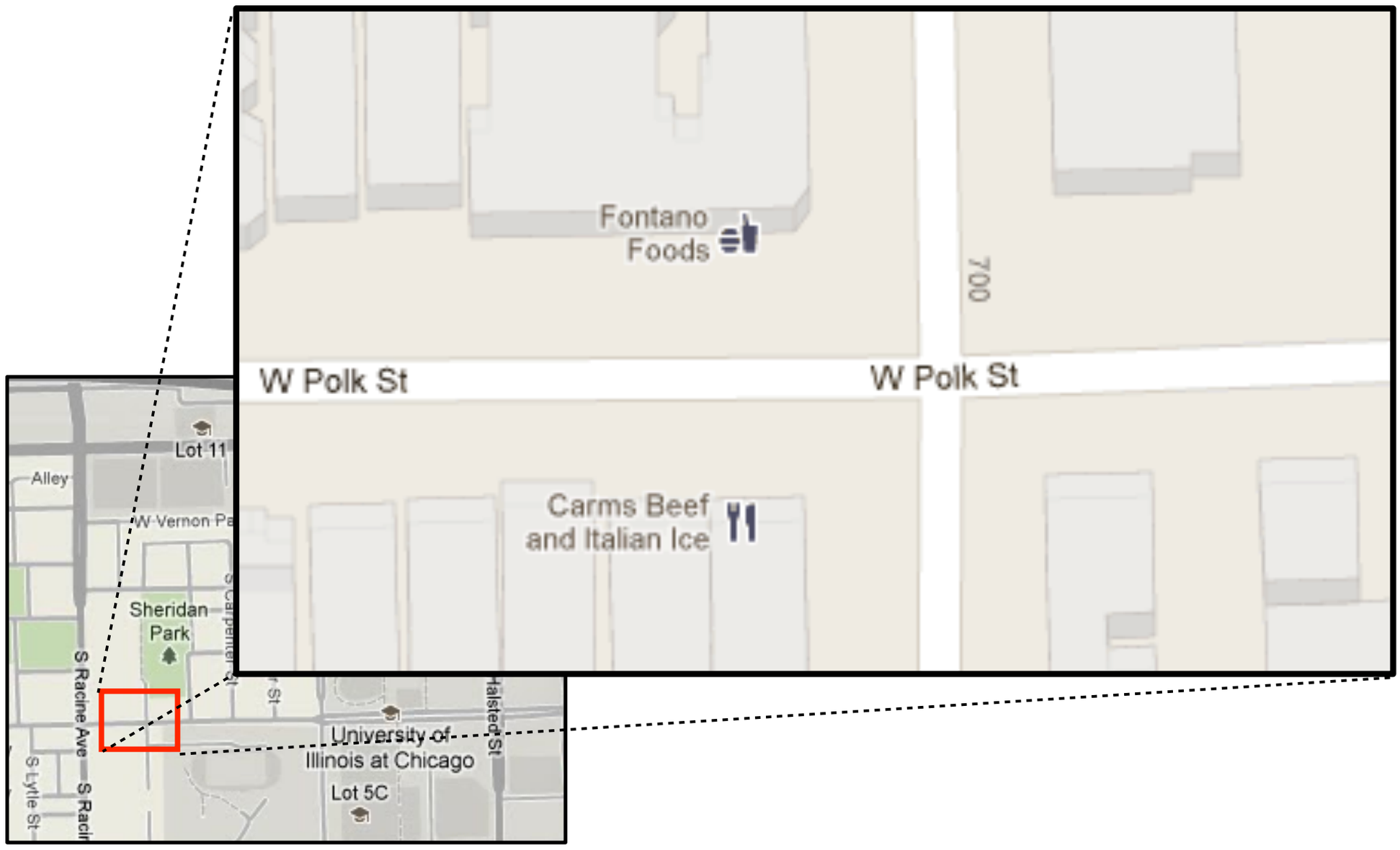
States & transition probabilities



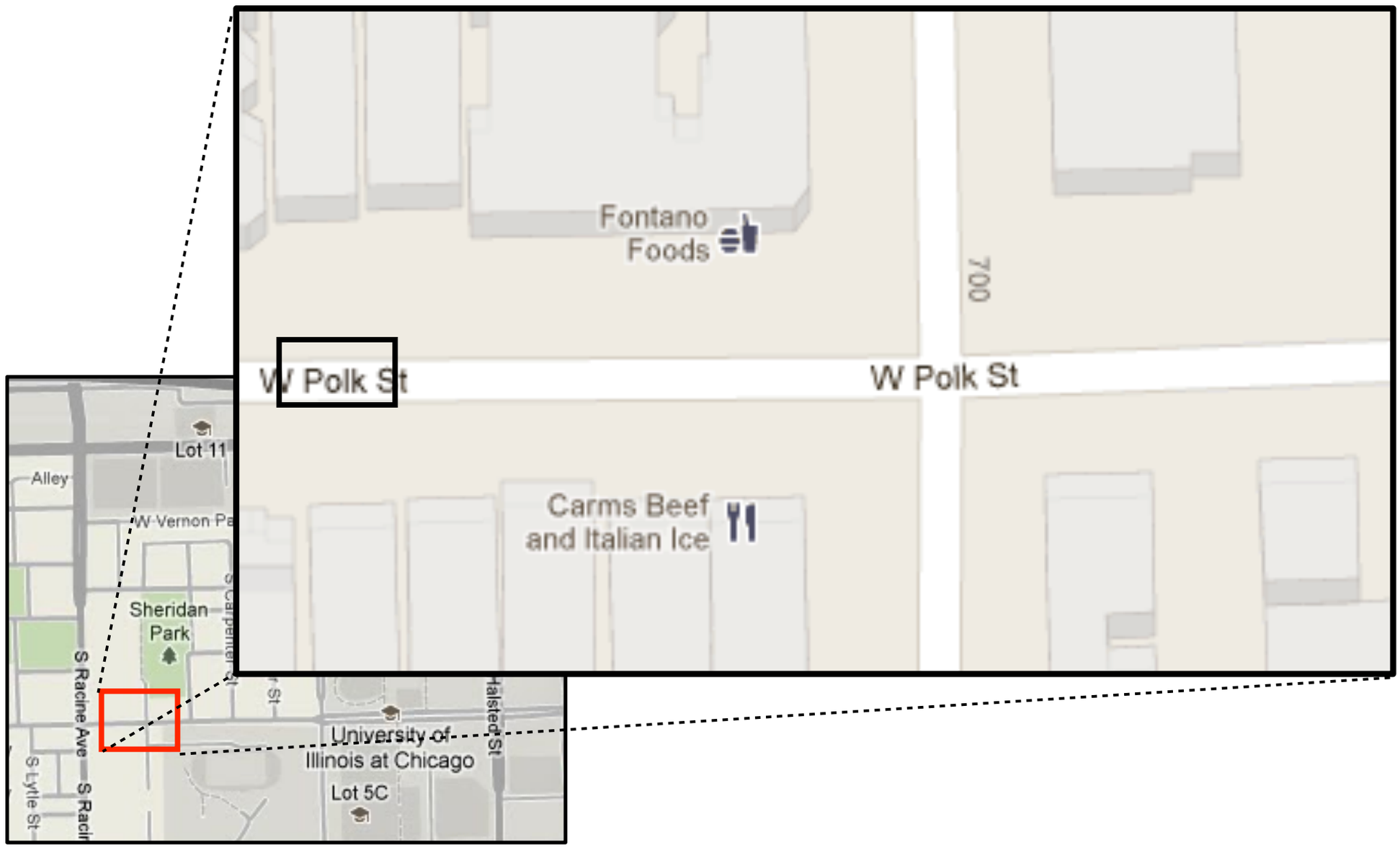
States & transition probabilities



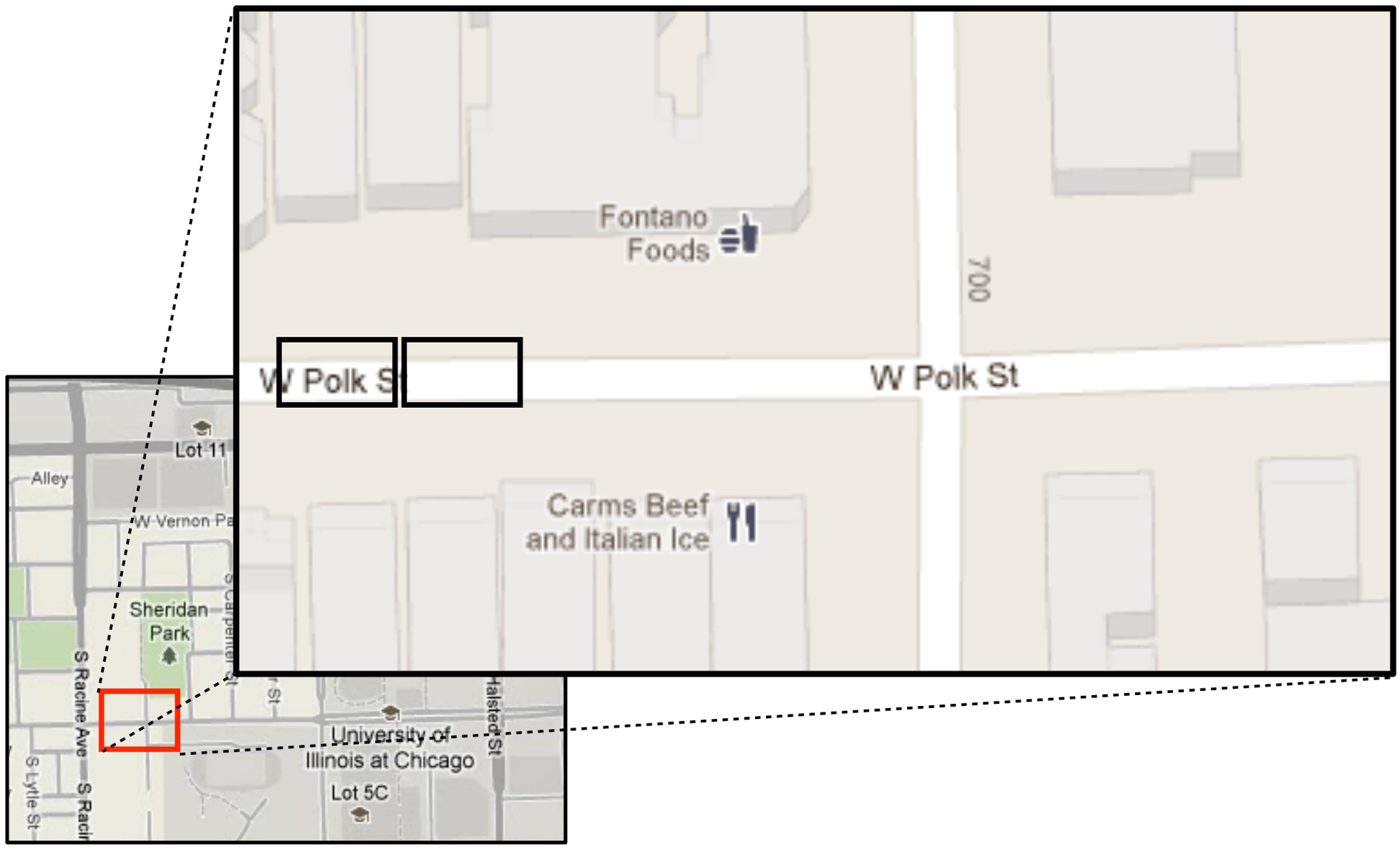
States & transition probabilities



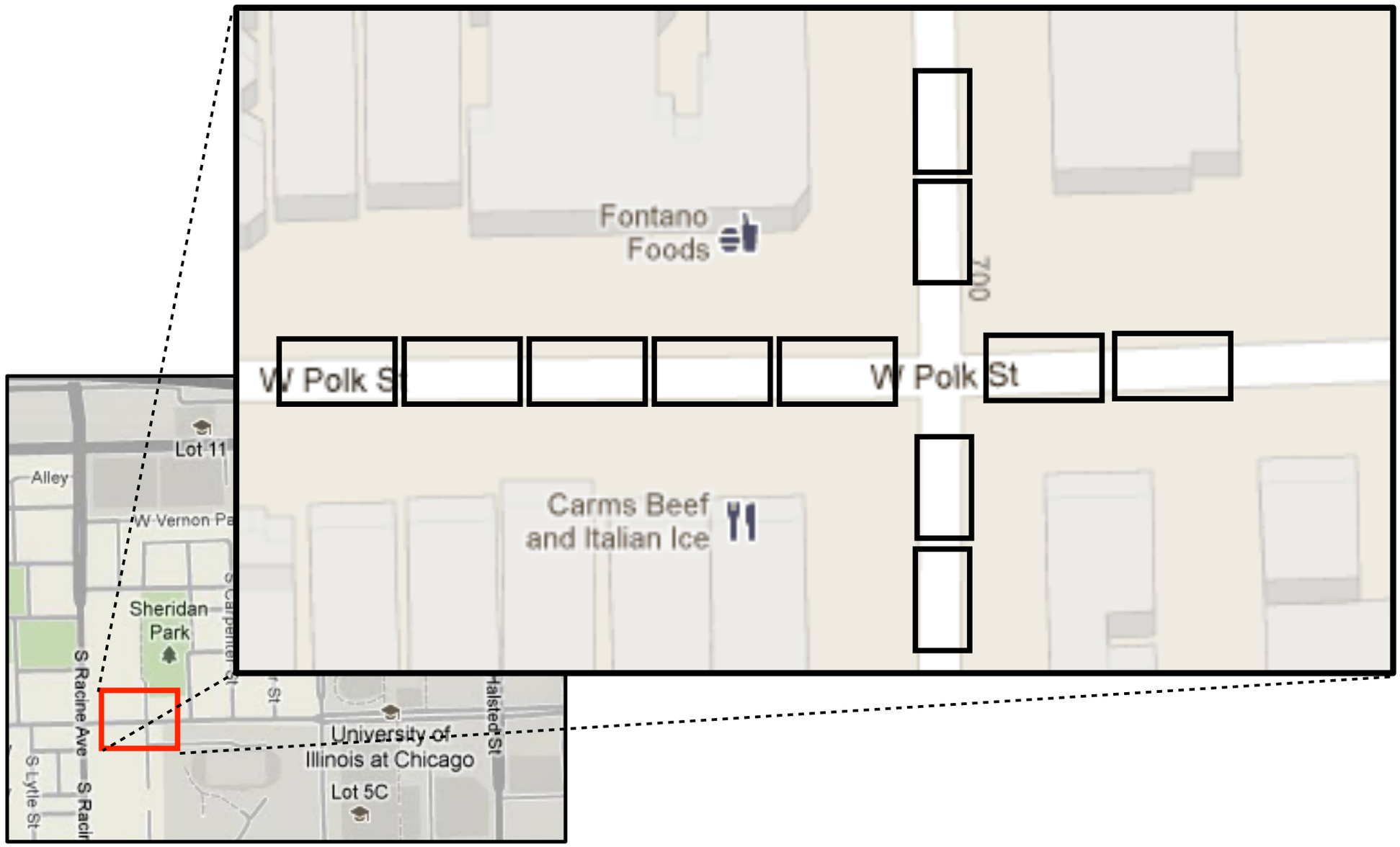
States & transition probabilities



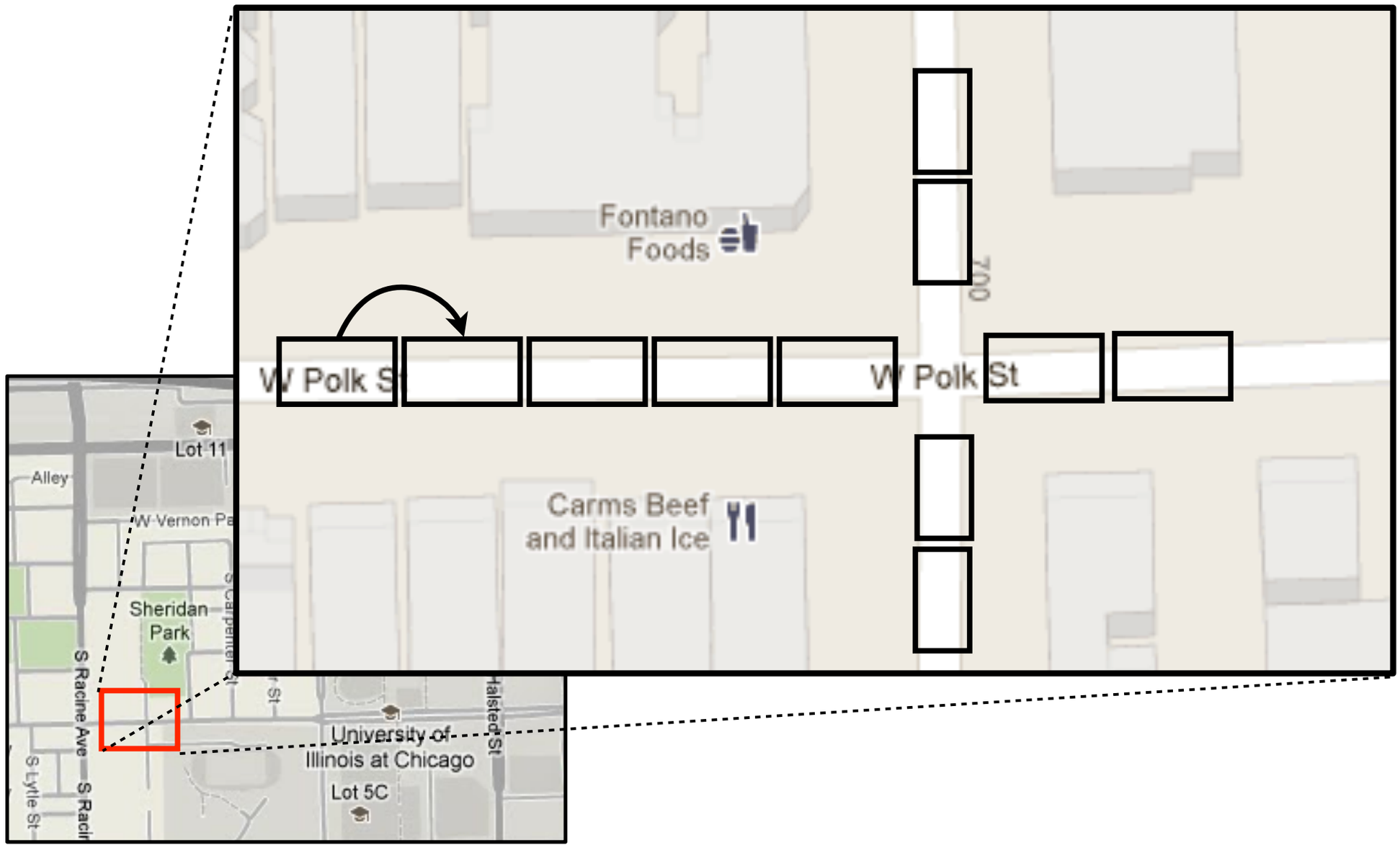
States & transition probabilities



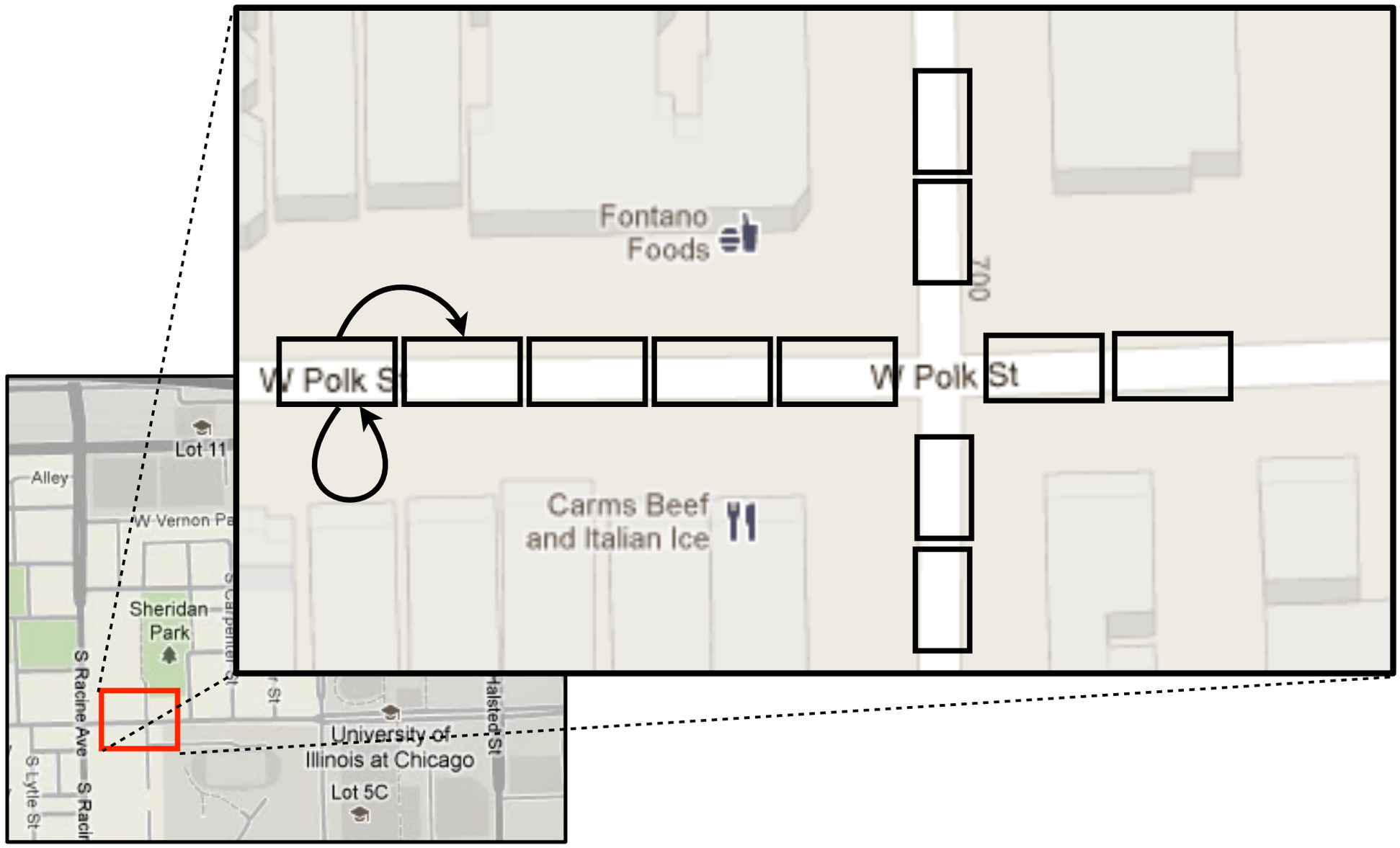
States & transition probabilities



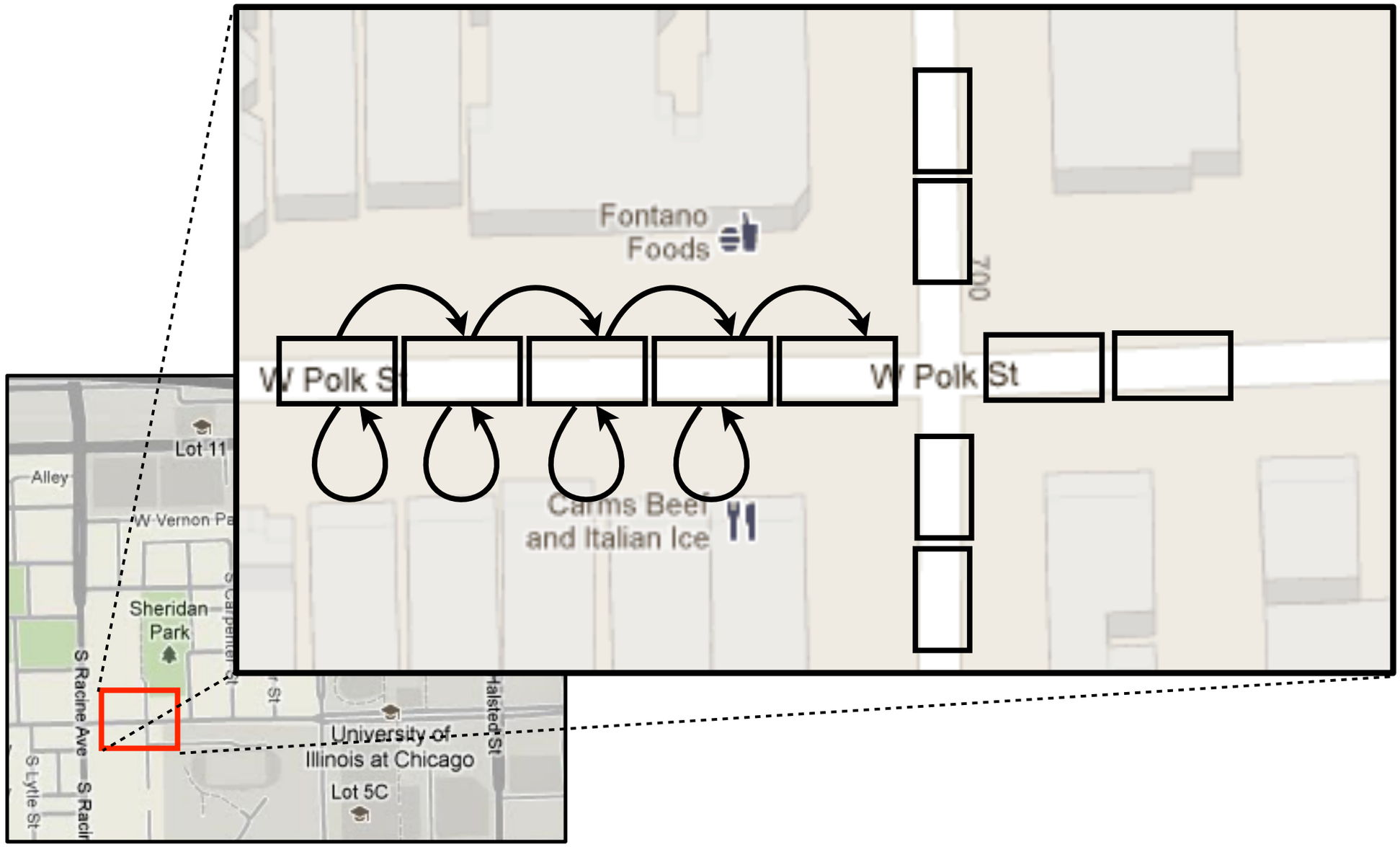
States & transition probabilities



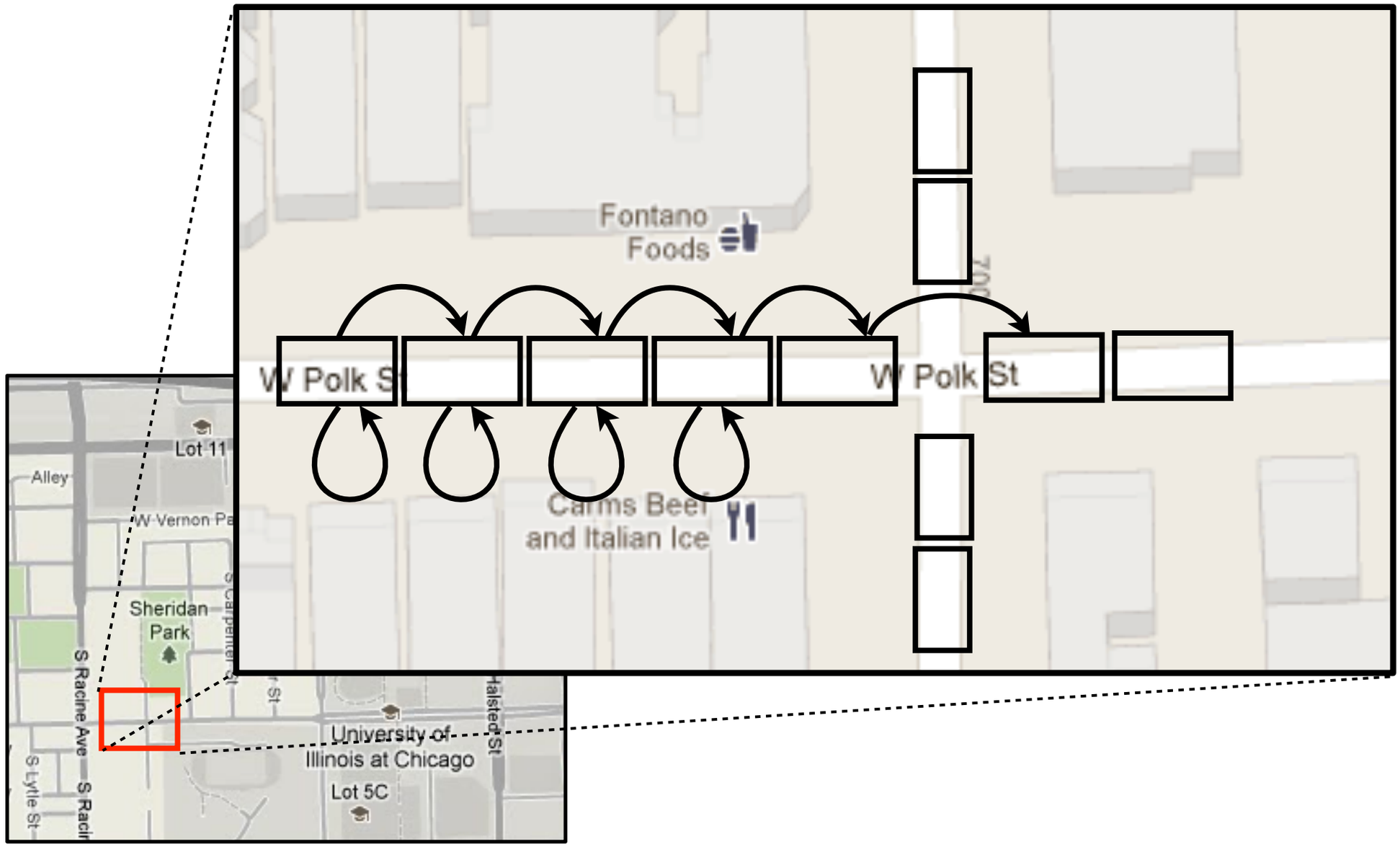
States & transition probabilities



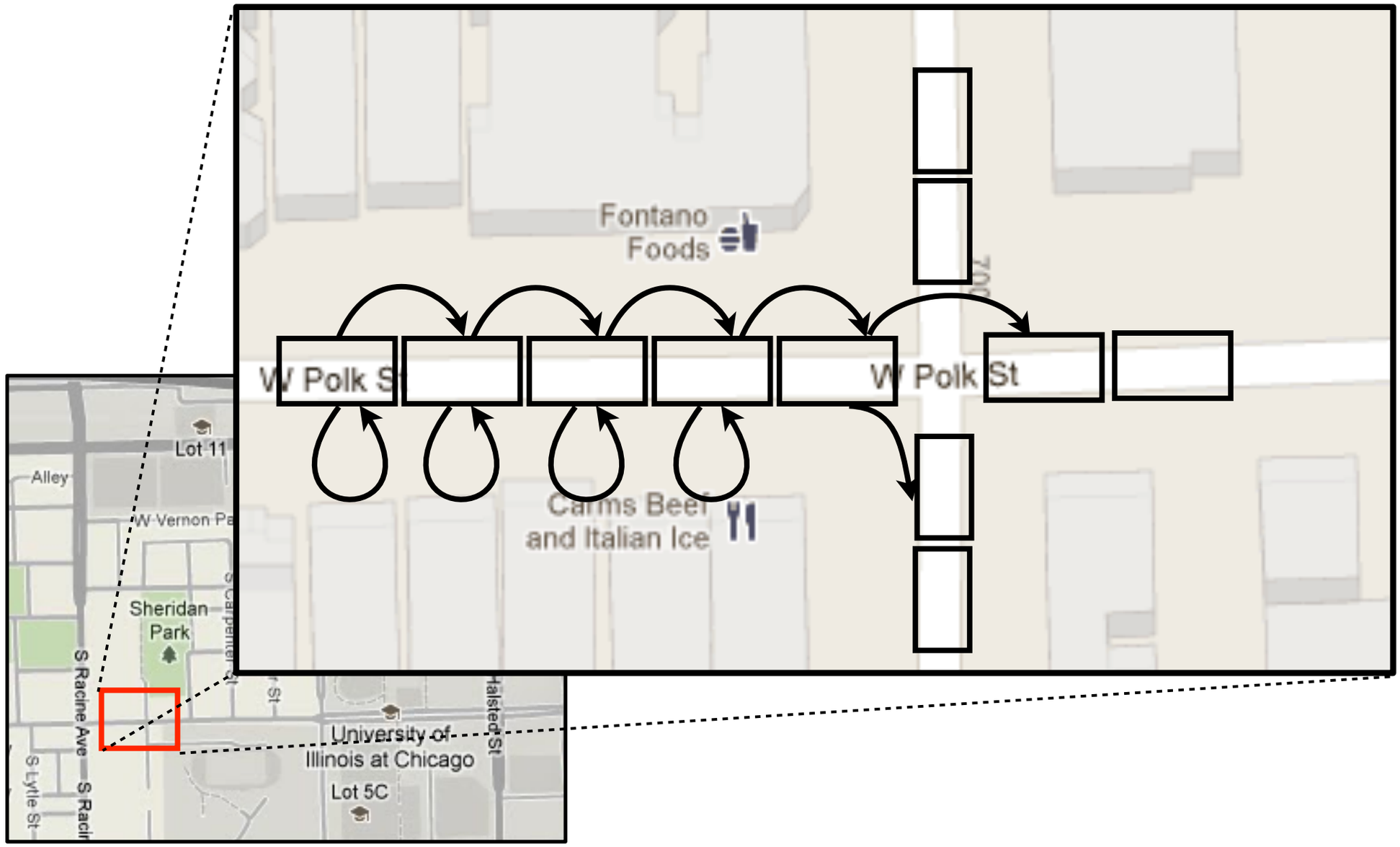
States & transition probabilities



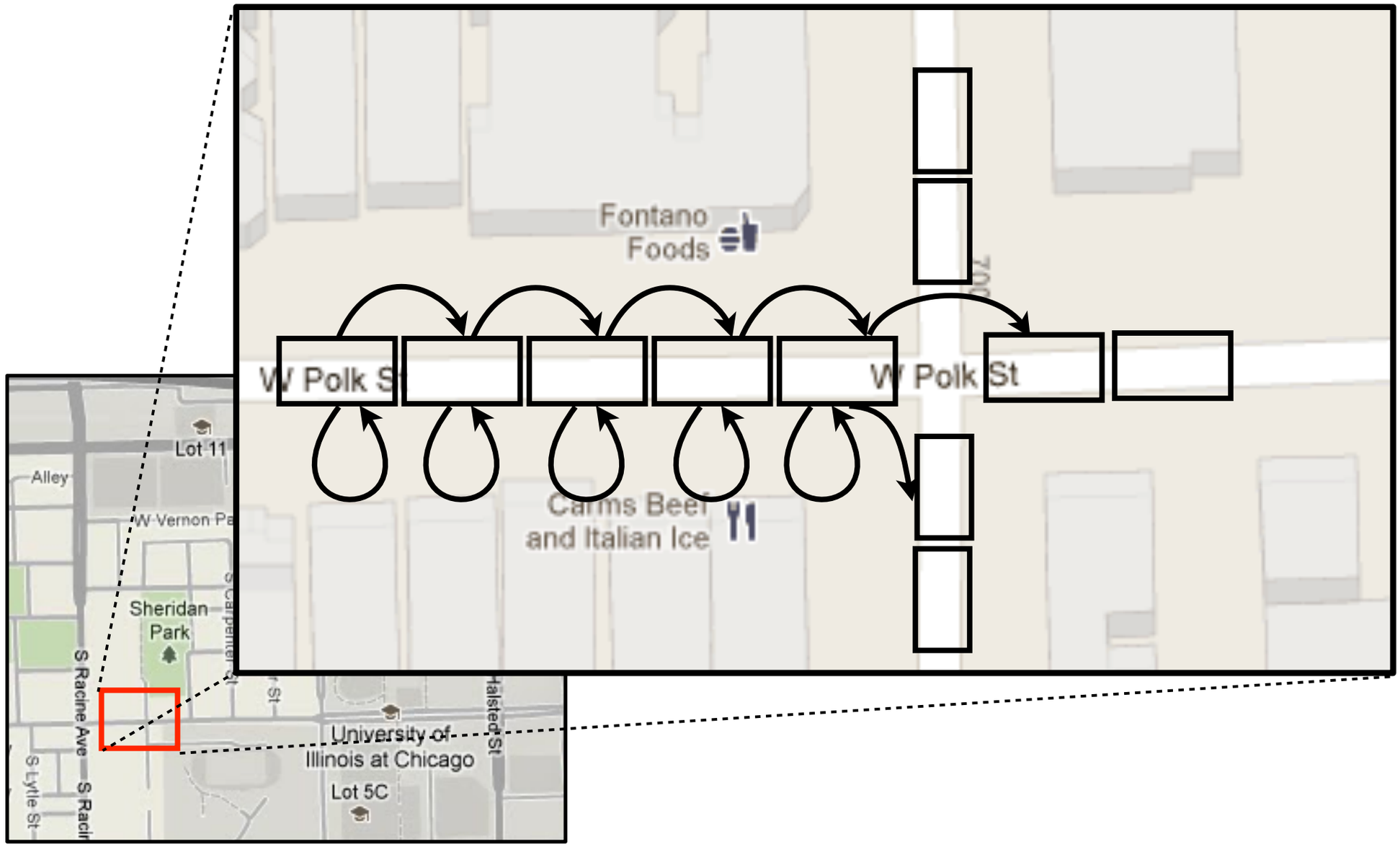
States & transition probabilities



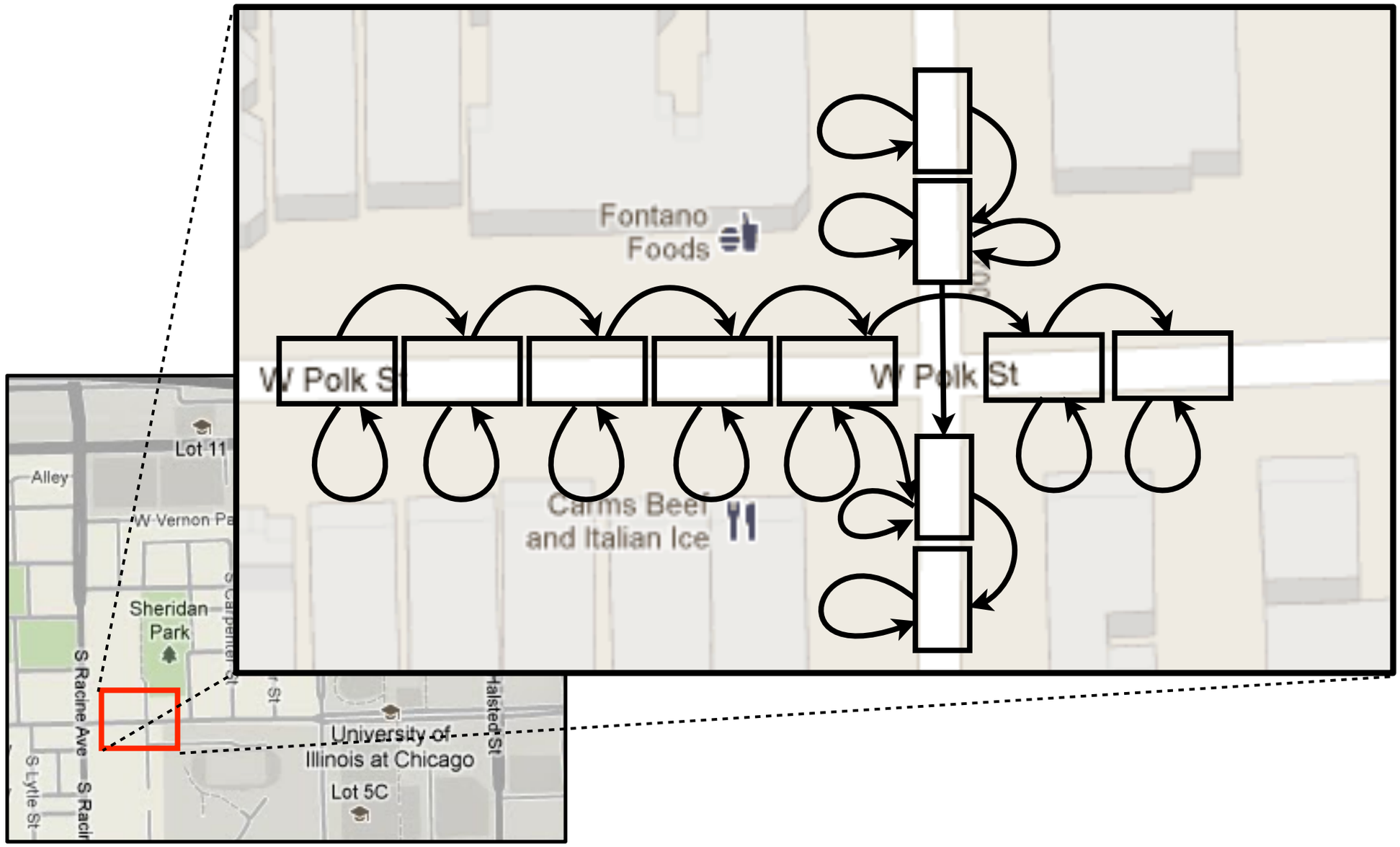
States & transition probabilities



States & transition probabilities



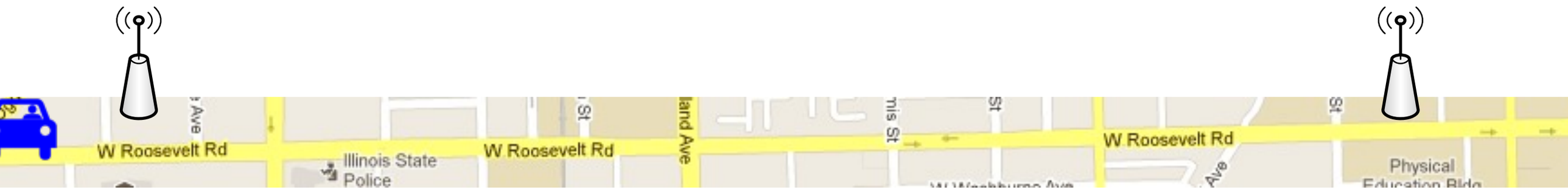
States & transition probabilities



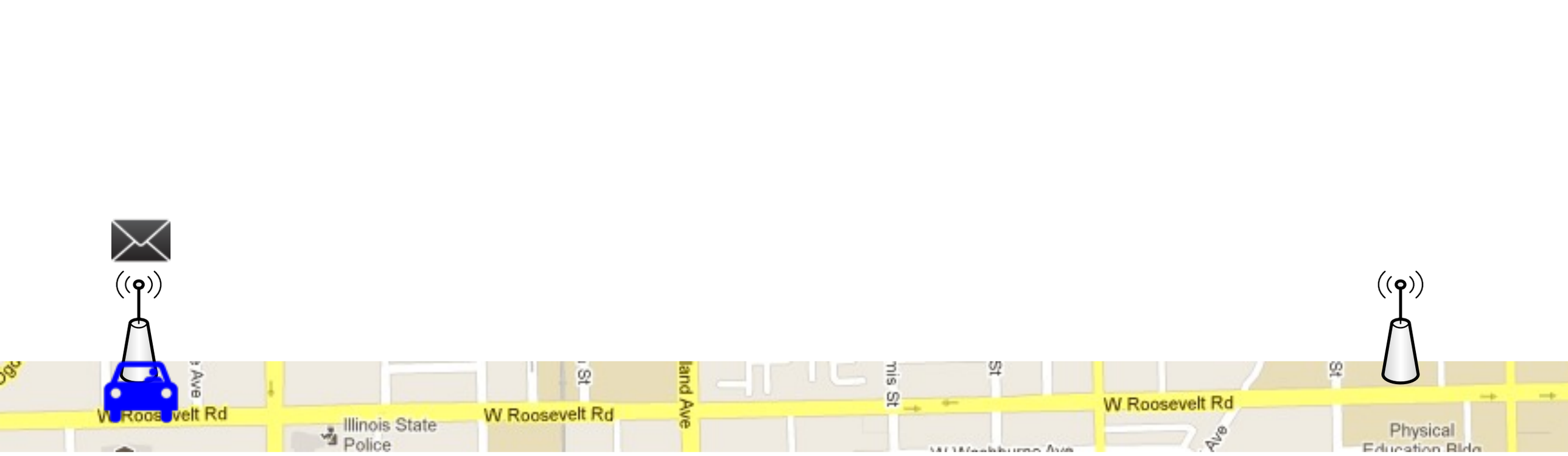
Emission Probability

- Probability of observation given a state (location)
- Observation: reception/non-reception of a packet at one or more monitors

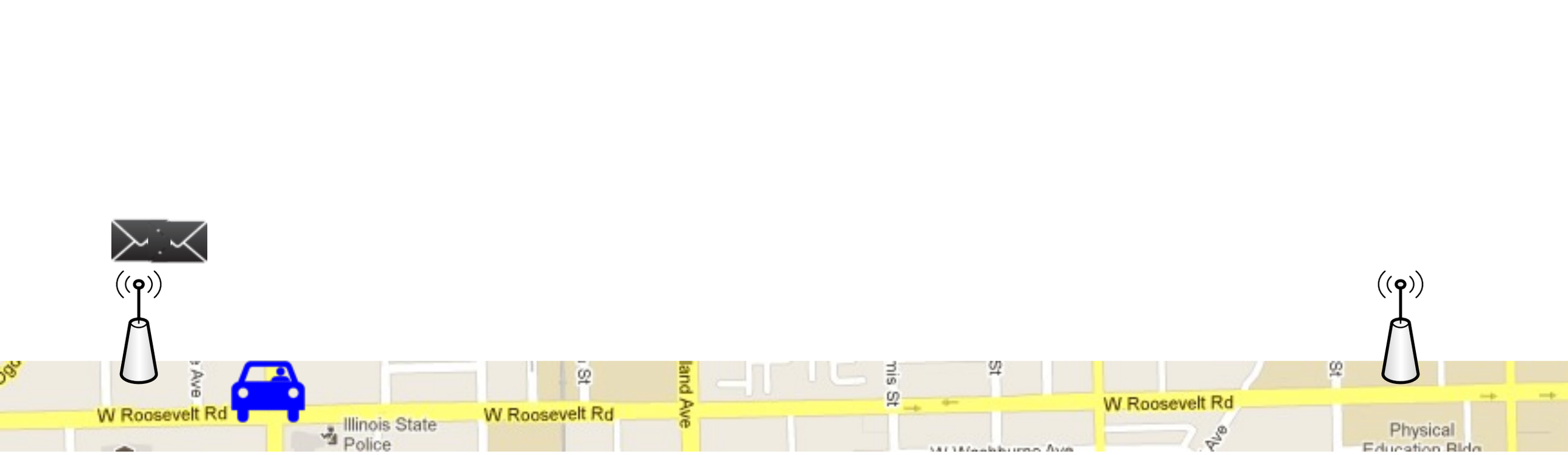
A simple model



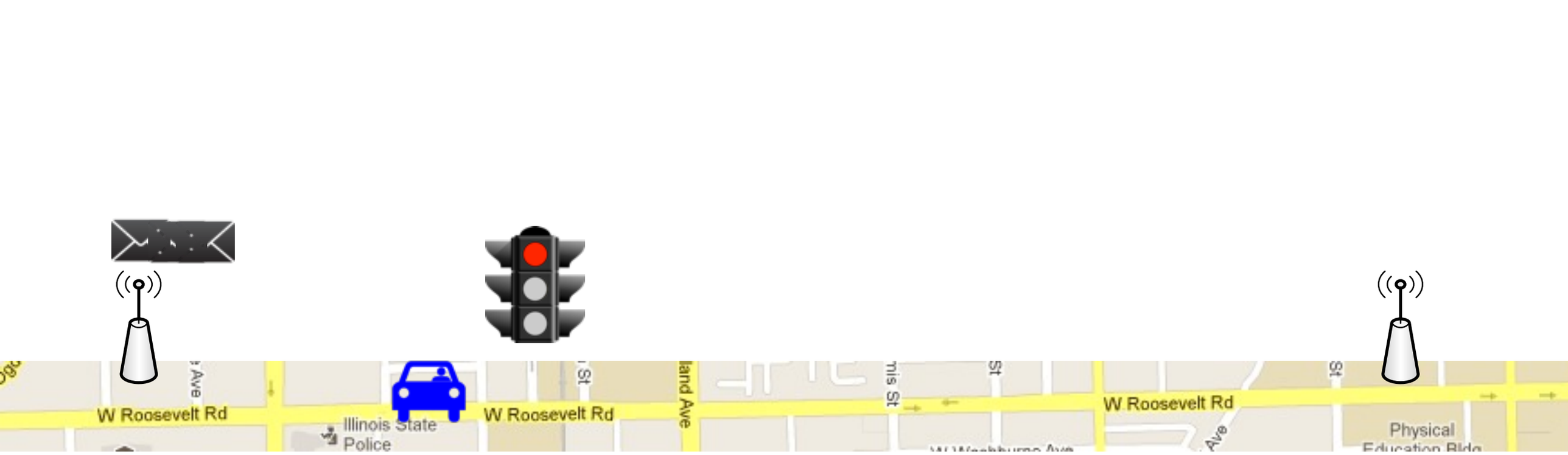
A simple model



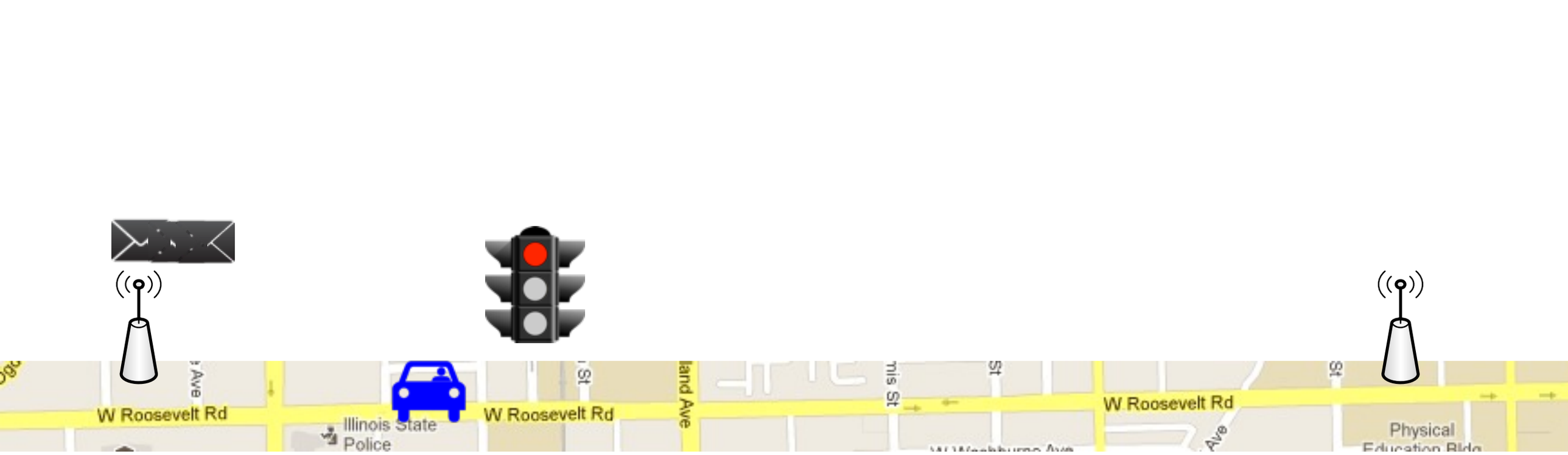
A simple model



A simple model



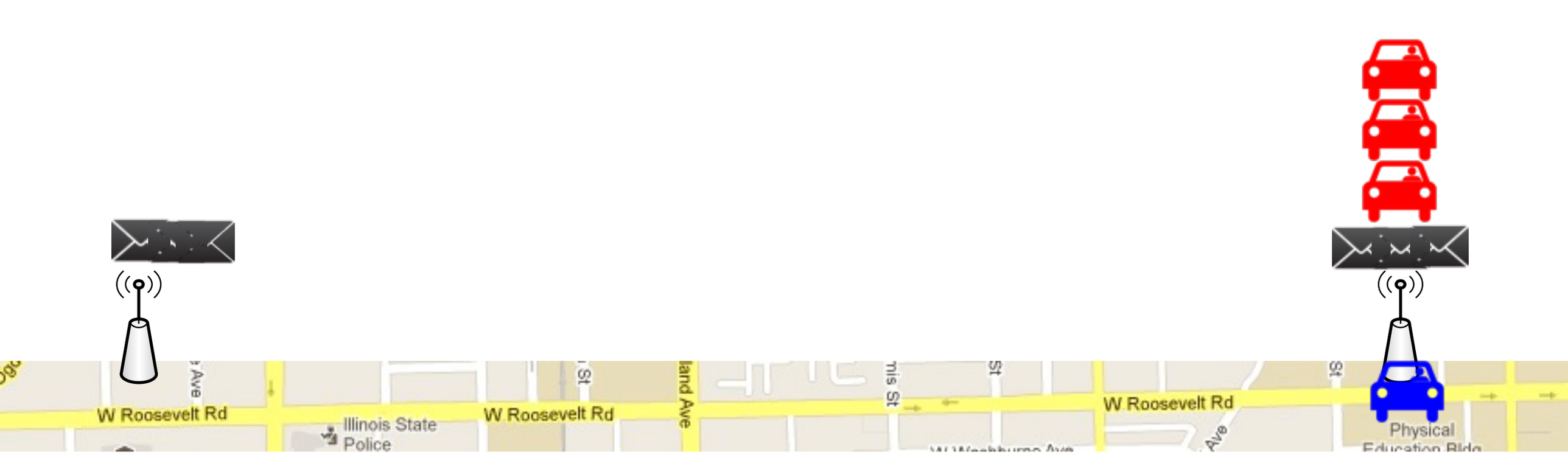
A simple model



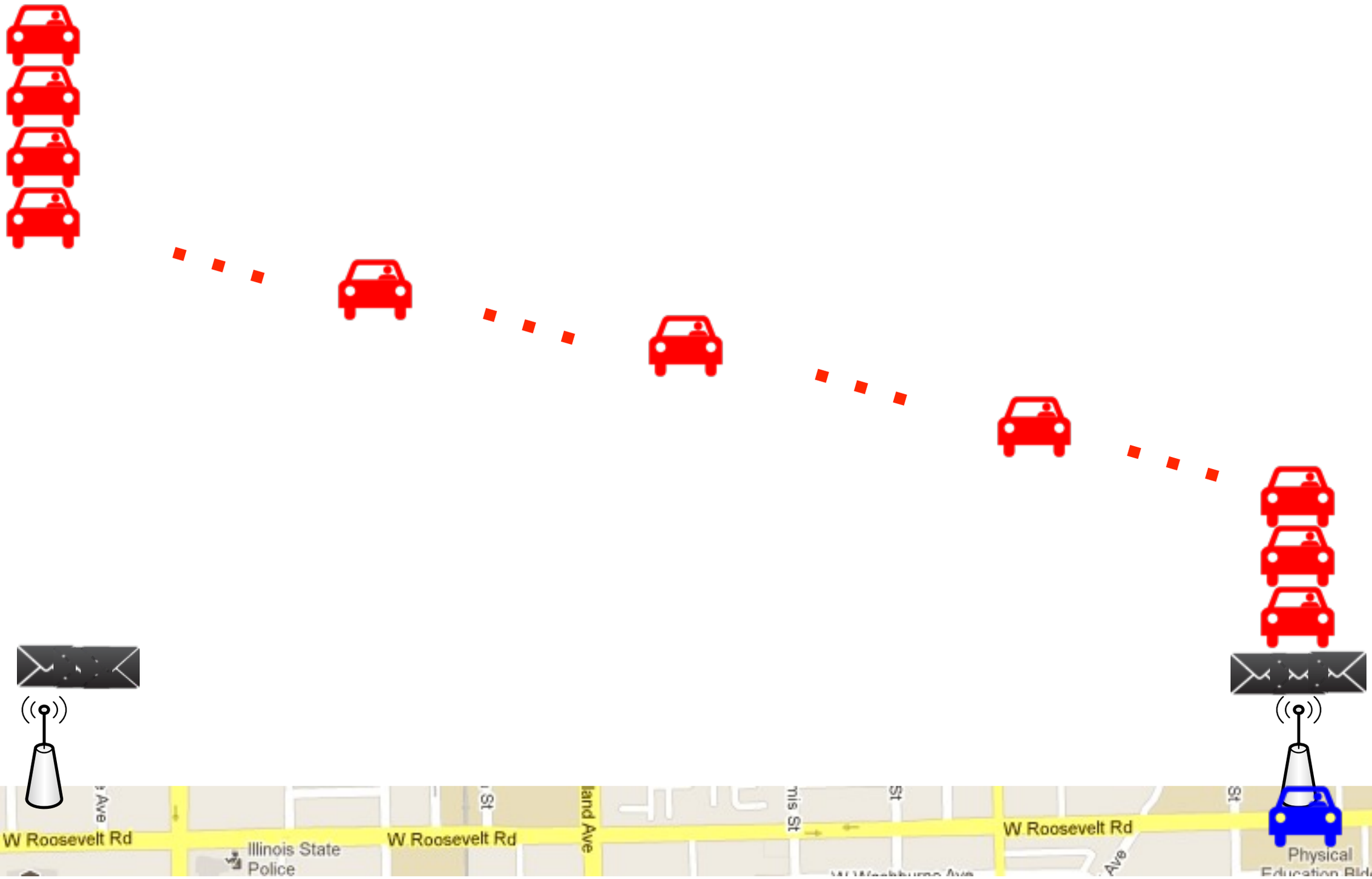
A simple model

A simple model

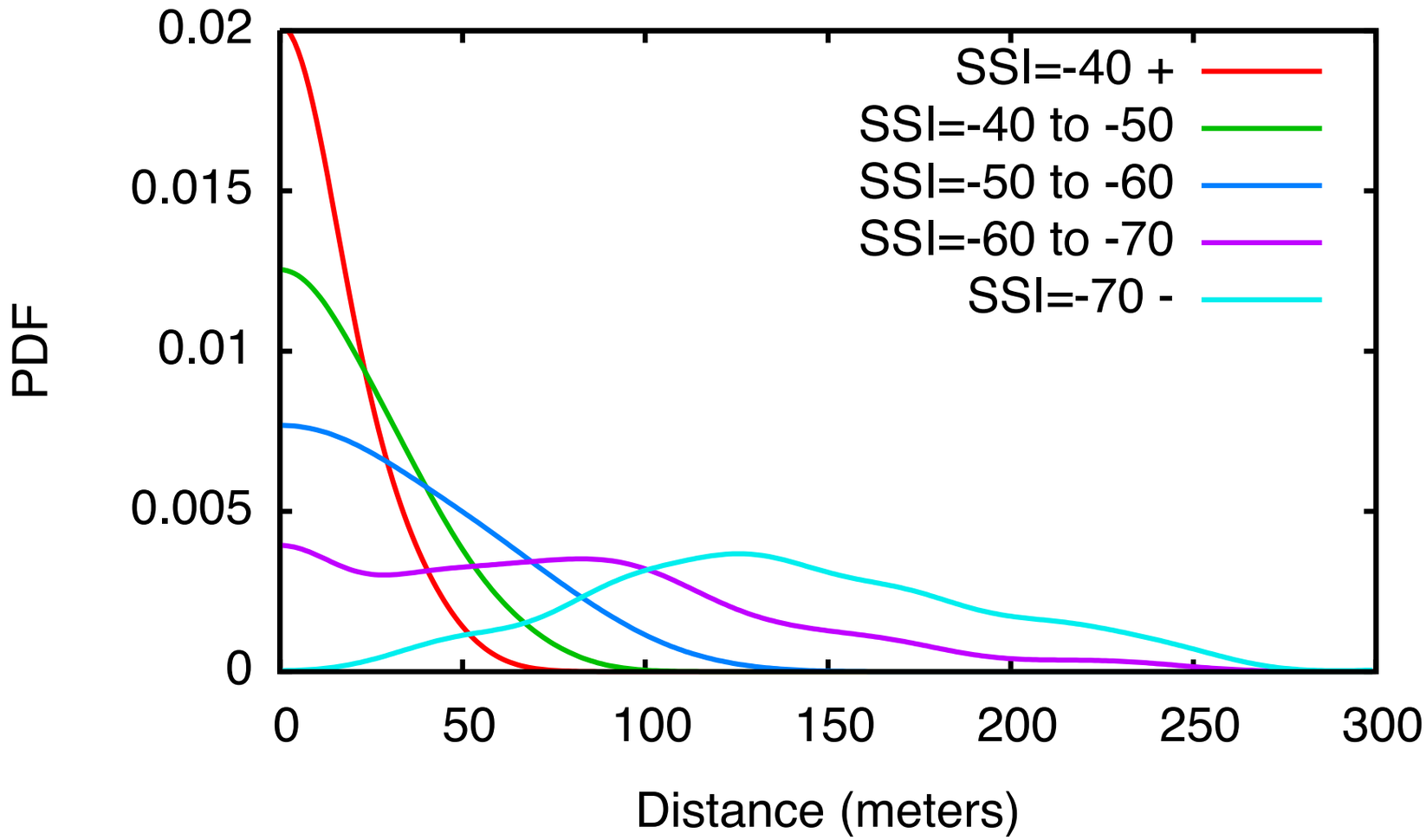
A simple model



A simple model

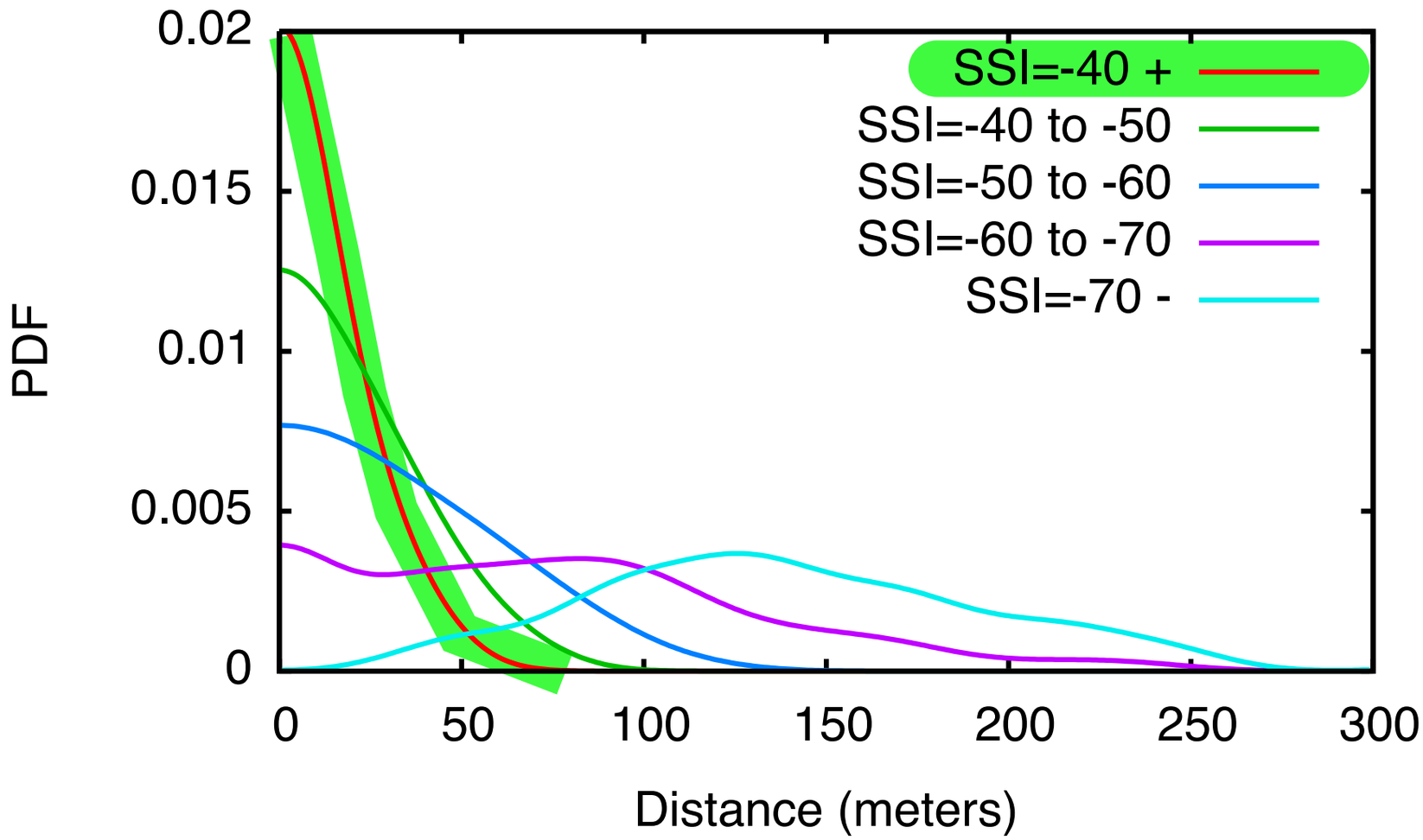


Experimental RSS characteristics



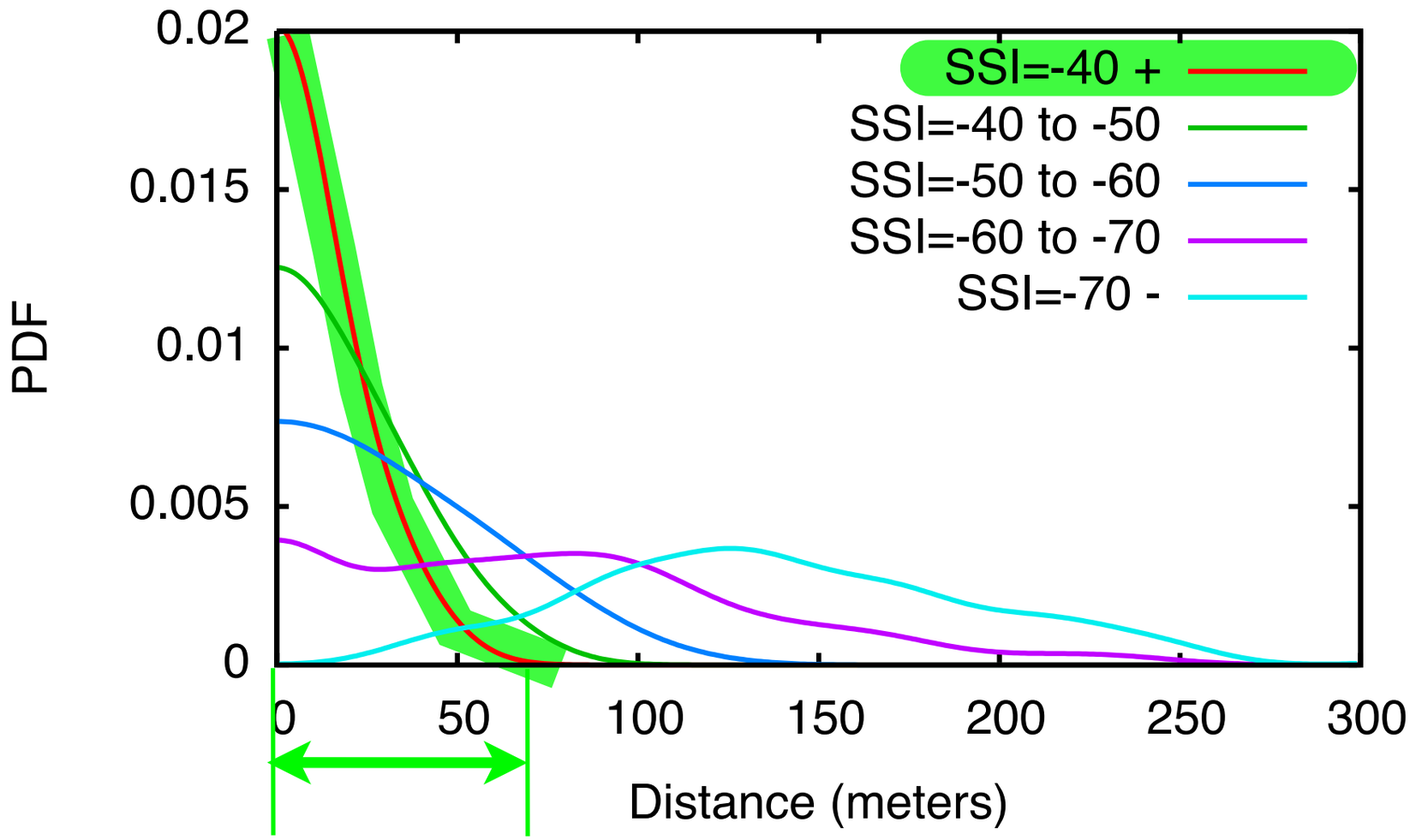
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

Experimental RSS characteristics



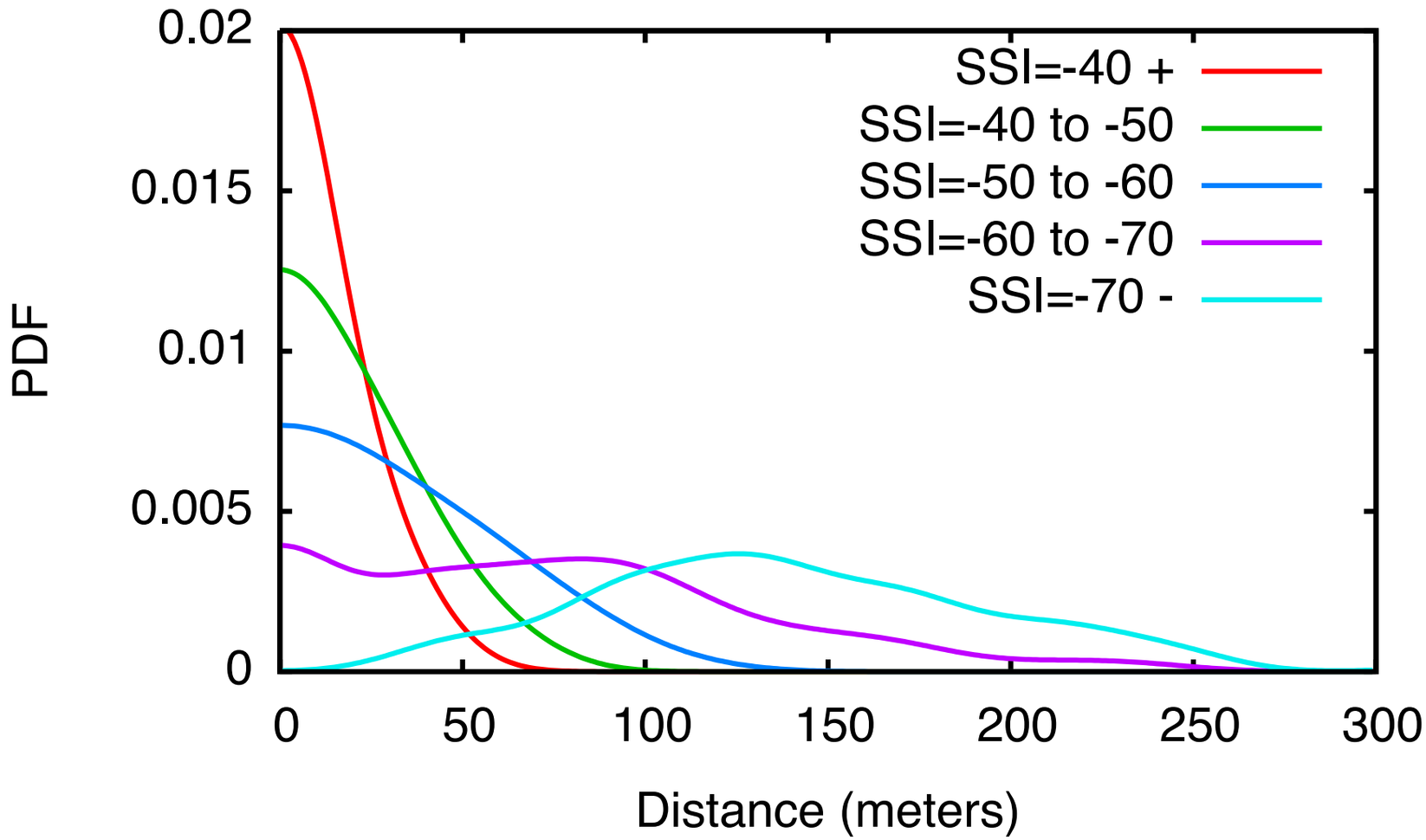
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

Experimental RSS characteristics



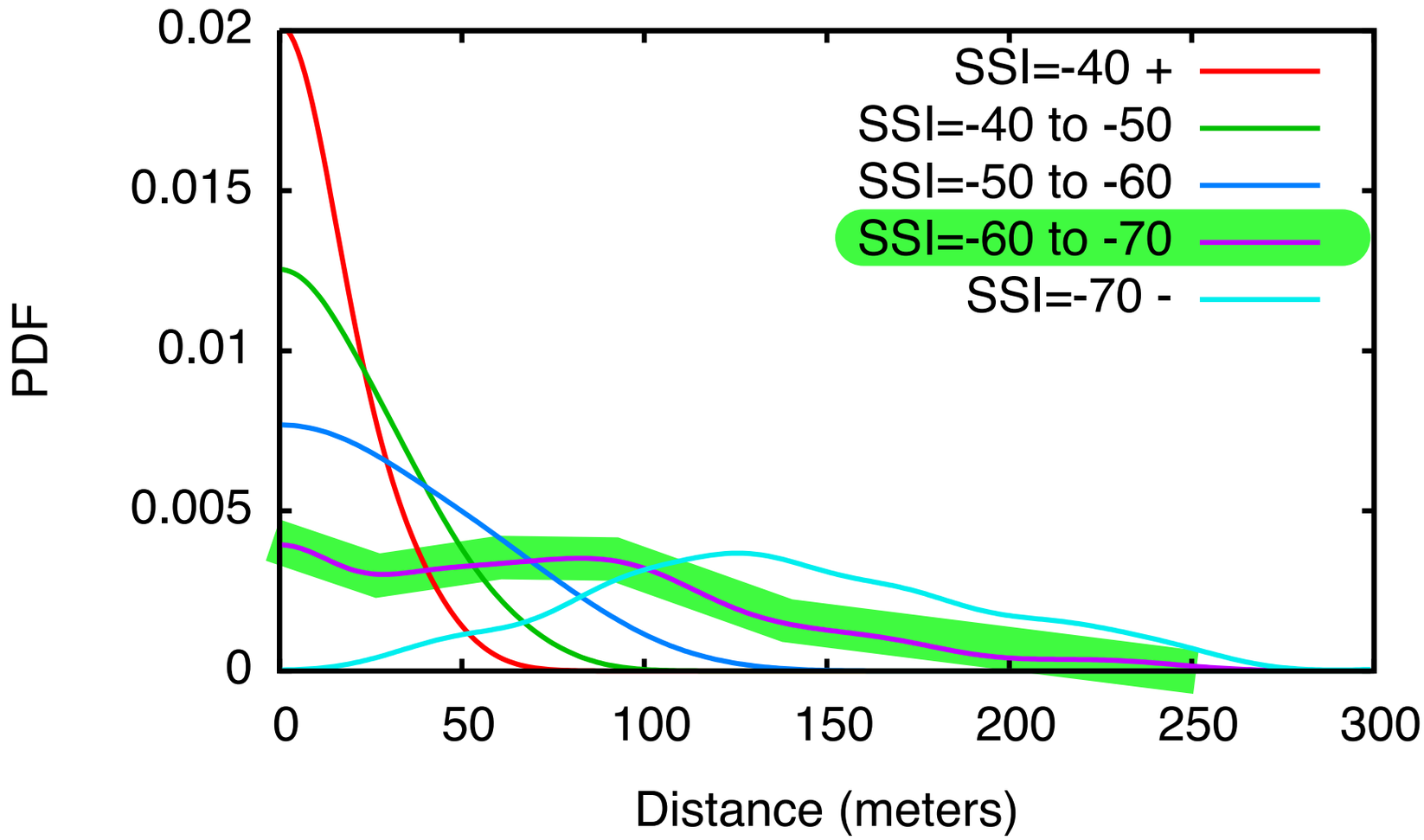
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

Experimental RSS characteristics



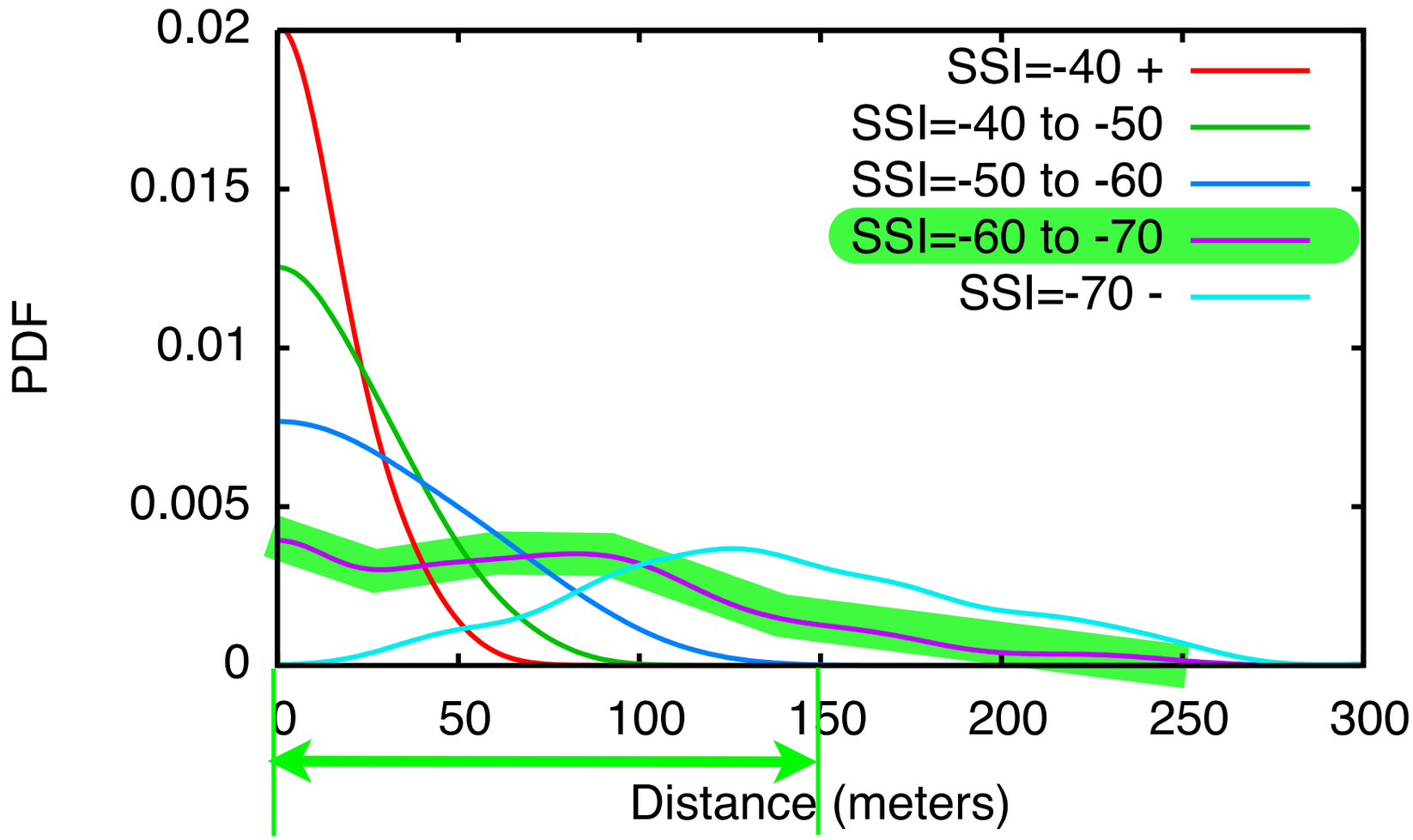
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

Experimental RSS characteristics



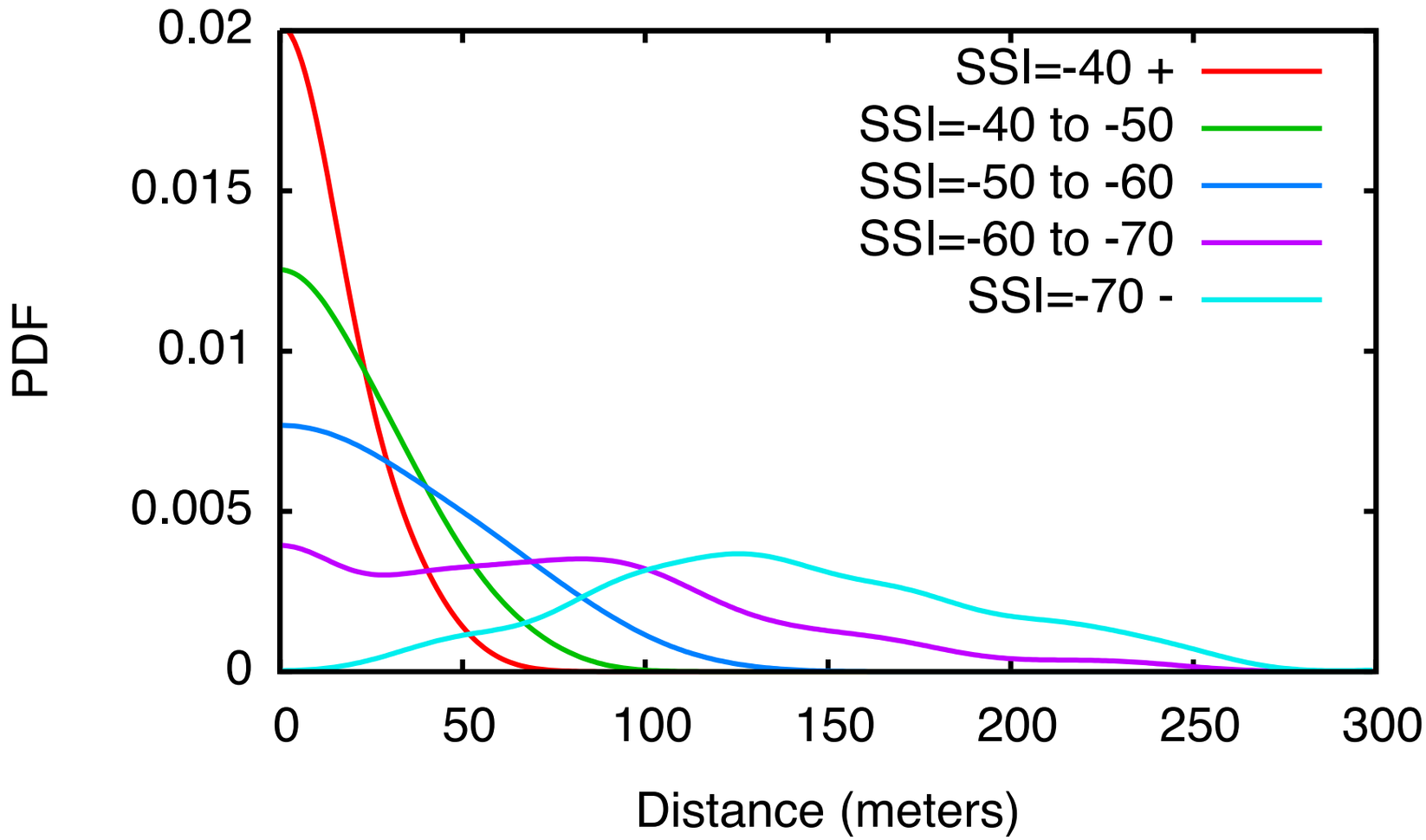
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

Experimental RSS characteristics



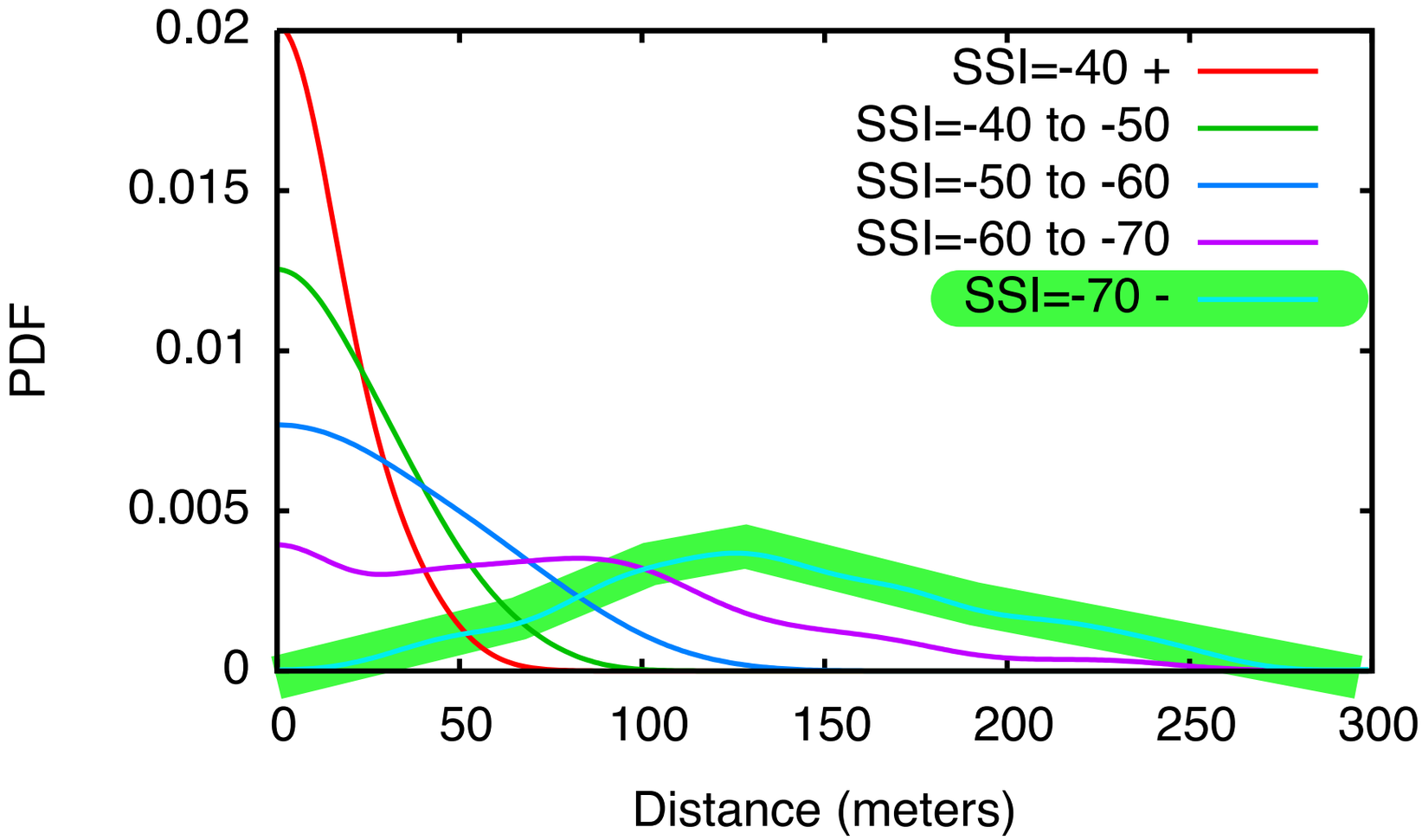
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

Experimental RSS characteristics



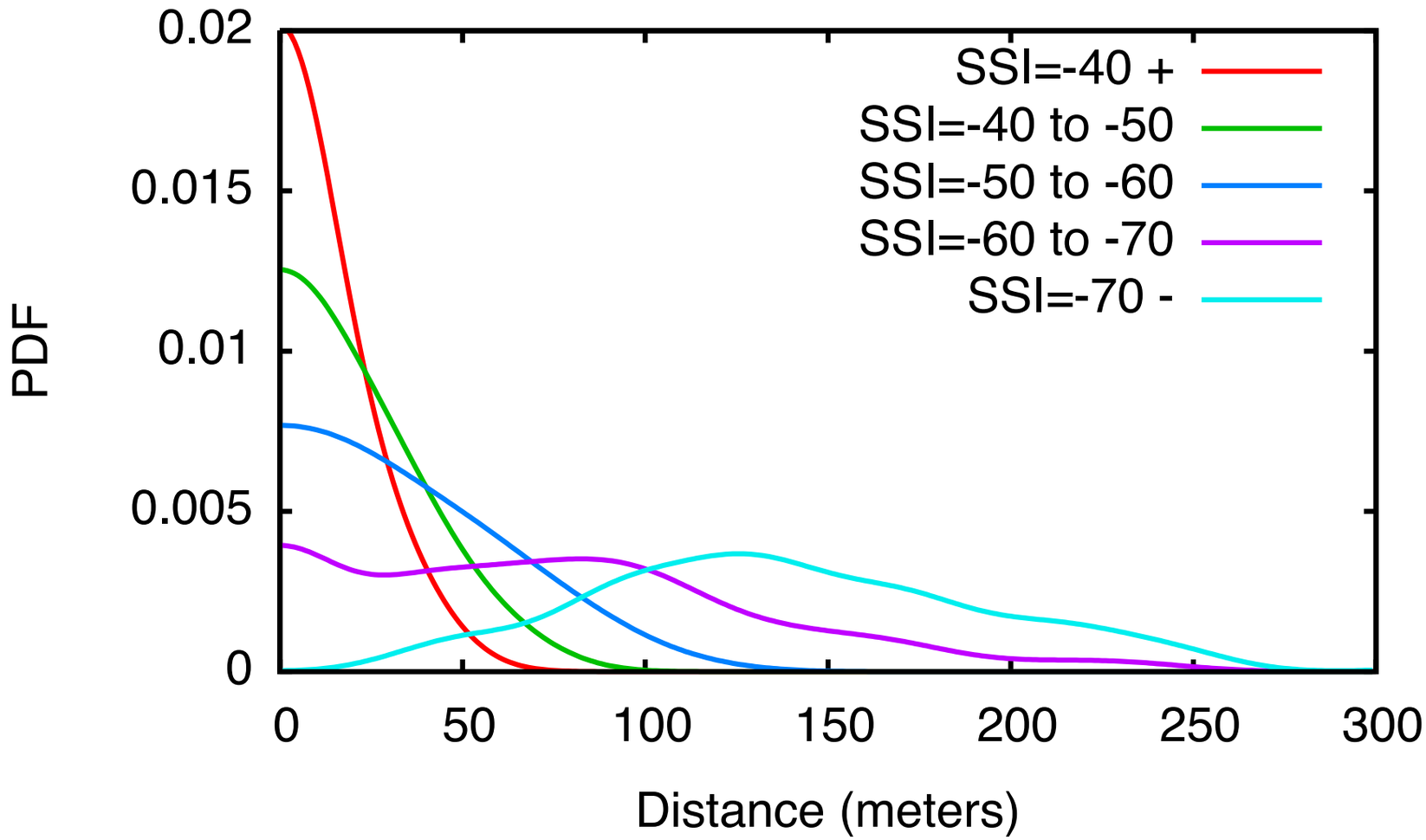
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

Experimental RSS characteristics



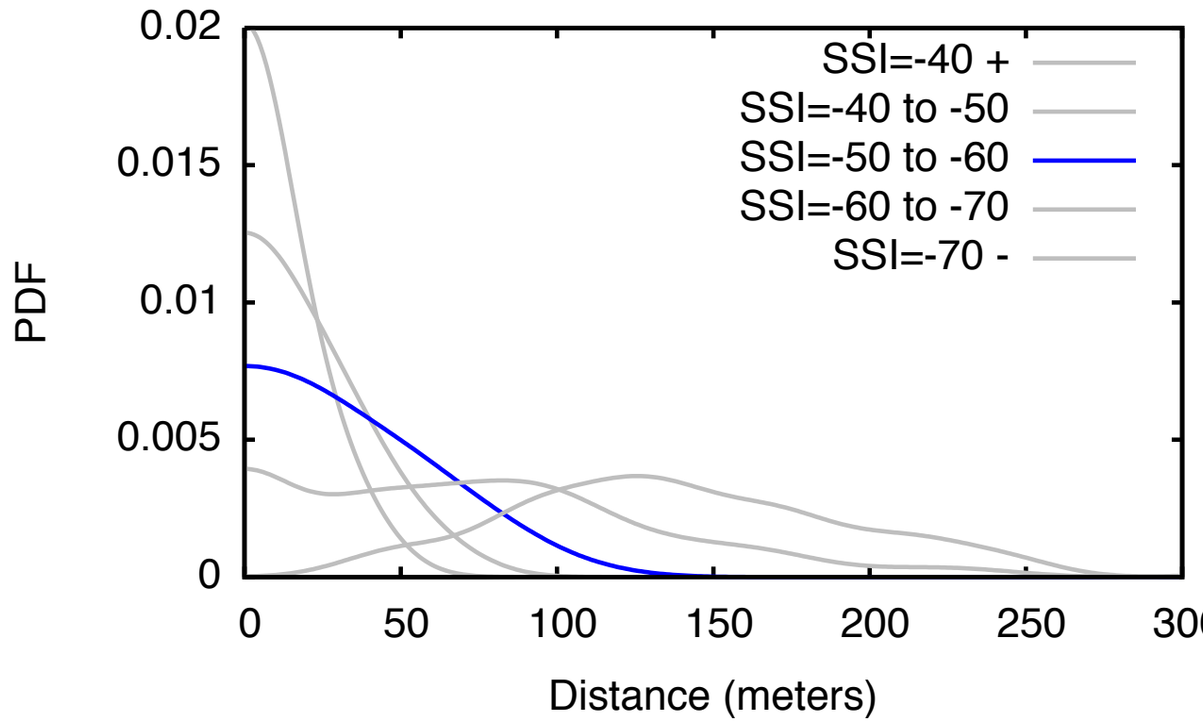
$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

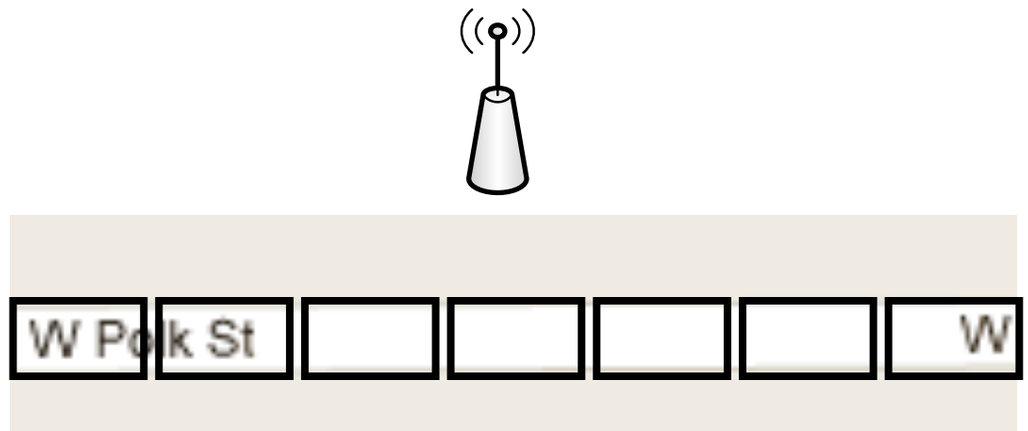
Experimental RSS characteristics



$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

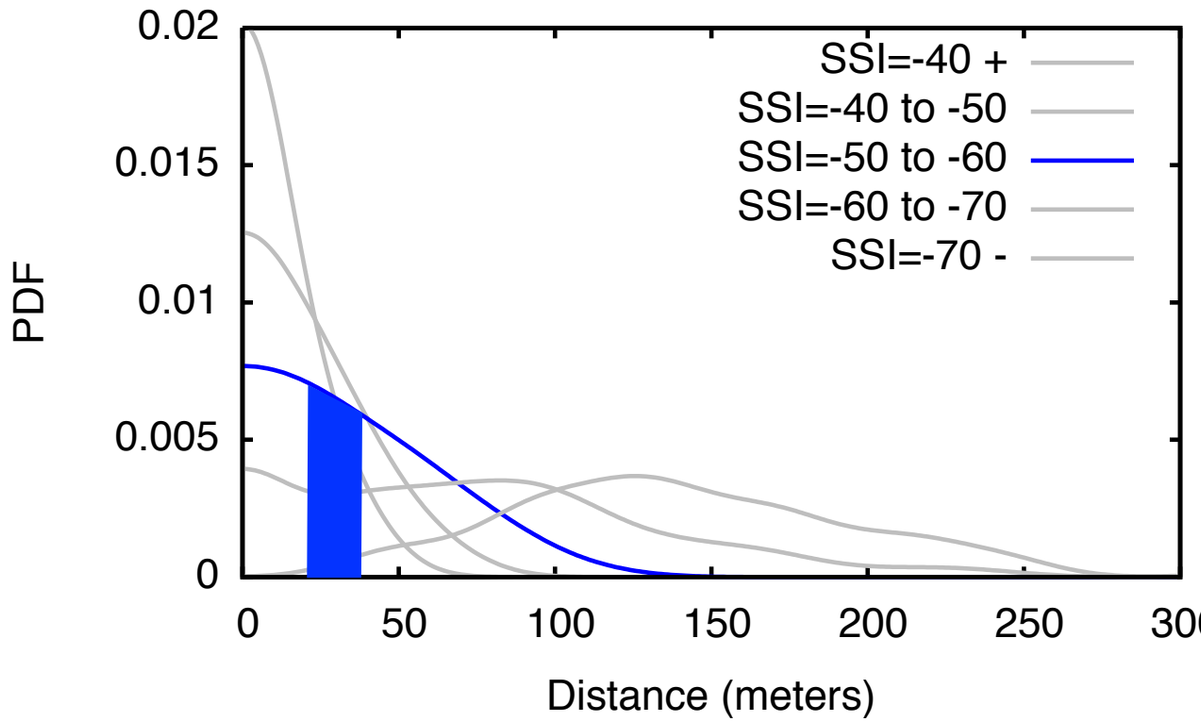
Experimental RSS characteristics

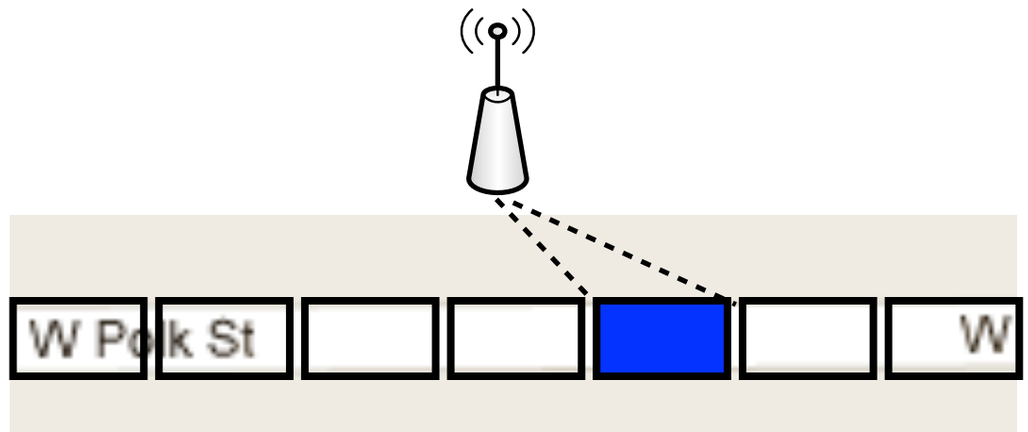




$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

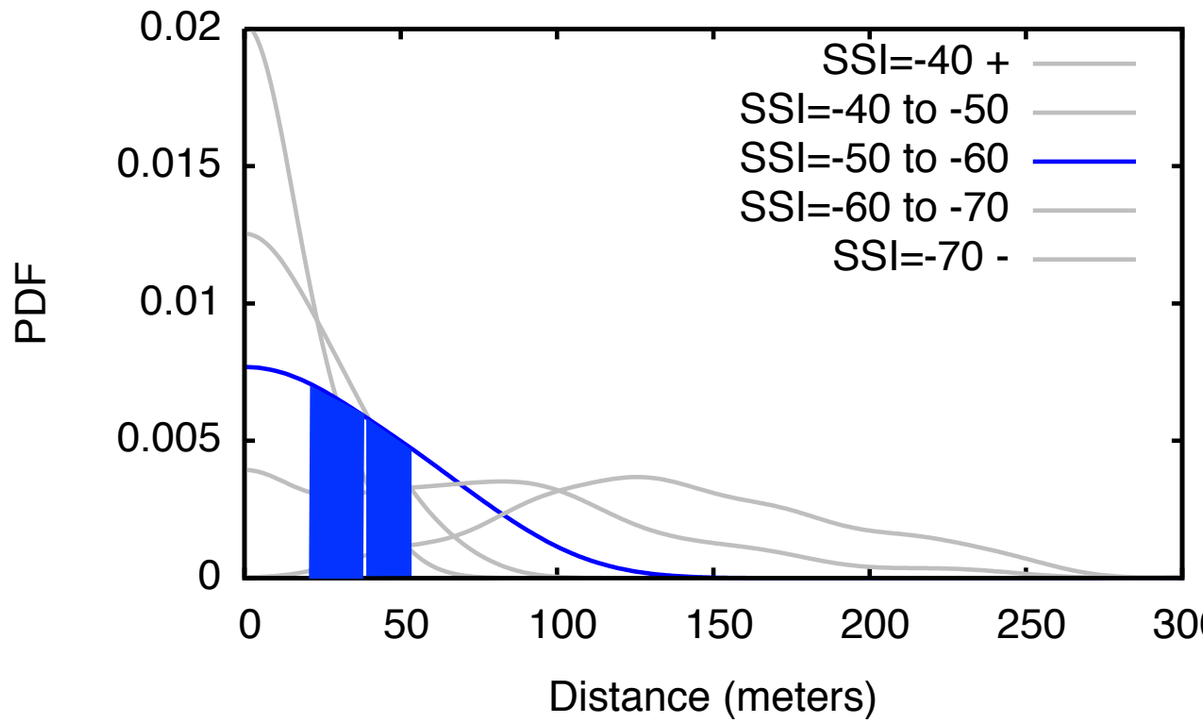
Experimental RSS characteristics

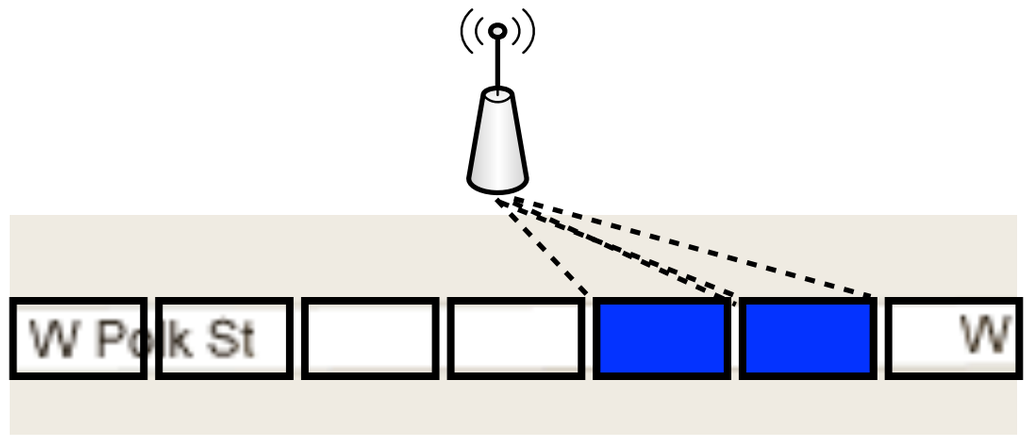




$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

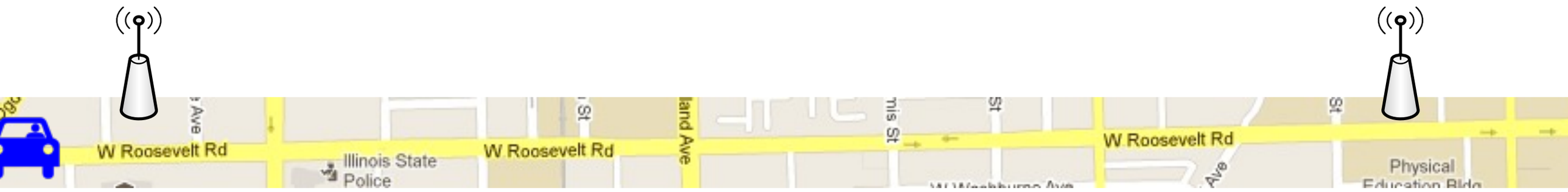
Experimental RSS characteristics



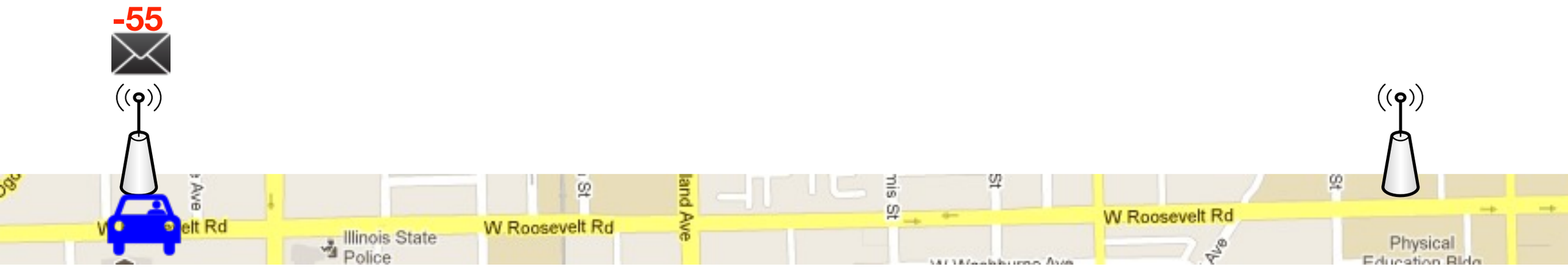


$$p(detection_m|s,tx) = \int_x \int_y p(dist(x,y,m)|RSS)dxdy$$

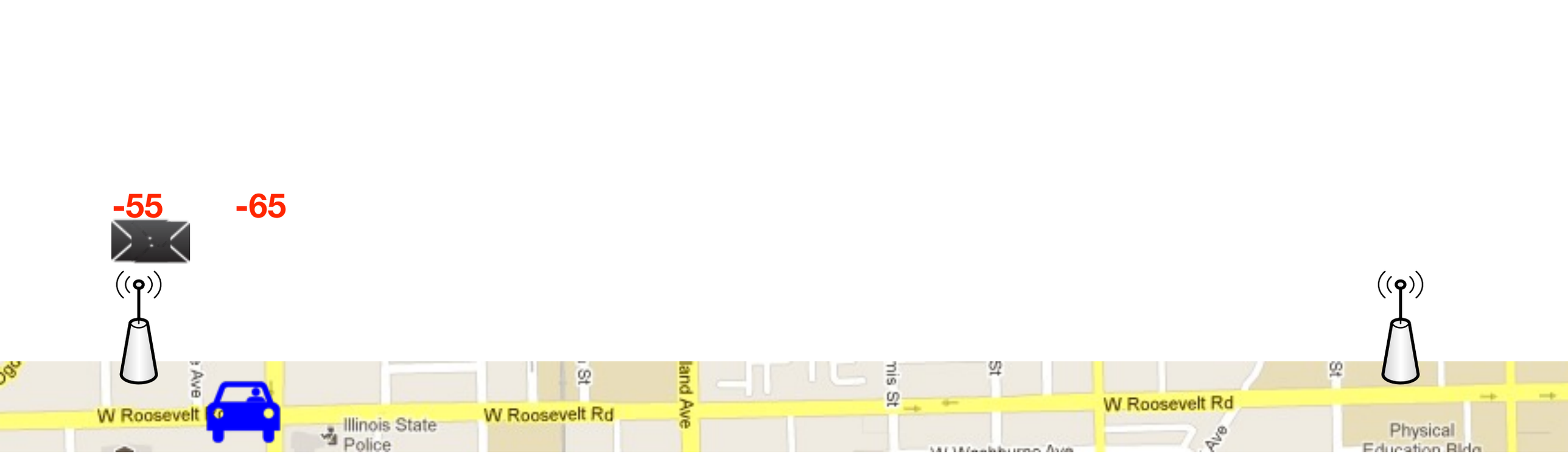
Augmenting detections with RSS



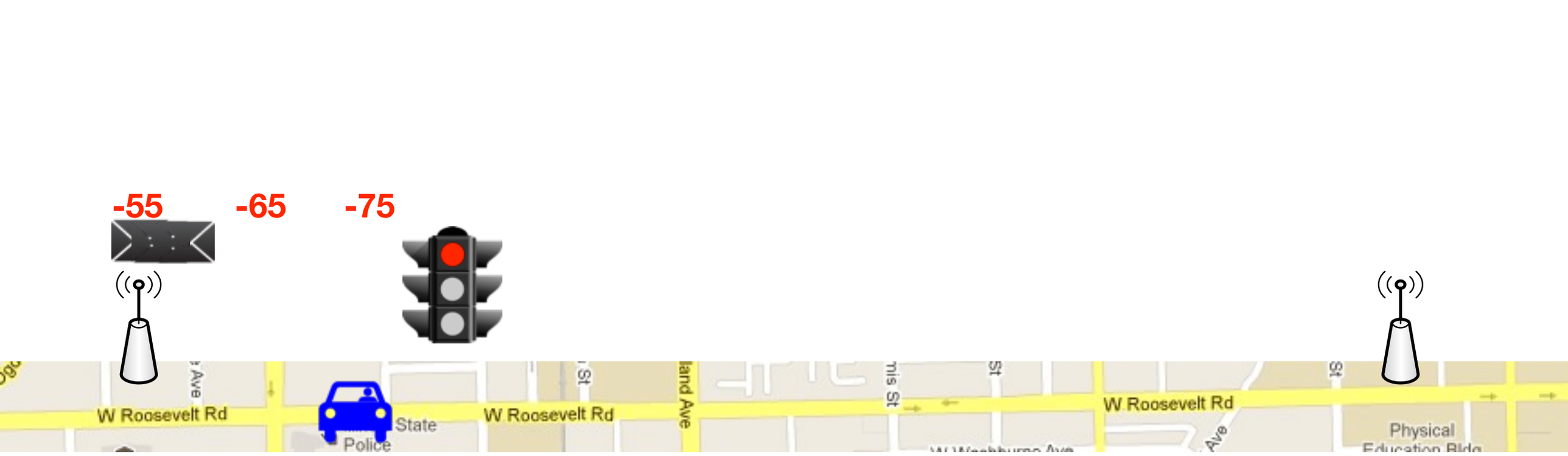
Augmenting detections with RSS



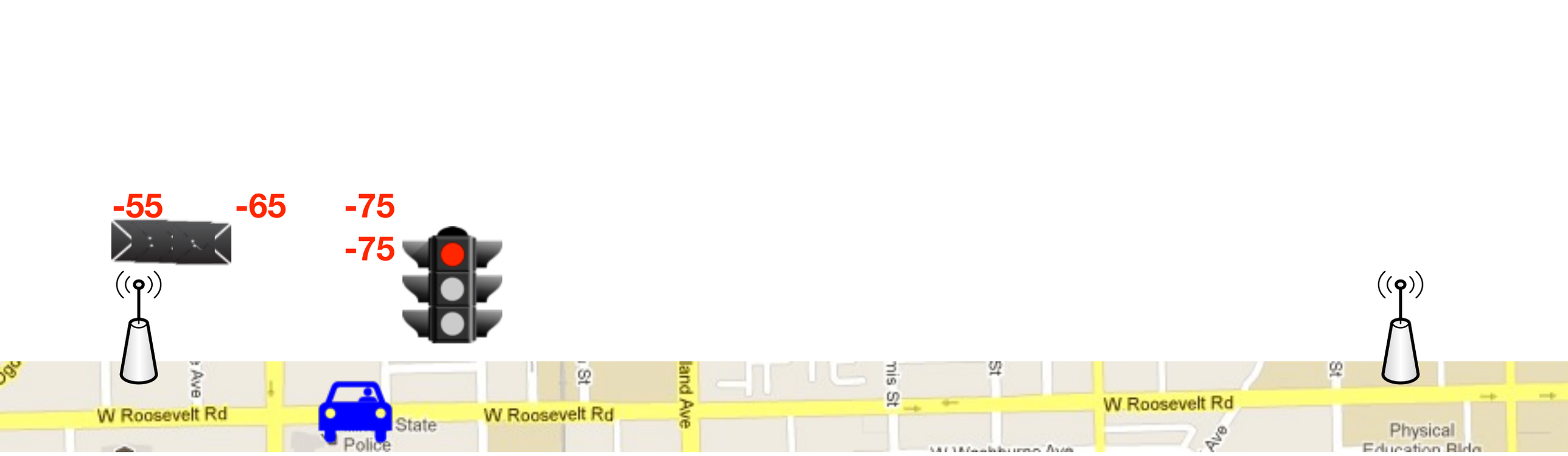
Augmenting detections with RSS



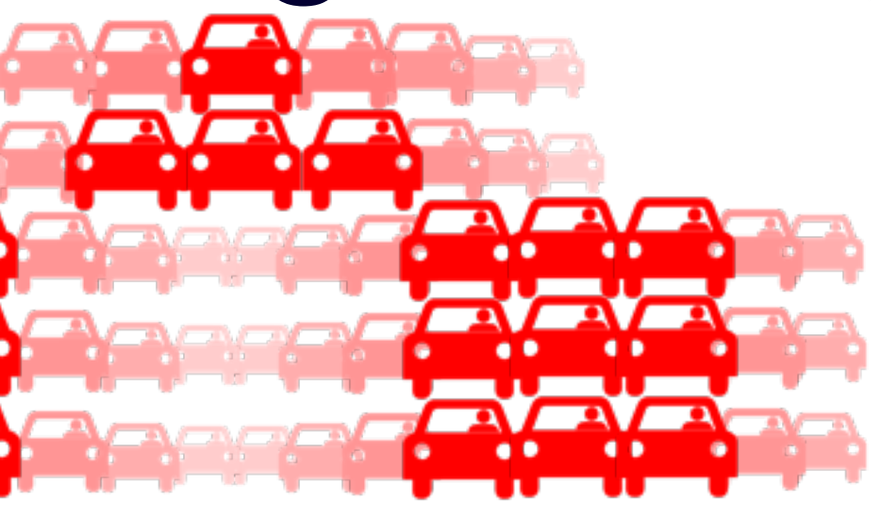
Augmenting detections with RSS

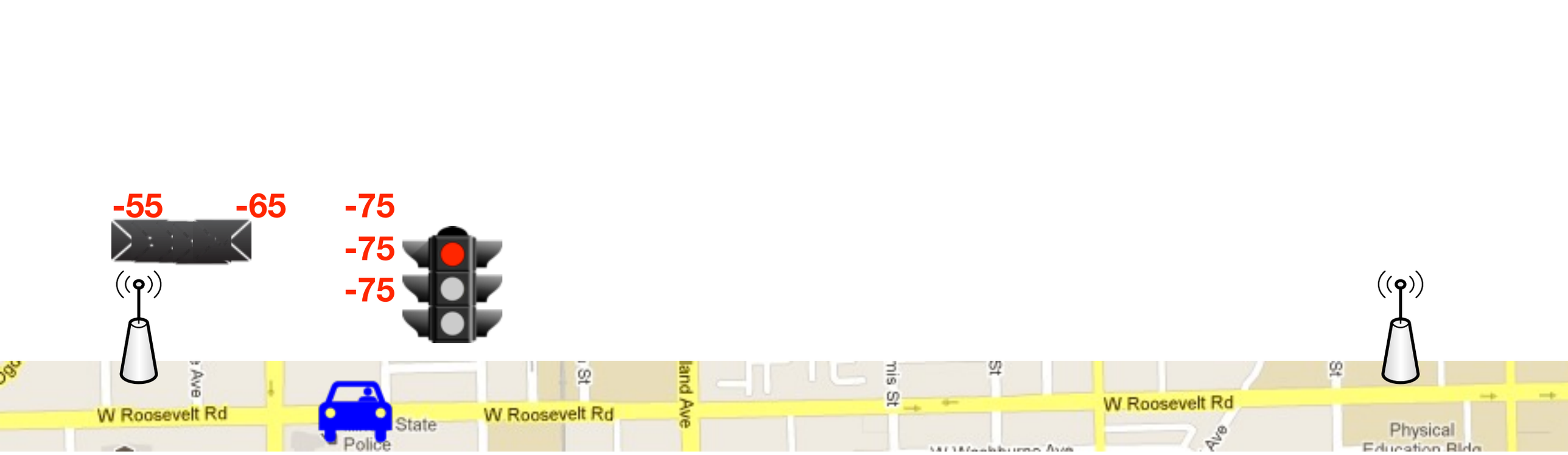


Augmenting detections with RSS

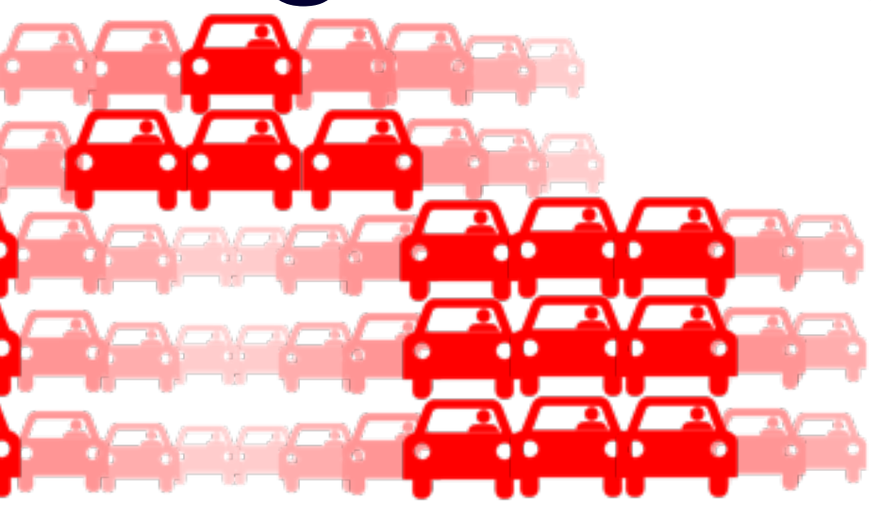


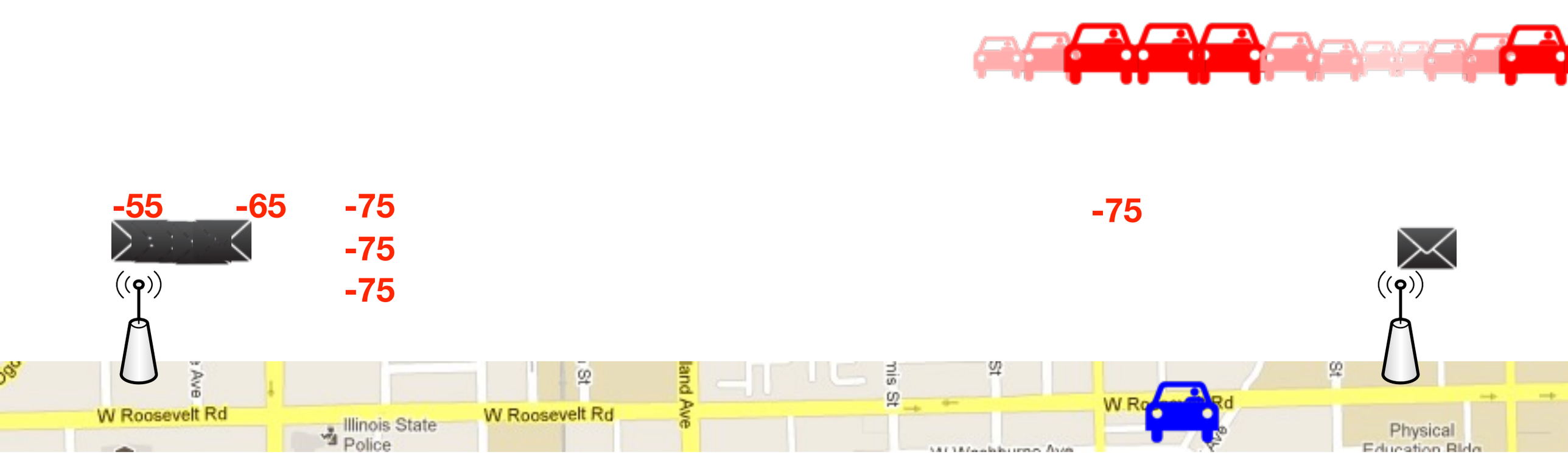
Augmenting detections with RSS



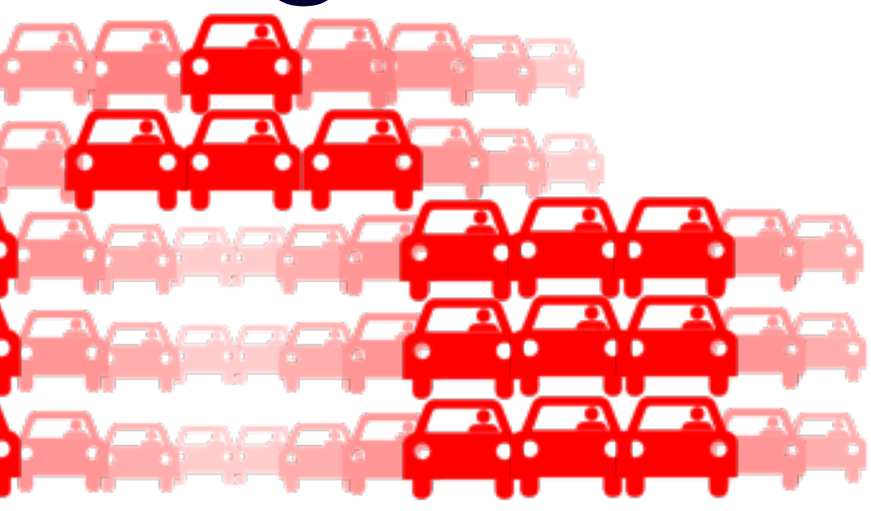


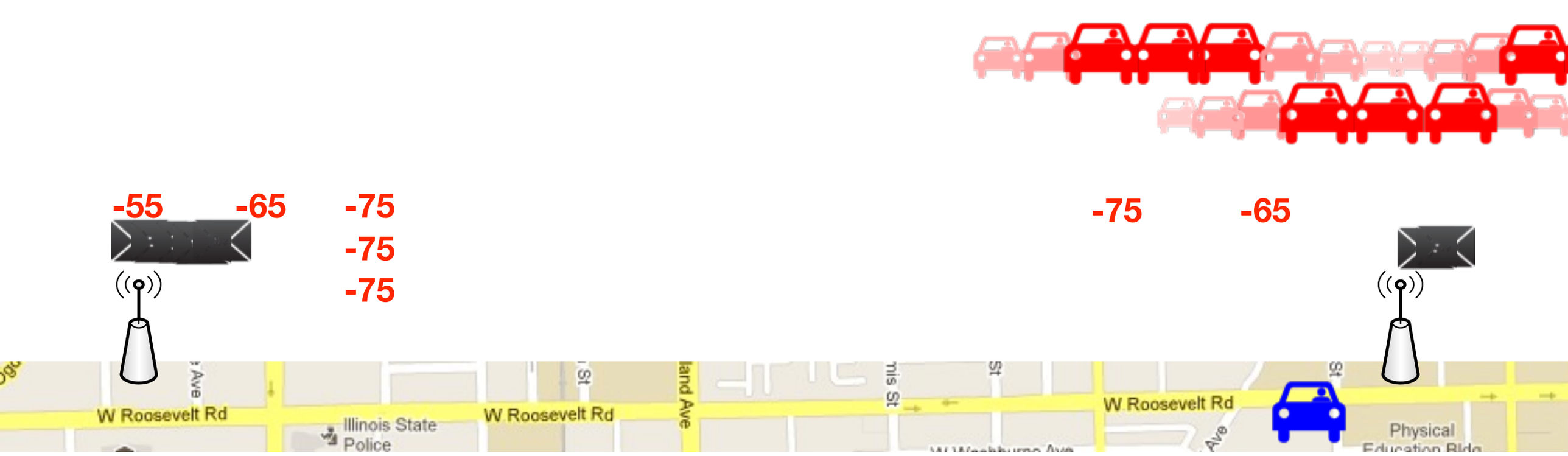
Augmenting detections with RSS



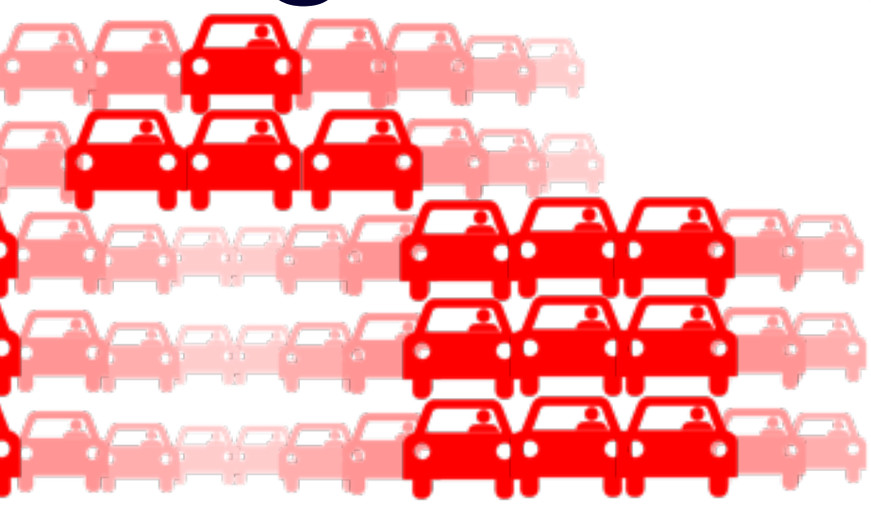


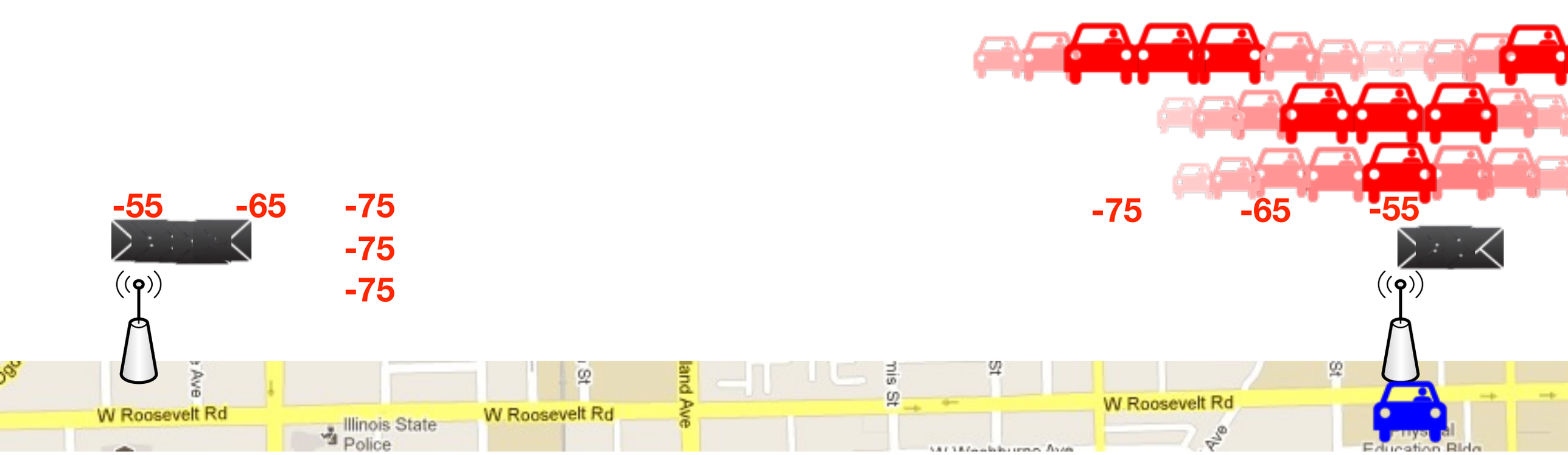
Augmenting detections with RSS



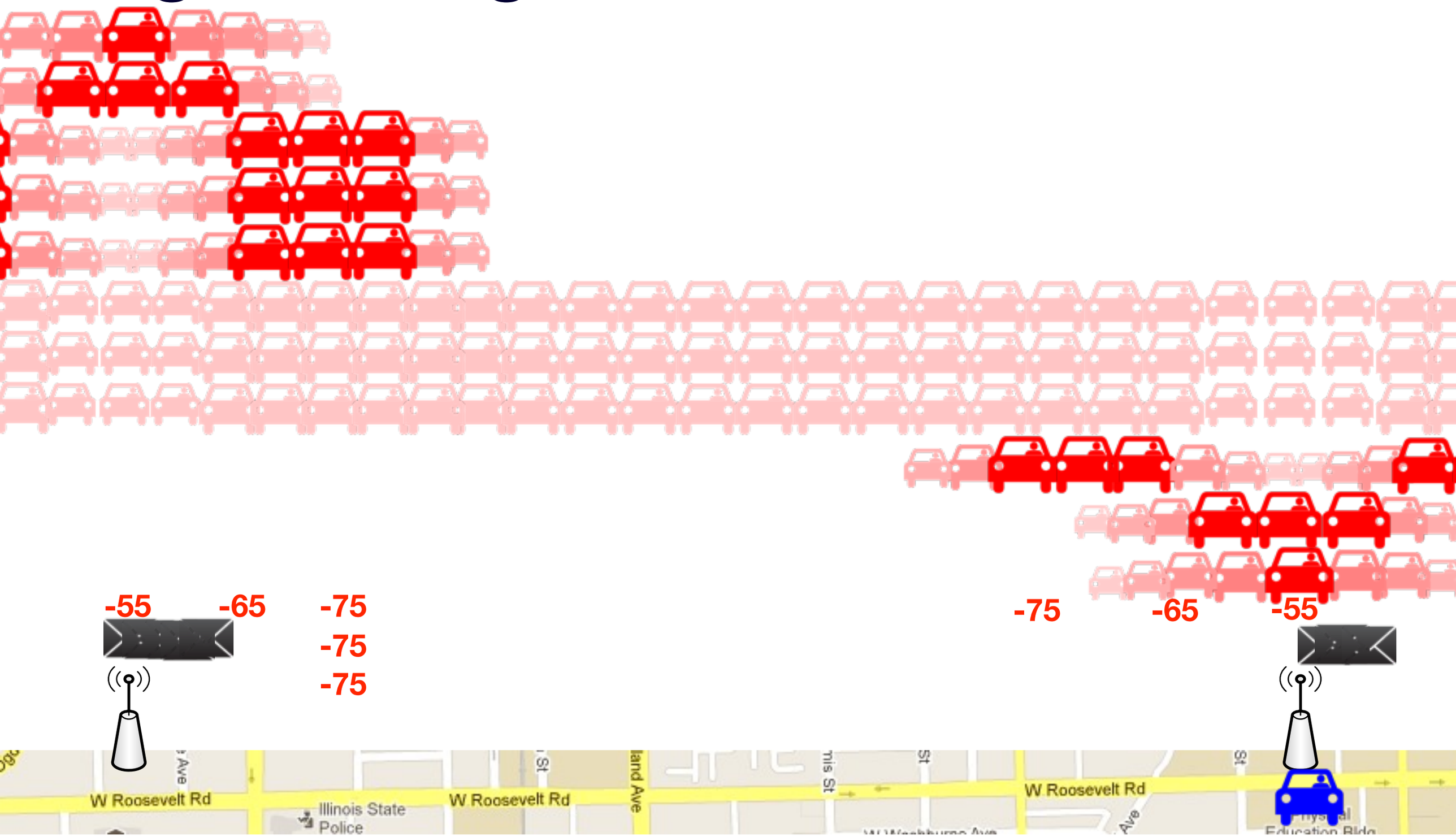


Augmenting detections with RSS

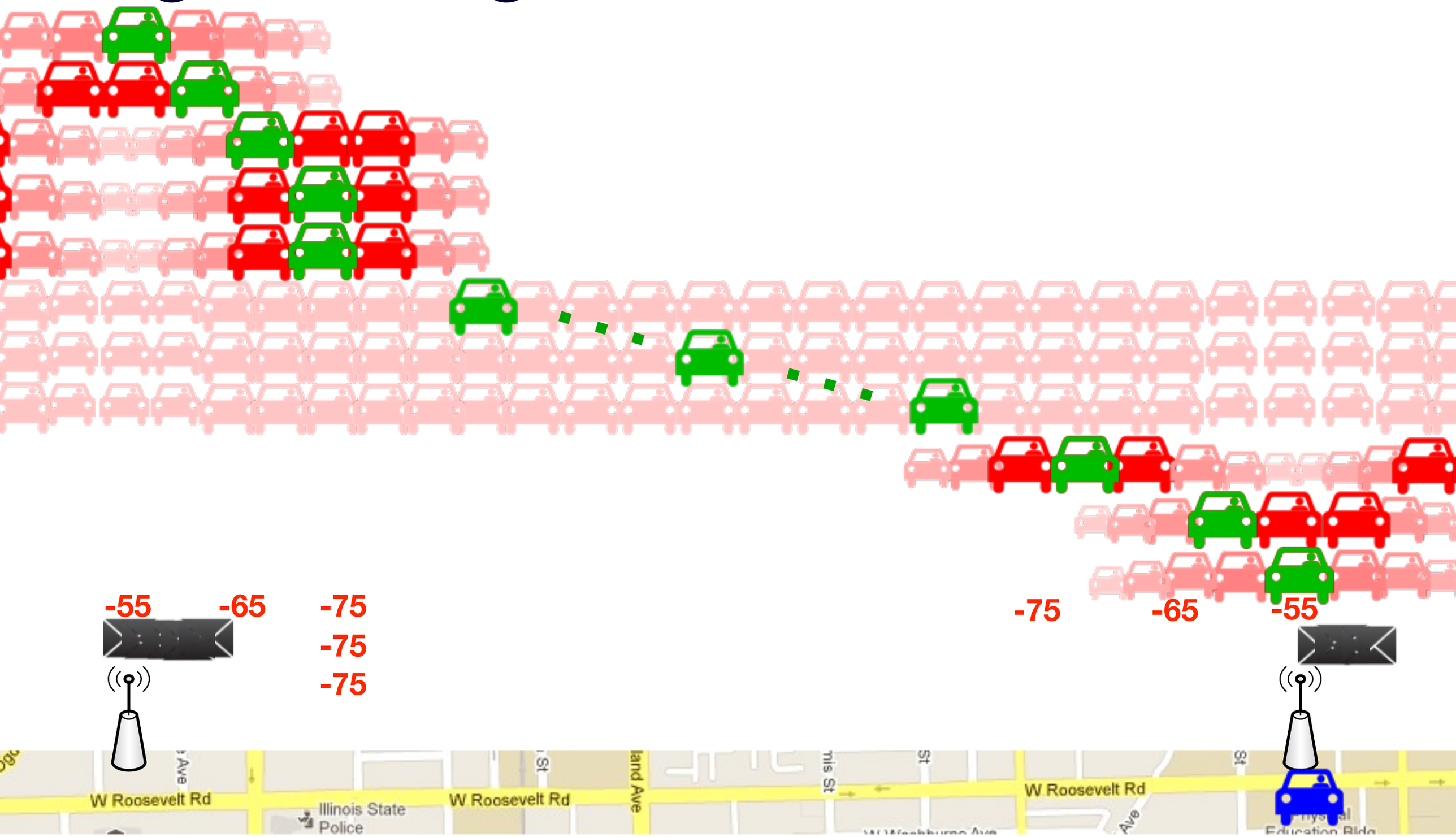




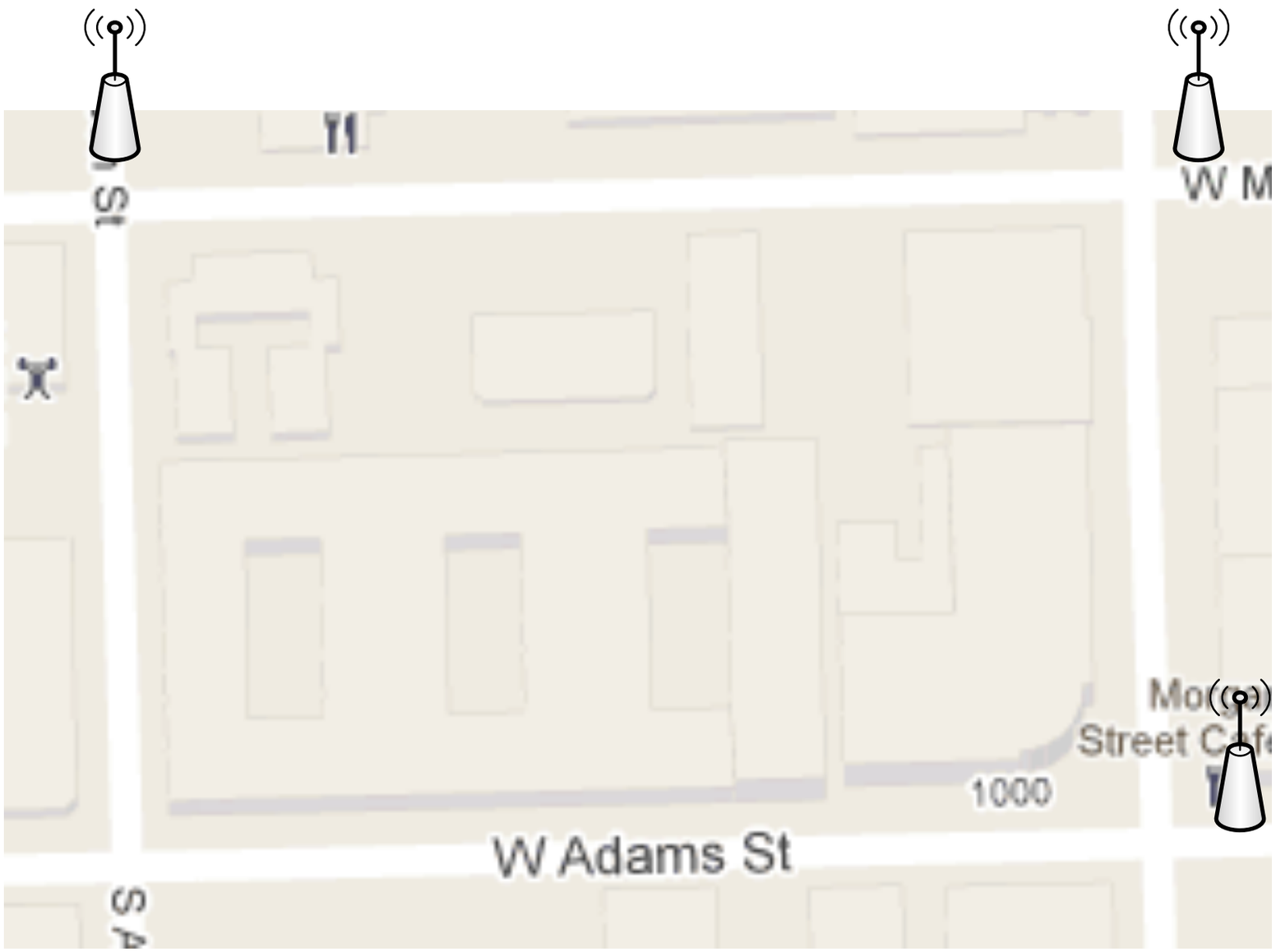
Augmenting detections with RSS



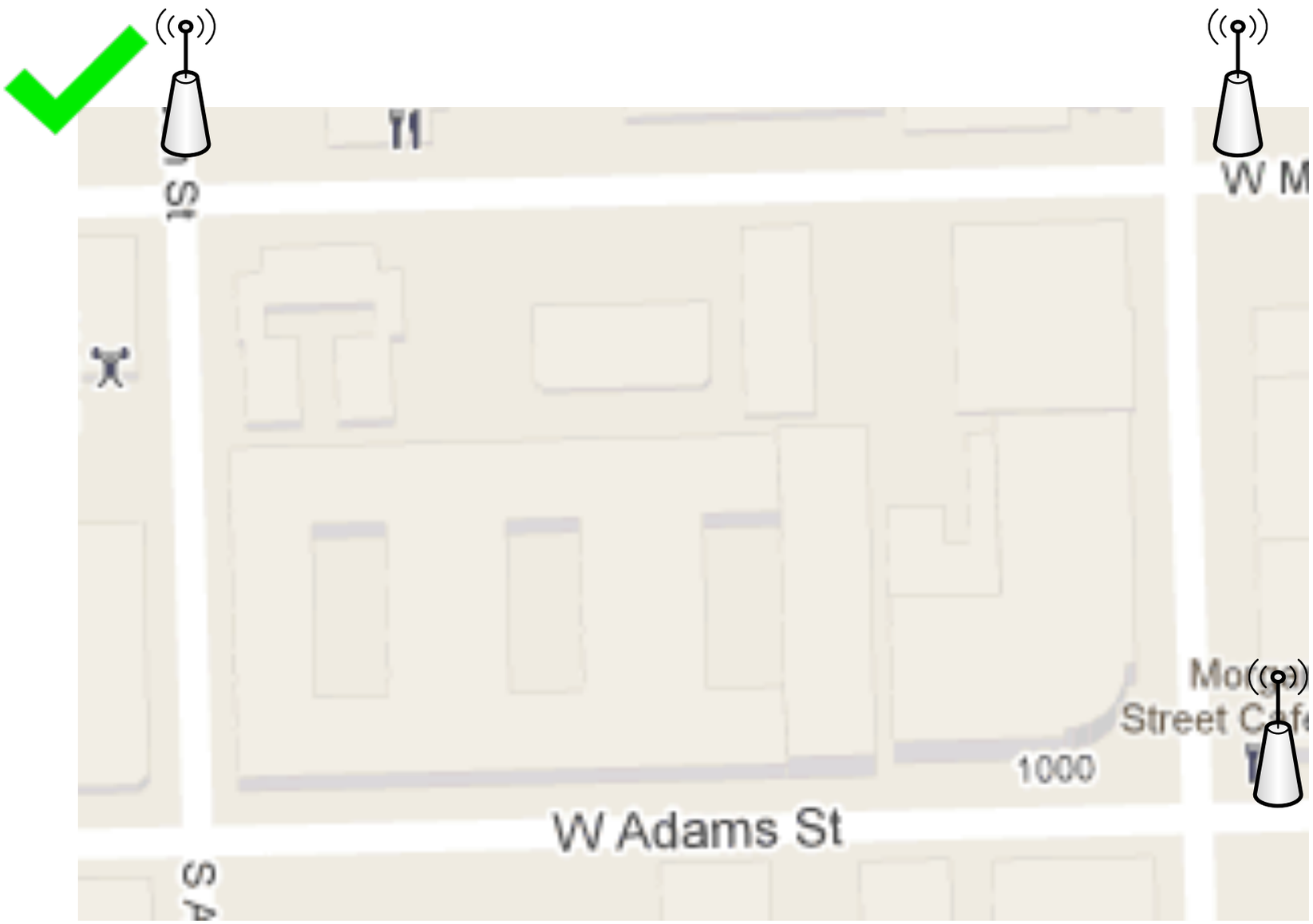
Augmenting detections with RSS



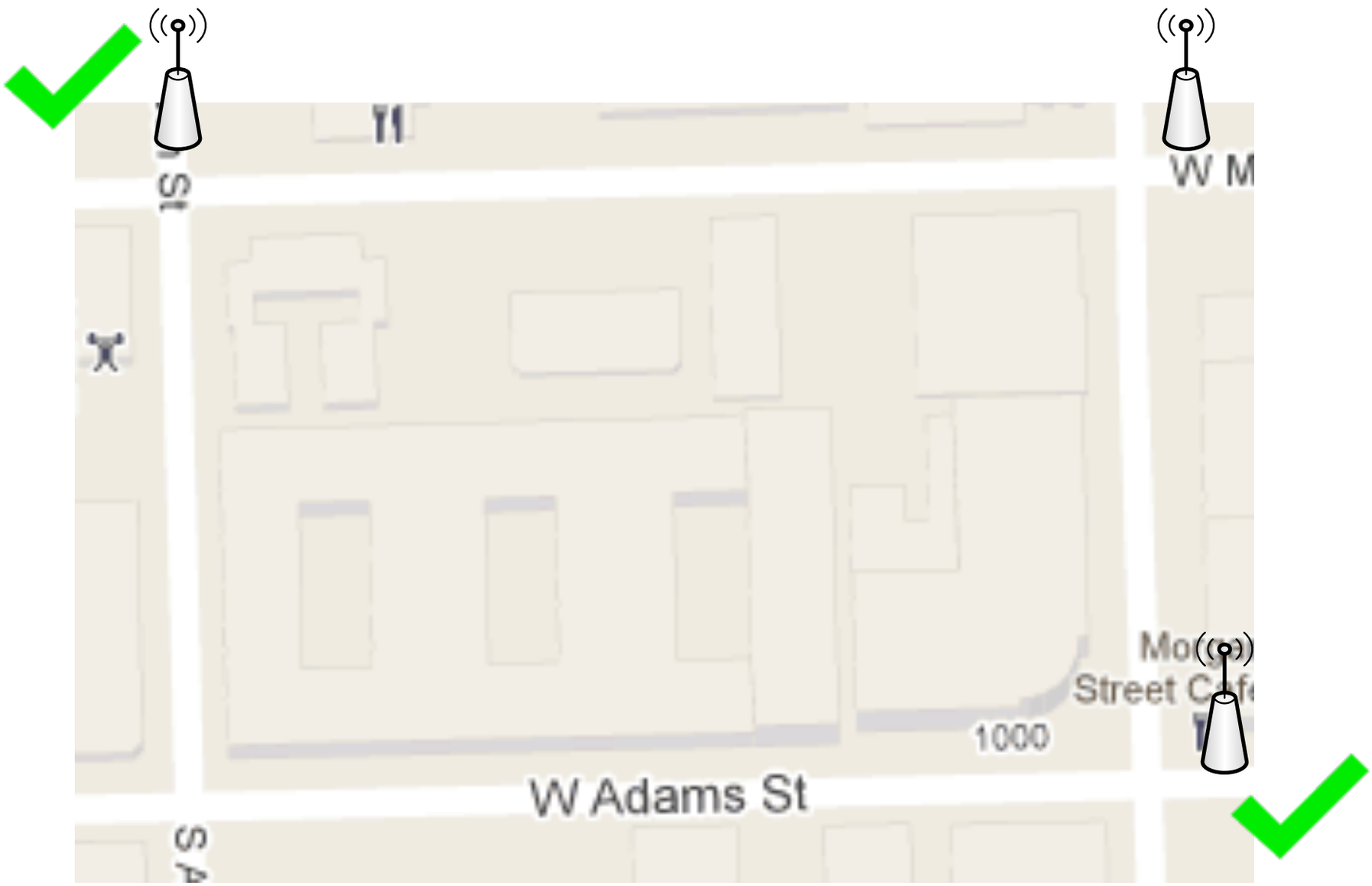
Non-detections are important



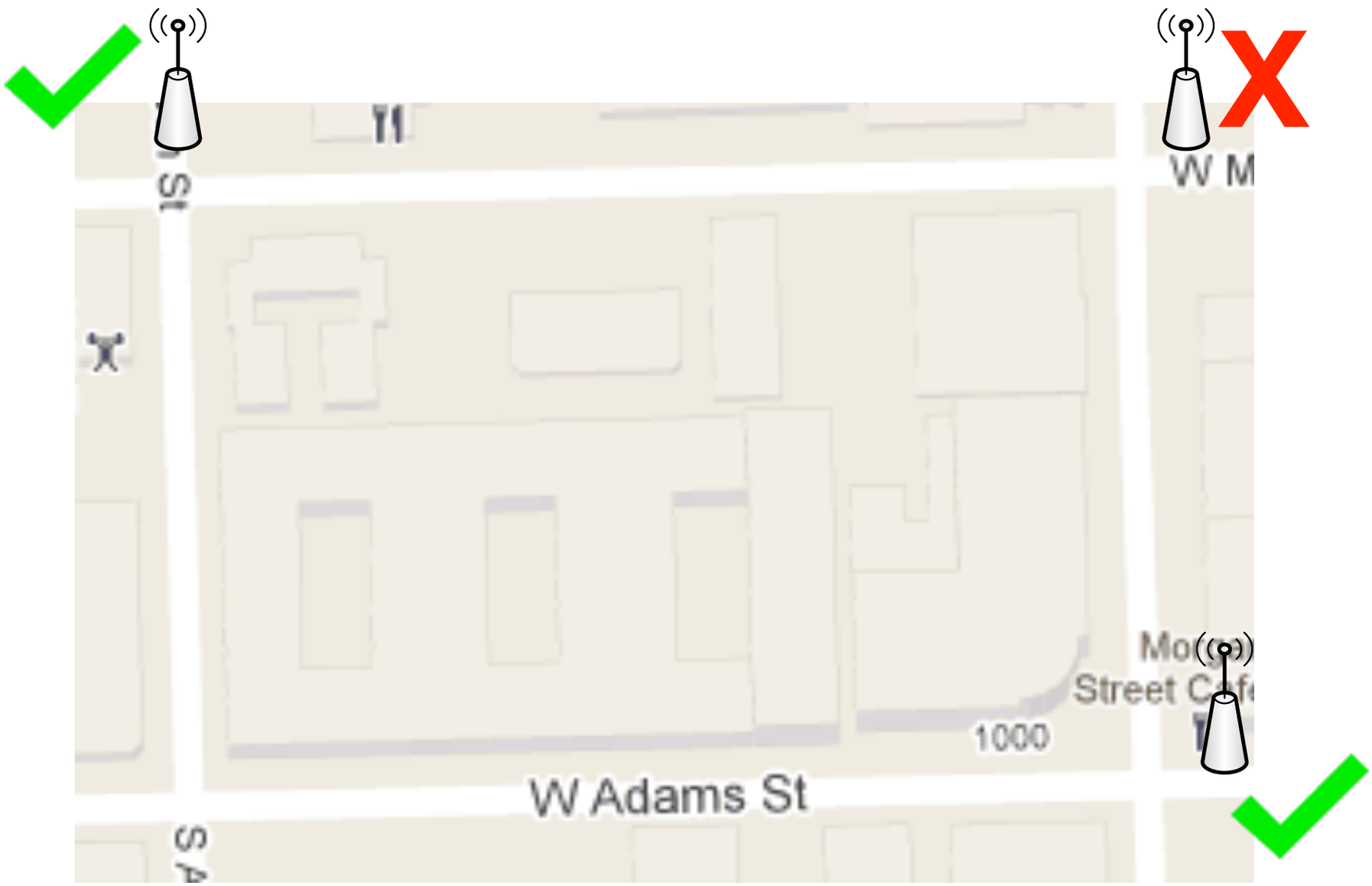
Non-detections are important



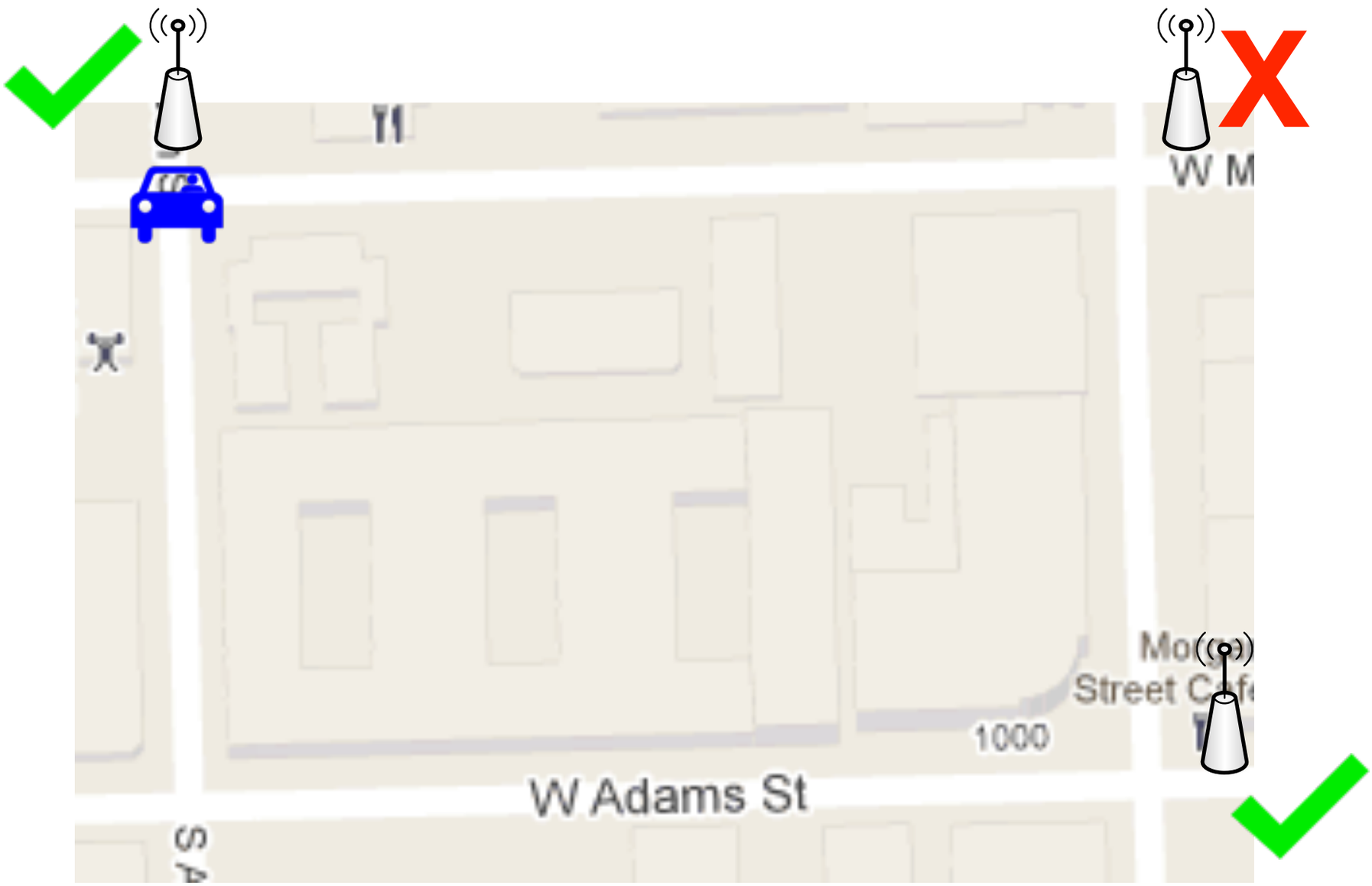
Non-detections are important



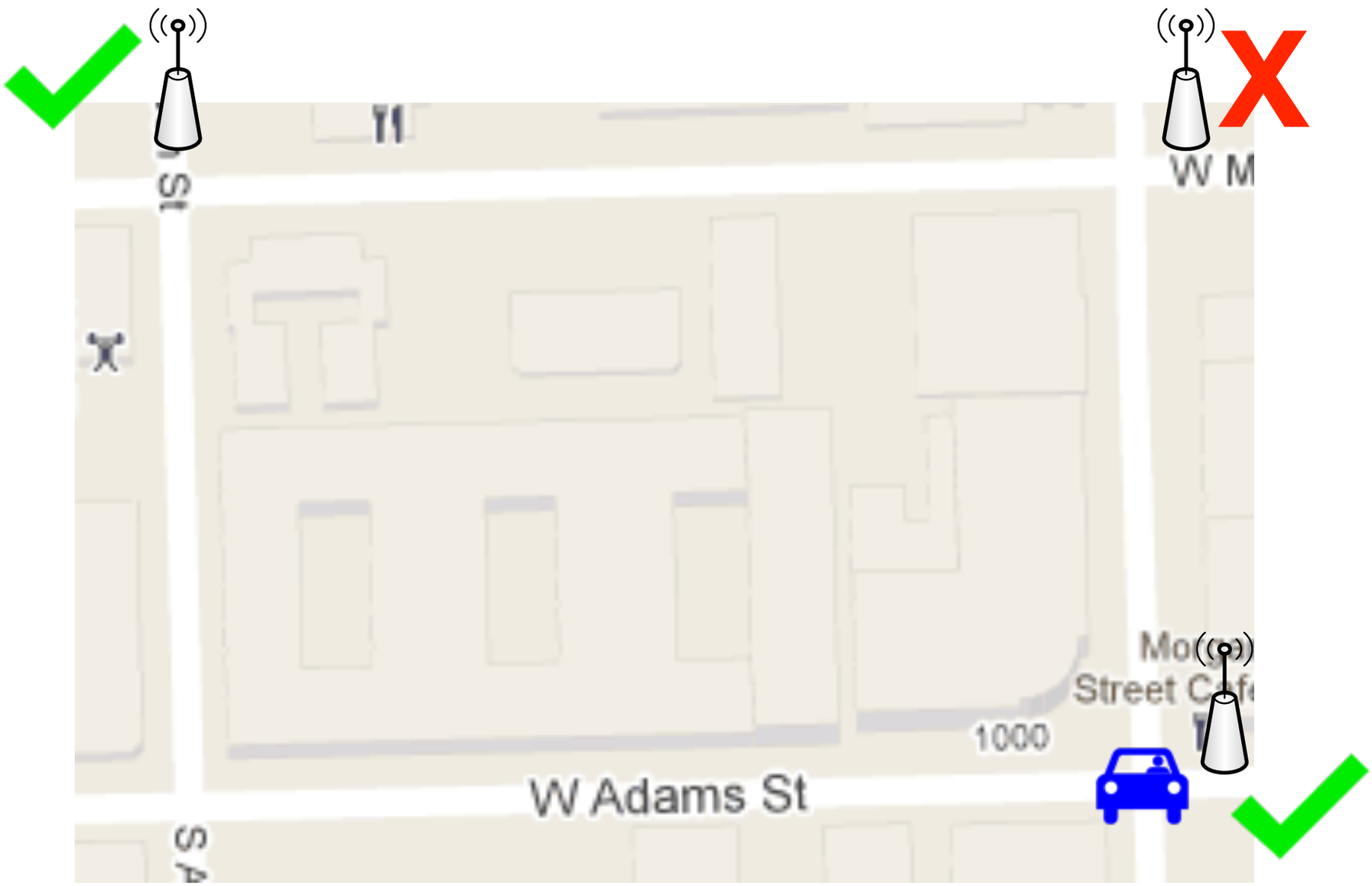
Non-detections are important



Non-detections are important



Non-detections are important



Emission probability

$$p(obs|s) = p_{tx} \prod_{m \in obs} p(e_m|s, tx)$$

Where

$$e_m = detection_m \text{ or } e_m = nondetection_m$$

$$p(detection_m|s, tx) = \int_x \int_y p(dist(x, y, m)|RSS)dxdy$$

$$p(nondetection_m|s) = 1 - p(detection_m|s)$$

Emission probability

$$p(obs|s) = p_{tx} \prod_{m \in obs} p(e_m|s, tx)$$

Where

$$e_m = detection_m \text{ or } e_m = nondetection_m$$

$$p(detection_m|s, tx) = \int_x \int_y p(dist(x, y, m)|RSS)dxdy$$

$$p(nondetection_m|s) = 1 - p(detection_m|s)$$

Emission probability

$$p(obs|s) = p_{tx} \prod_{m \in obs} p(e_m|s, tx)$$

Where

$$e_m = detection_m \text{ or } e_m = nondetection_m$$

$$p(detection_m|s, tx) = \int_x \int_y p(dist(x, y, m)|RSS)dxdy$$

$$p(nondetection_m|s) = 1 - p(detection_m|s)$$

Emission probability

$$p(obs|s) = p_{tx} \prod_{m \in obs} p(e_m|s, tx)$$

Where

$e_m = detection_m$ or $e_m = nondetection_m$

$$p(detection_m|s, tx) = \int_x \int_y p(dist(x, y, m)|RSS)dxdy$$

$$p(nondetection_m|s) = 1 - p(detection_m|s)$$

Emission probability

$$p(obs|s) = p_{tx} \prod_{m \in obs} p(e_m|s, tx)$$

Where

$$e_m = detection_m \text{ or } e_m = nondetection_m$$

$$p(detection_m|s, tx) = \int_x \int_y p(dist(x, y, m)|RSS)dxdy$$

$$p(nondetection_m|s) = 1 - p(detection_m|s)$$

Emission probability

$$p(obs|s) = p_{tx} \prod_{m \in obs} p(e_m|s, tx)$$

Where

$$e_m = detection_m \text{ or } e_m = nondetection_m$$

$$p(detection_m|s, tx) = \int_x \int_y p(dist(x, y, m)|RSS)dxdy$$

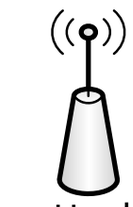
$$p(nondetection_m|s) = 1 - p(detection_m|s)$$

Prompting Additional Transmissions

Popular AP emulation

Popular AP emulation

Popular AP emulation



attwifi
tmobile

Popular AP emulation

Popular AP emulation

Popular AP emulation

Beacon (TIM=...5...)

Popular AP emulation

Beacon (TIM=...5...)

Popular AP emulation

Beacon (TIM=...5...)

Null function

Popular AP emulation

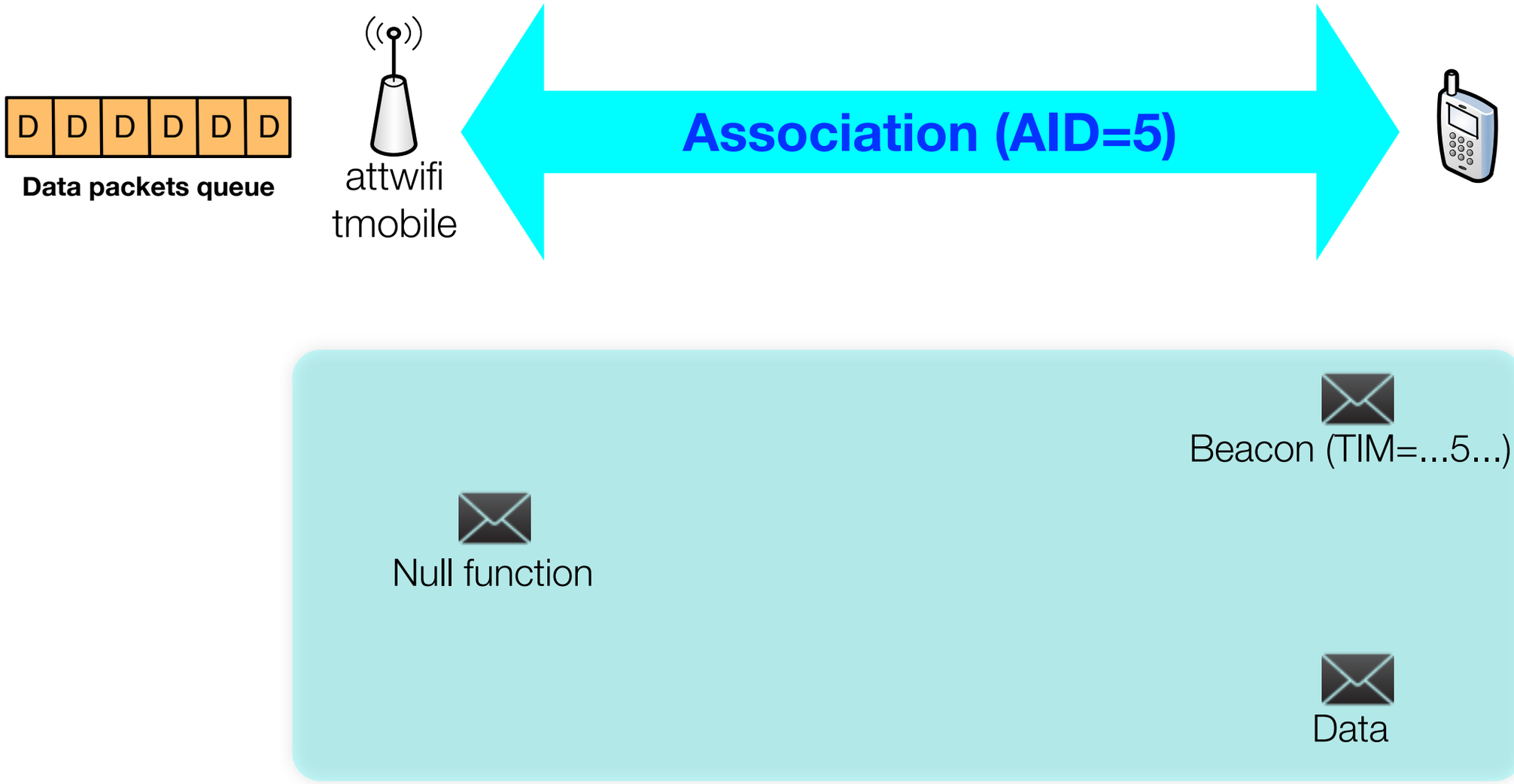

Beacon (TIM=...5...)


Null function


Data

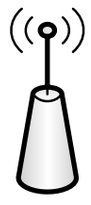
Popular AP emulation

Popular AP emulation



Opportunistic AP emulation

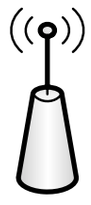
Opportunistic AP emulation



Opportunistic AP emulation

Probe Request (Broadcast)

Opportunistic AP emulation



Opportunistic AP emulation

Probe Request (MyHomeAP)

Opportunistic AP emulation

MyHomeAP security = Open

Probe Request (MyHomeAP)

Opportunistic AP emulation

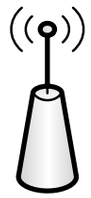
MyHomeAP security = Open

Probe Request (MyHomeAP)

Probe Response (MyHomeAP, Security=Open)

Opportunistic AP emulation

MyHomeAP security = Open



Probe Request (MyHomeAP)

Probe Response (MyHomeAP, Security=Open)

Opportunistic AP emulation

MyHomeAP security = Open

Association

Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP

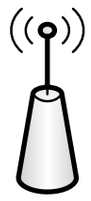
Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP

Probe Request (MyHomeAP)

Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP



Probe Request (MyHomeAP)

Probe Response (MyHomeAP, Security=WPA2 TKIP)

Probe Response (MyHomeAP, Security=WPA2 CCMP)

Opportunistic AP emulation

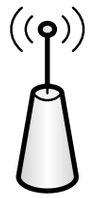
MyHomeAP security = WPA2 TKIP

Probe Response (MyHomeAP, Security=WPA2 TKIP)

Probe Response (MyHomeAP, Security=WPA2 CCMP)

Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP



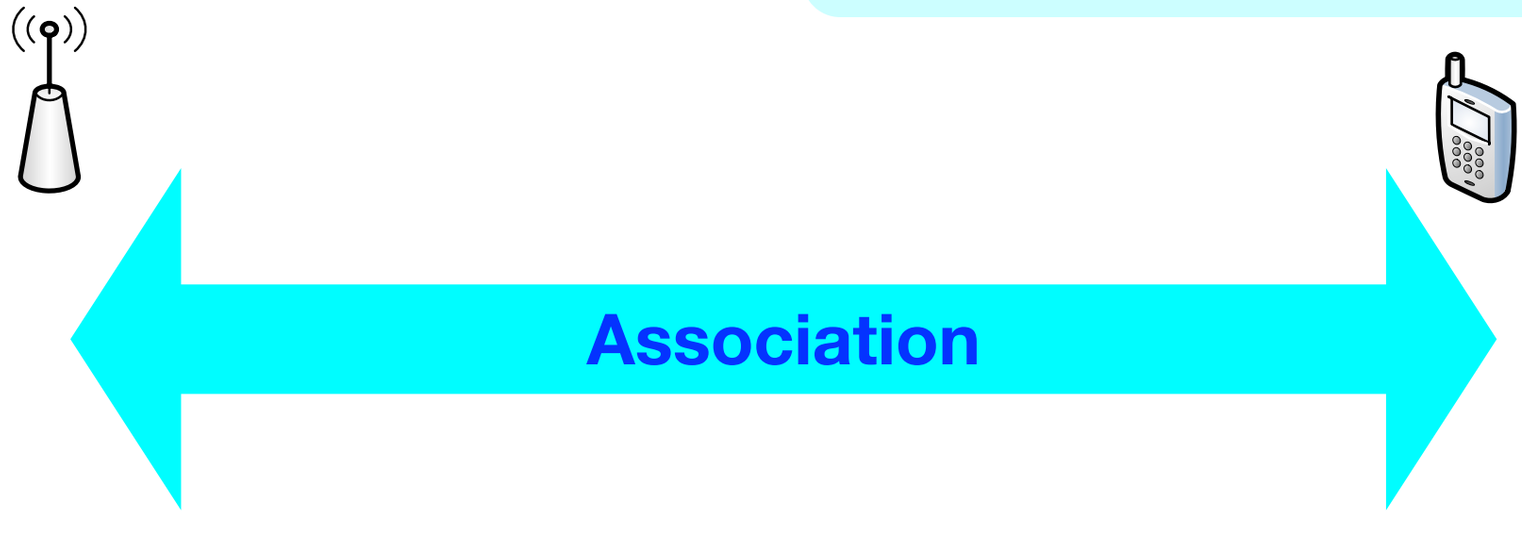
Association

Probe Response (MyHomeAP, Security=WPA2 TKIP)

Probe Response (MyHomeAP, Security=WPA2 CCMP)

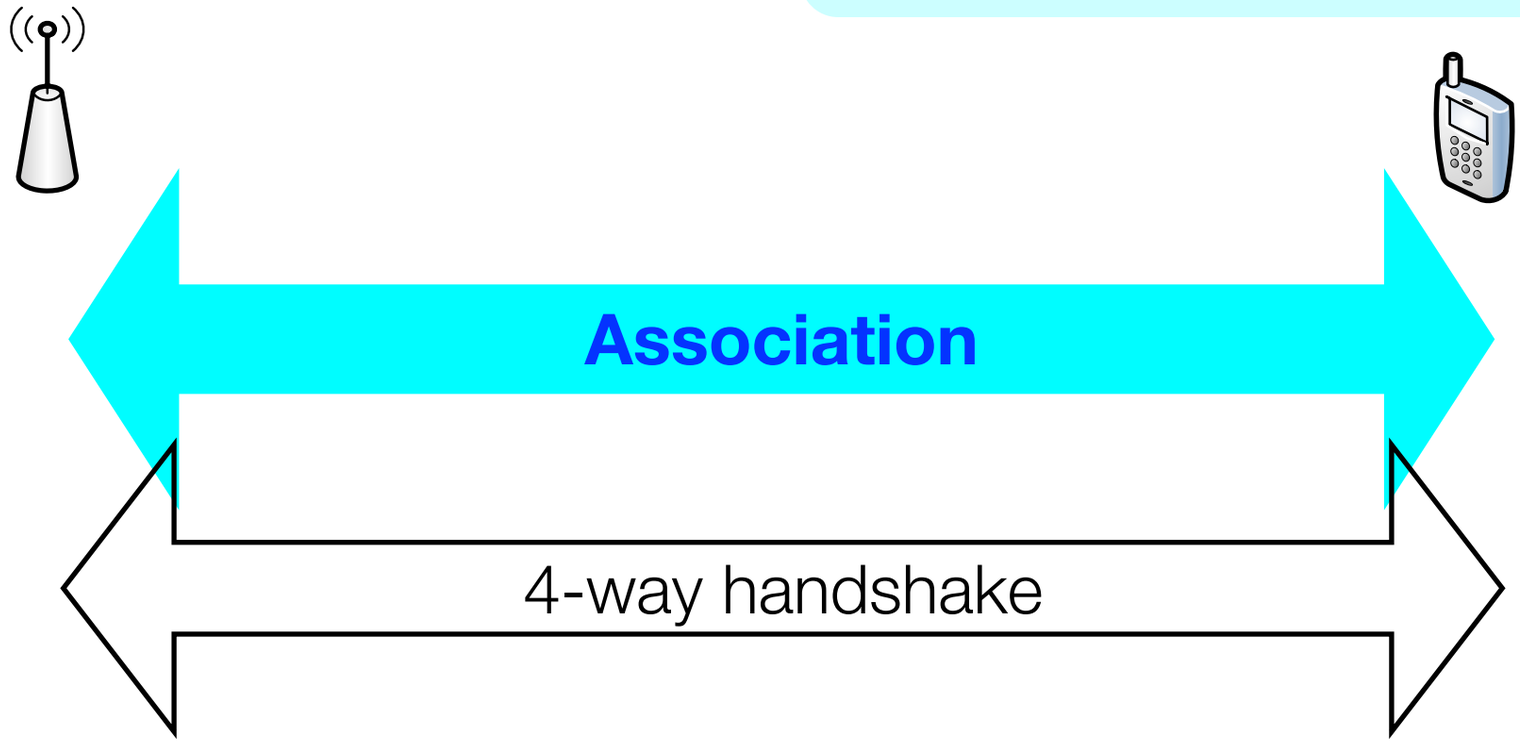
Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP



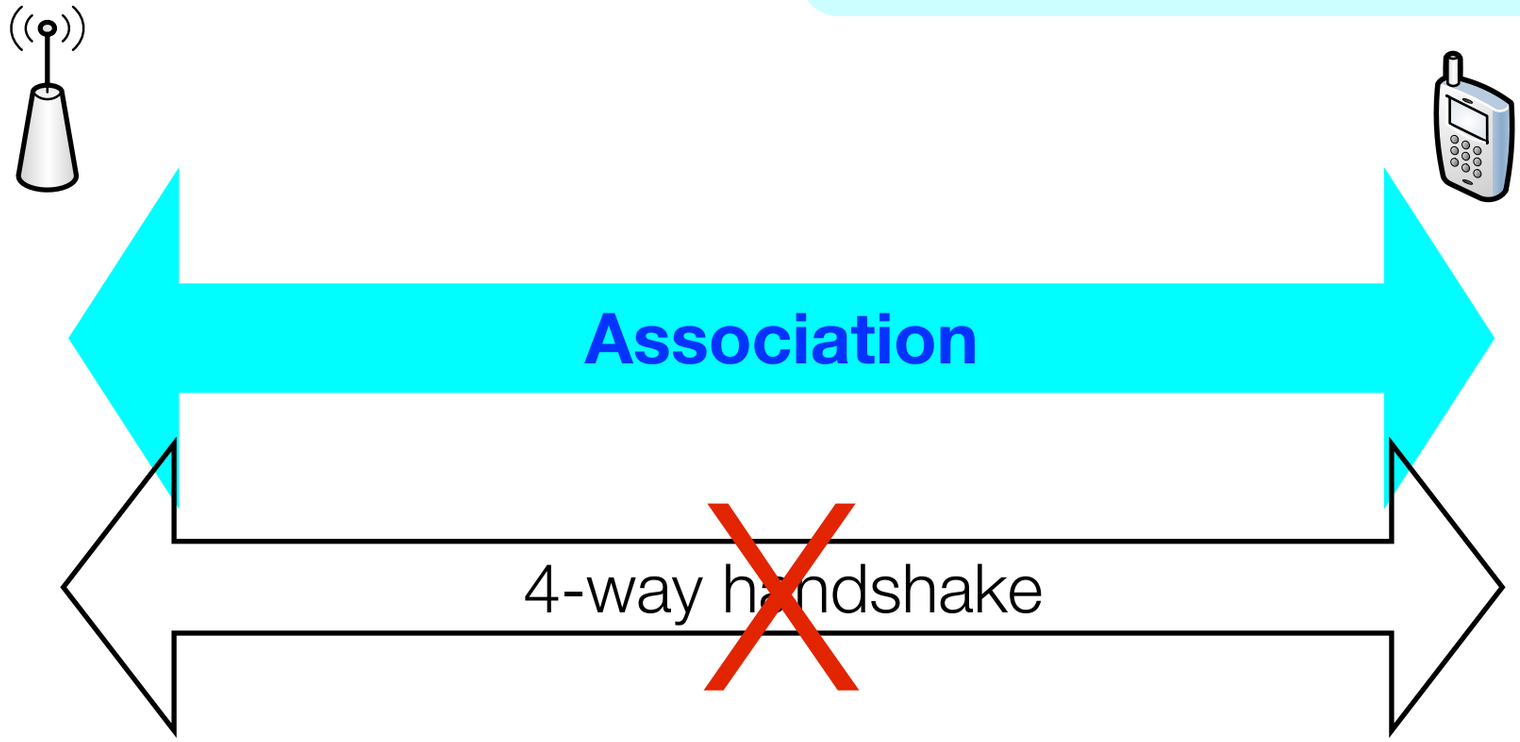
Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP



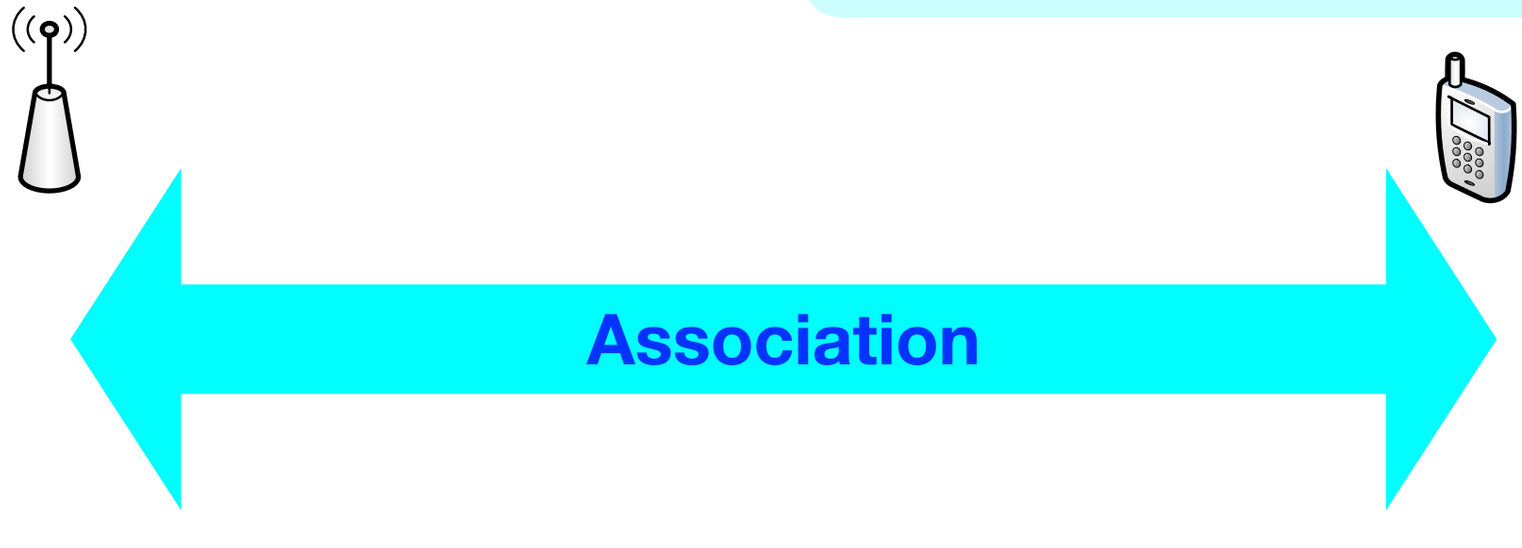
Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP



Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP



Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP

Association

Null function (MyHomeAP)

Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP

Association

Null function (MyHomeAP)

Null function (MyHomeAP)

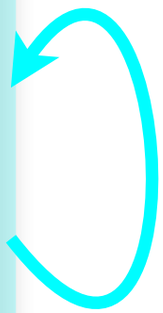
Opportunistic AP emulation

MyHomeAP security = WPA2 TKIP

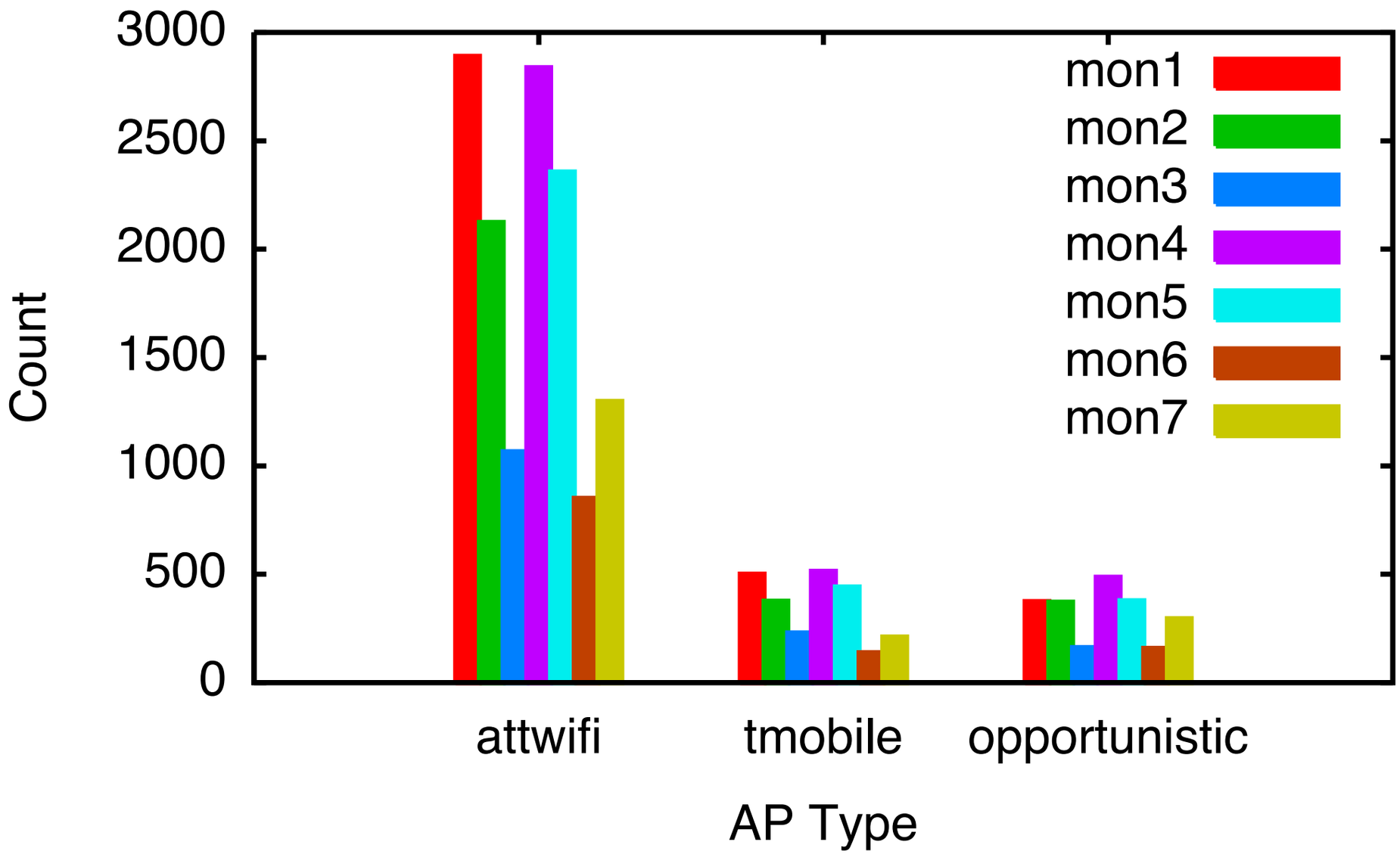
Association

Null function (MyHomeAP)

Null function (MyHomeAP)



AP emulation results



RTS injection

RTS injection

Monitor MAC=E0:...:80

RTS injection

Monitor MAC=E0:...:80

Phone MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

Probe Request (Broadcast)
TX MAC=7C:...:65

Phone MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=E0:...:65
RX MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

Probe Request (Broadcast)
TX MAC=7C:...:65

Phone MAC=7C:...:65

RTS
TX MAC=E0:...:65
RX MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

Probe Request (Broadcast)
TX MAC=7C:...:65

Phone MAC=7C:...:65

RTS
TX MAC=E0:...:65
RX MAC=7C:...:65

CTS
RX MAC=E0:...:80

RTS injection

Monitor MAC=E0:...:80

Probe Request (Broadcast)
TX MAC=7C:...:65

Phone MAC=7C:...:65

RTS
TX MAC=E0:...:65
RX MAC=7C:...:65

CTS
RX MAC=E0:...:80

RTS injection

Monitor MAC=E0:...:80

Probe Request (Broadcast)
TX MAC=7C:...:65

Phone MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

Probe Request (Broadcast)
TX MAC=7C:...:65

Phone MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

CTS
RX MAC=F6:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

CTS
RX MAC=F6:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

CTS
RX MAC=F6:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

CTS
RX MAC=F6:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

CTS
RX MAC=F6:...:65

RTS injection

Monitor MAC=E0:...:80

F6:...:65 = 7C:...:65

Phone MAC=7C:...:65

Probe Request (Broadcast)
TX MAC=7C:...:65

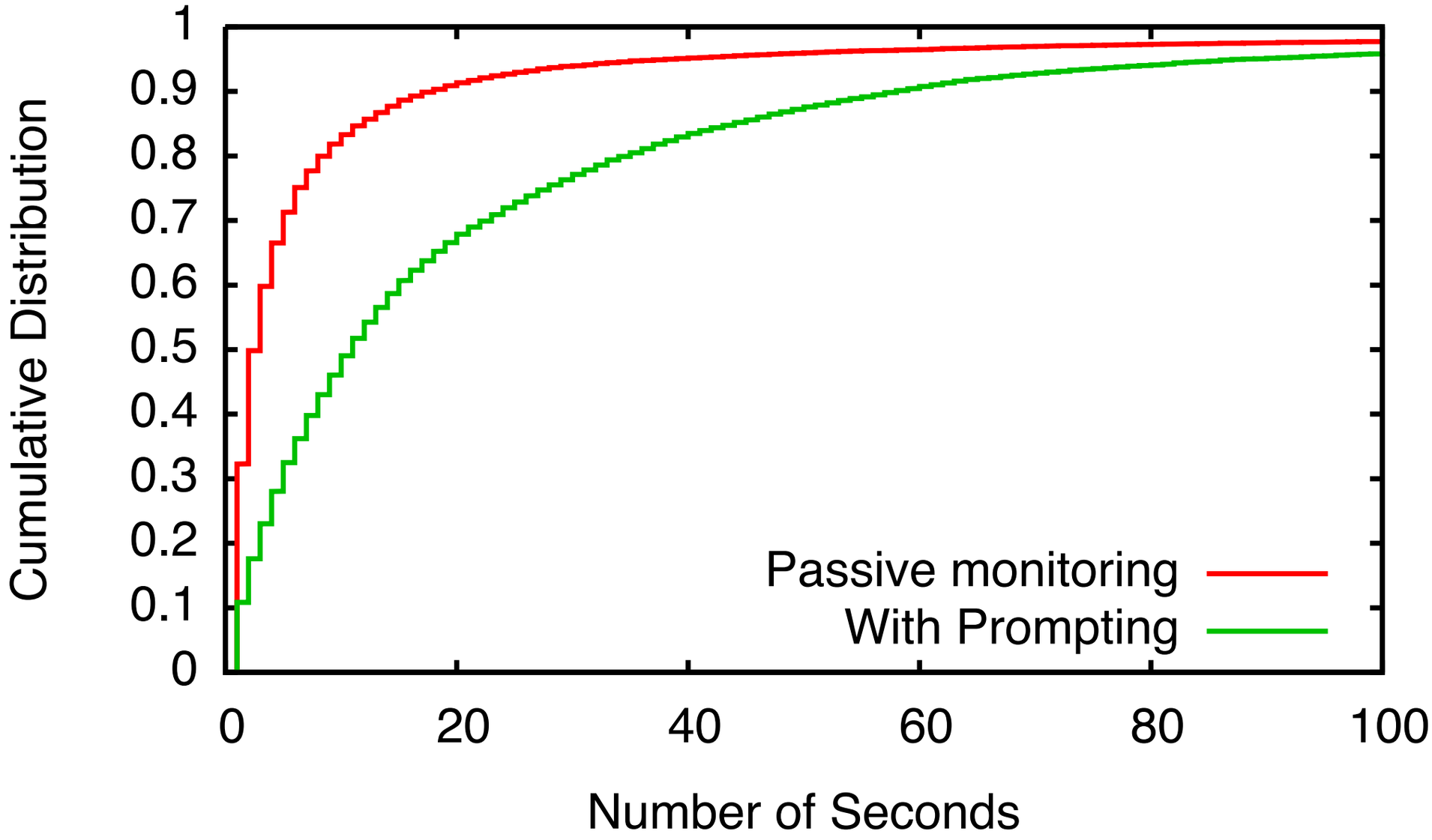
RTS
TX MAC=F6:...:65
RX MAC=7C:...:65

CTS
RX MAC=F6:...:65

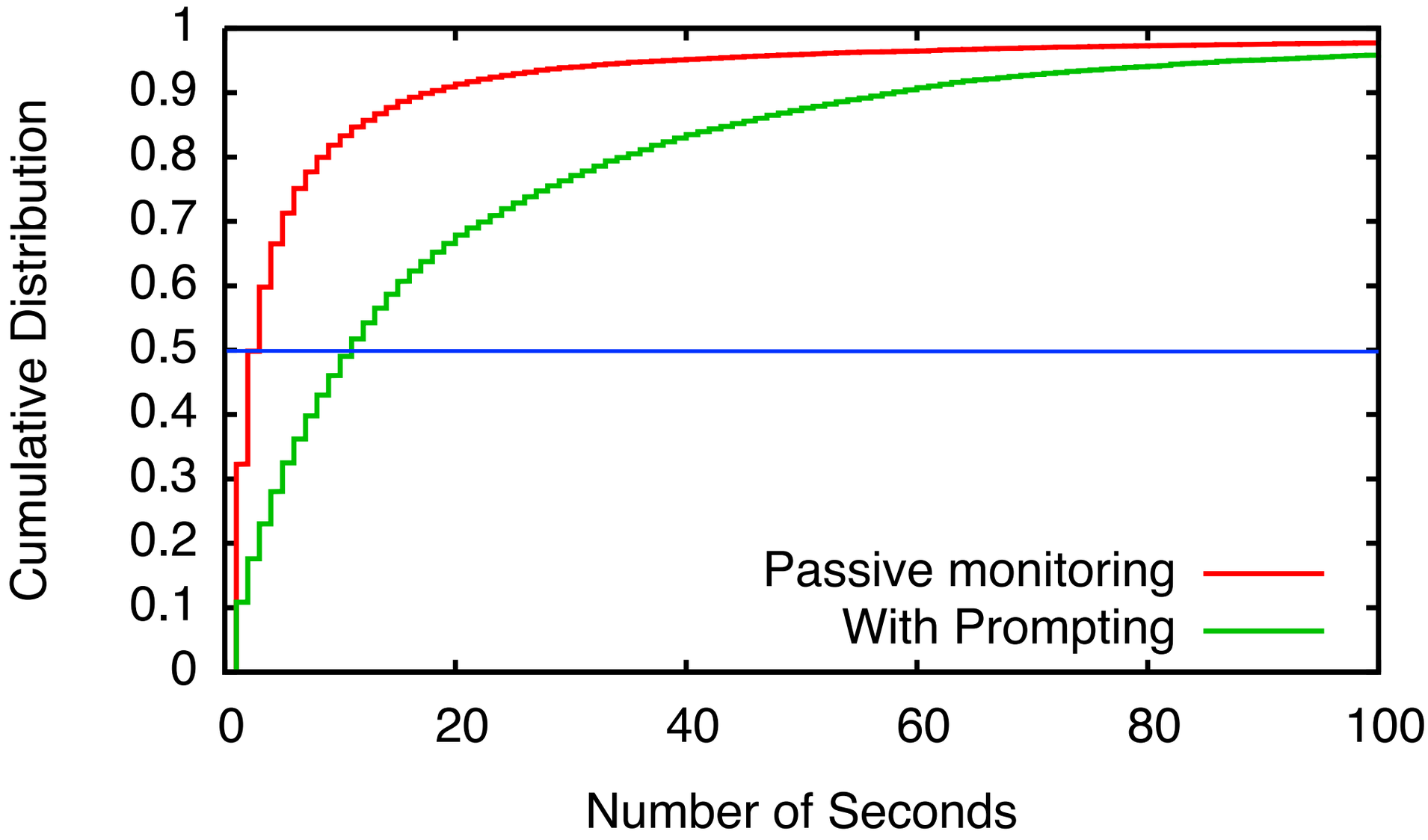
Performance of probing techniques

	Mean Duration
Popular AP emulation:	**31** seconds
Opportunistic AP emulation:	**24** seconds
RTS injection:	**2** seconds

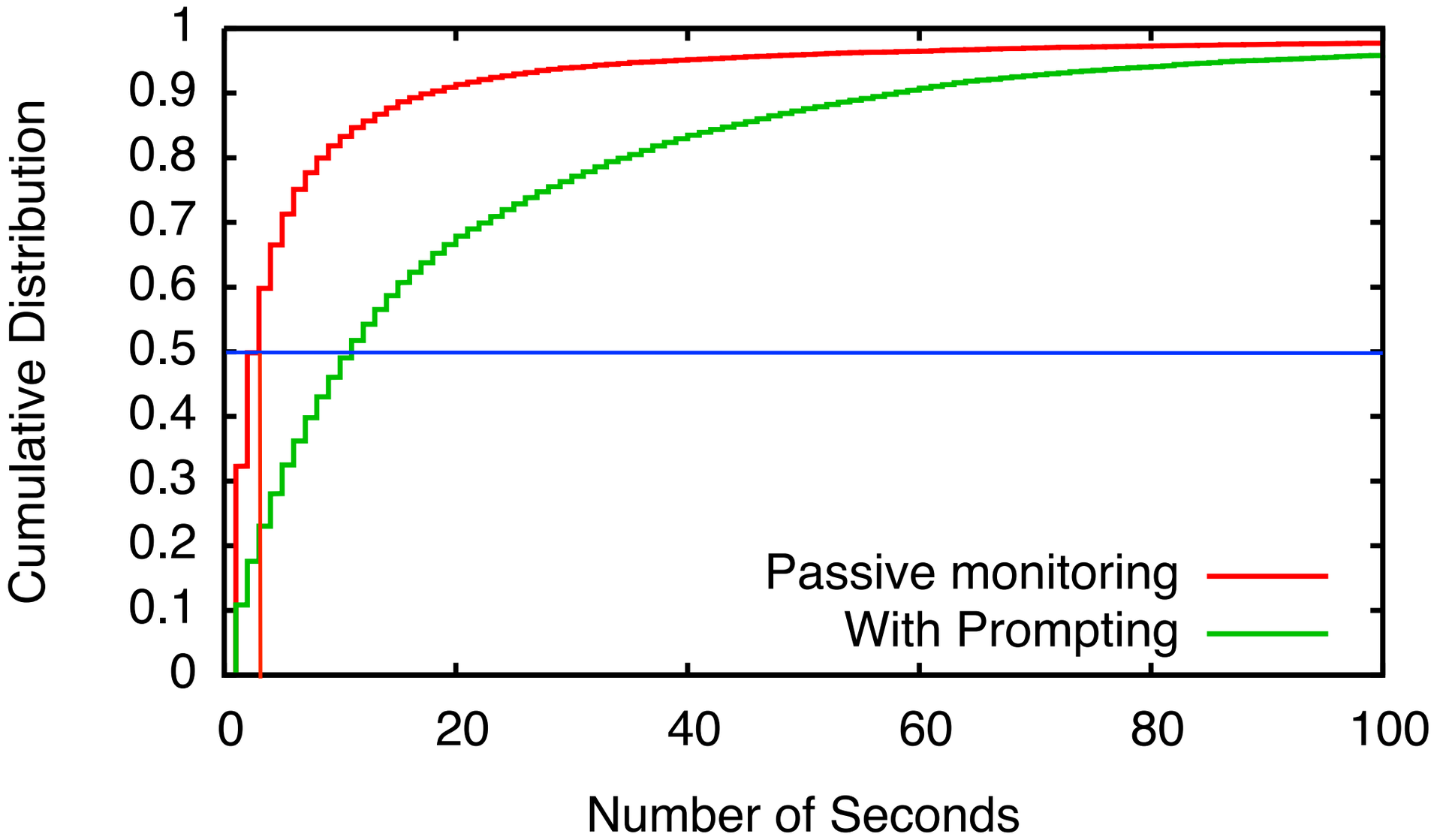
Encounter duration



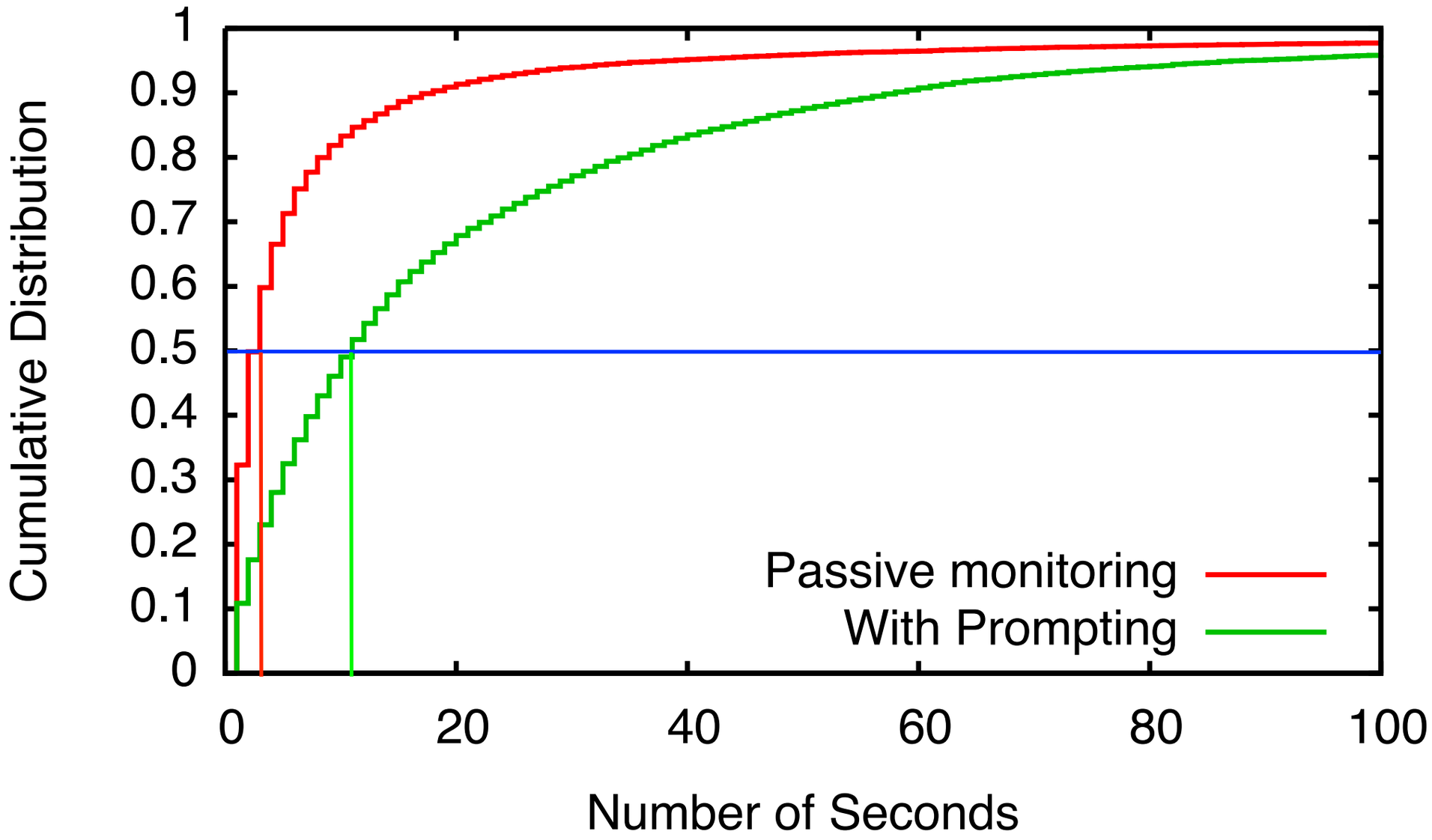
Encounter duration



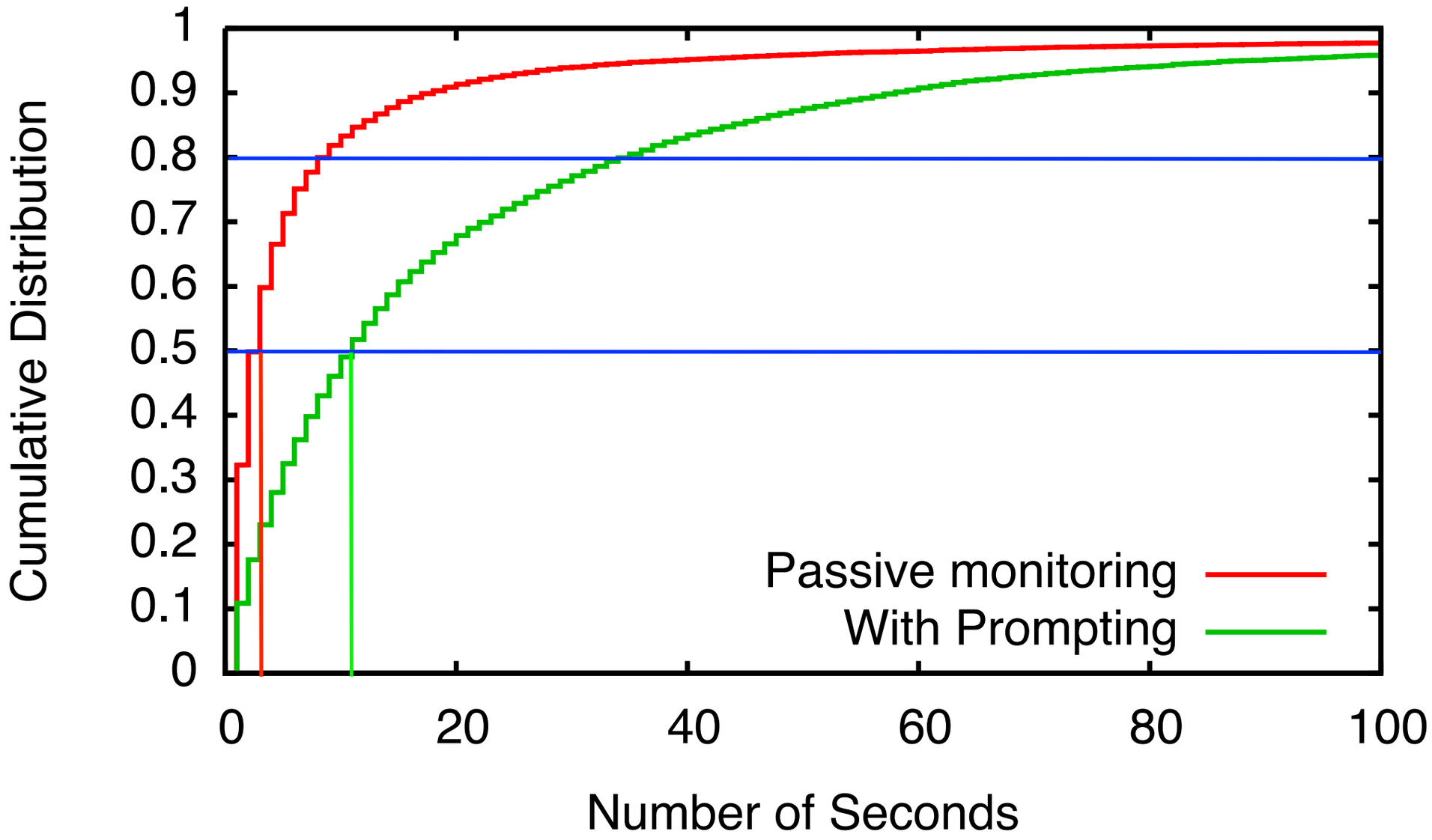
Encounter duration



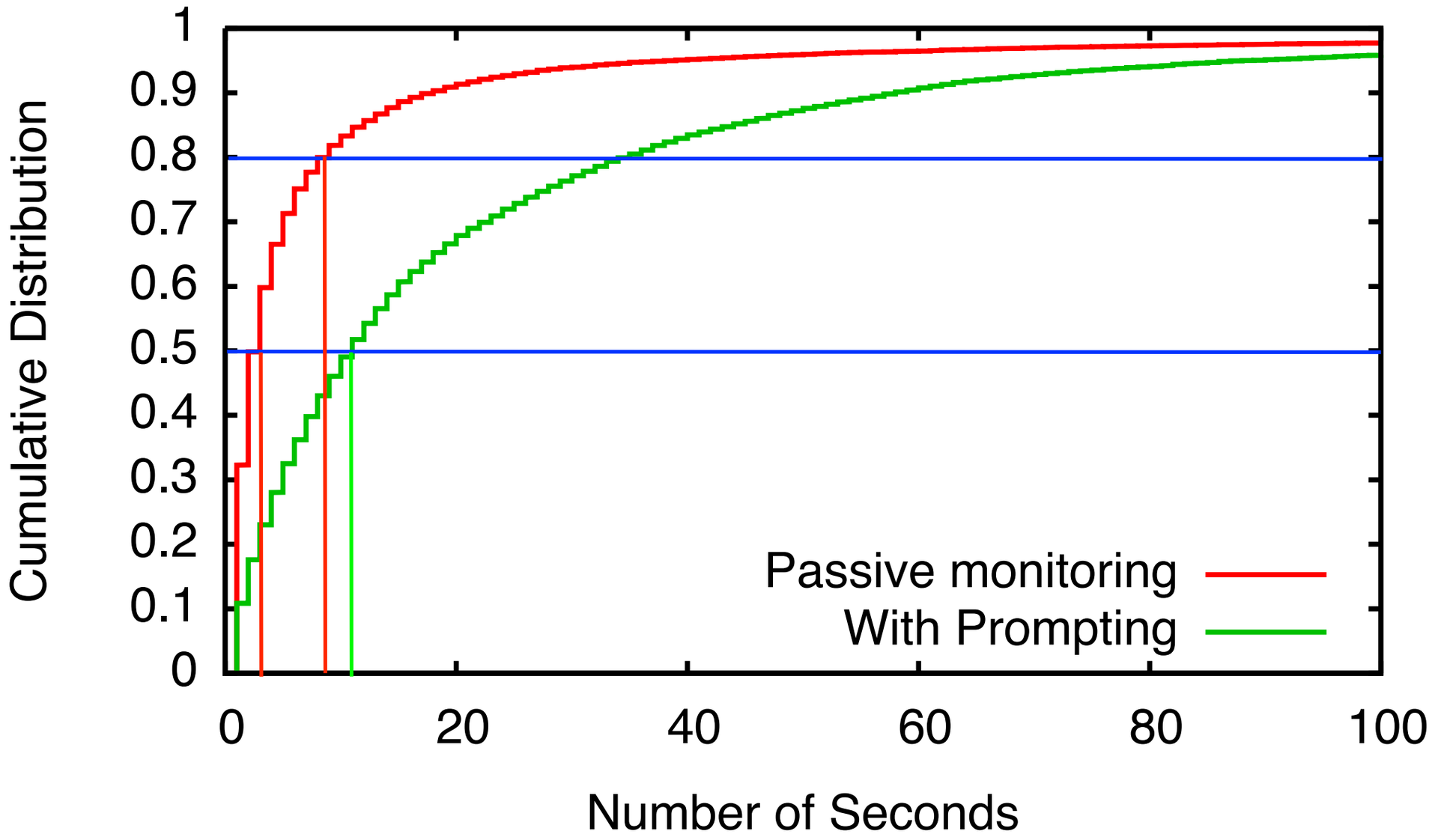
Encounter duration



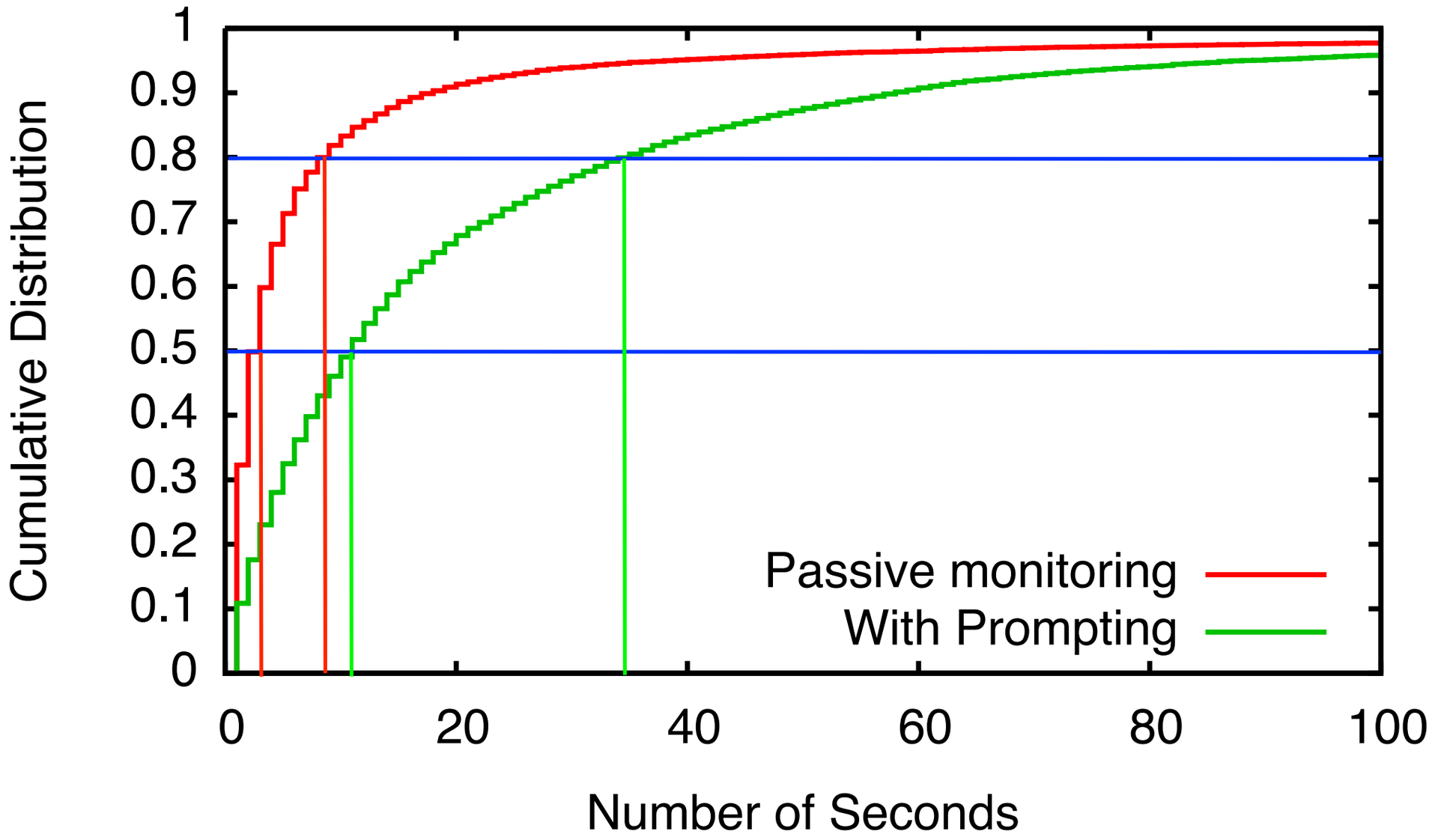
Encounter duration



Encounter duration



Encounter duration

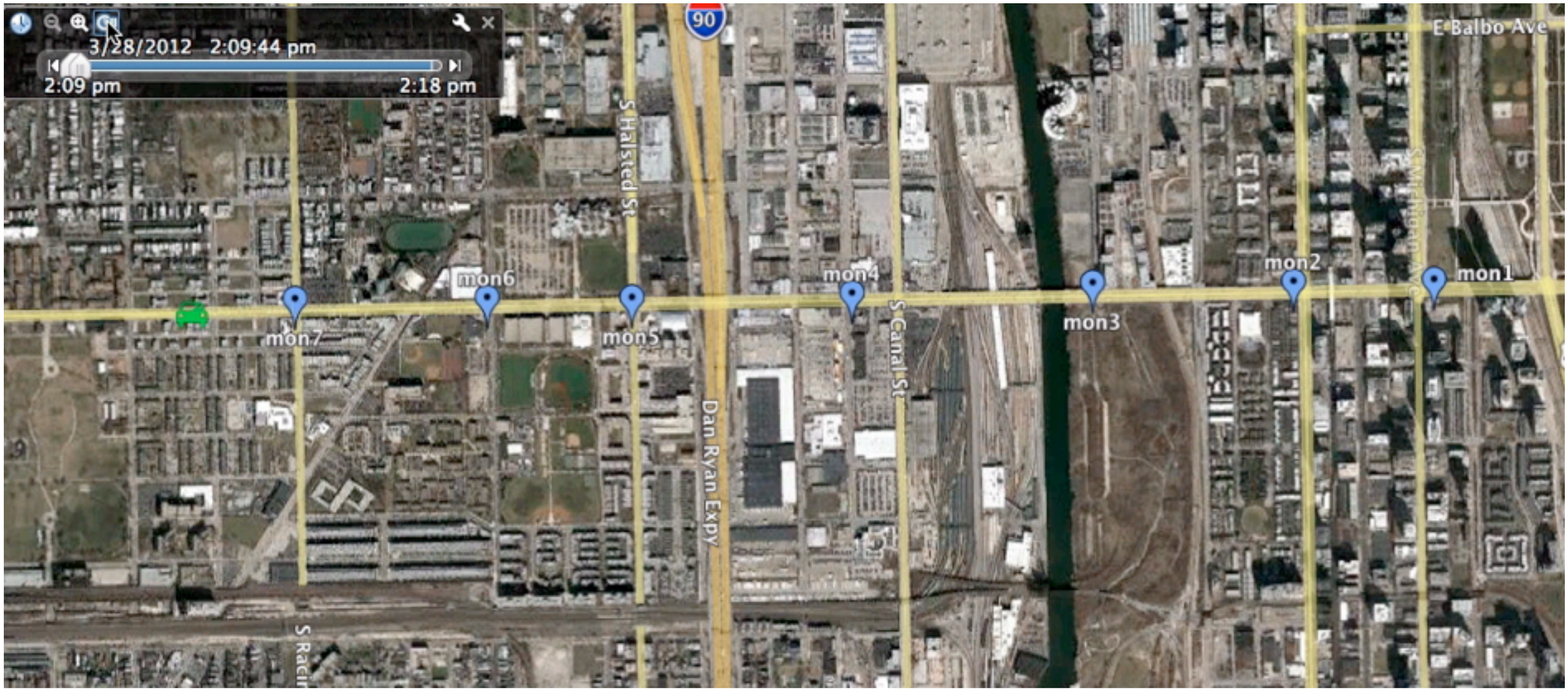


Tracking Performance

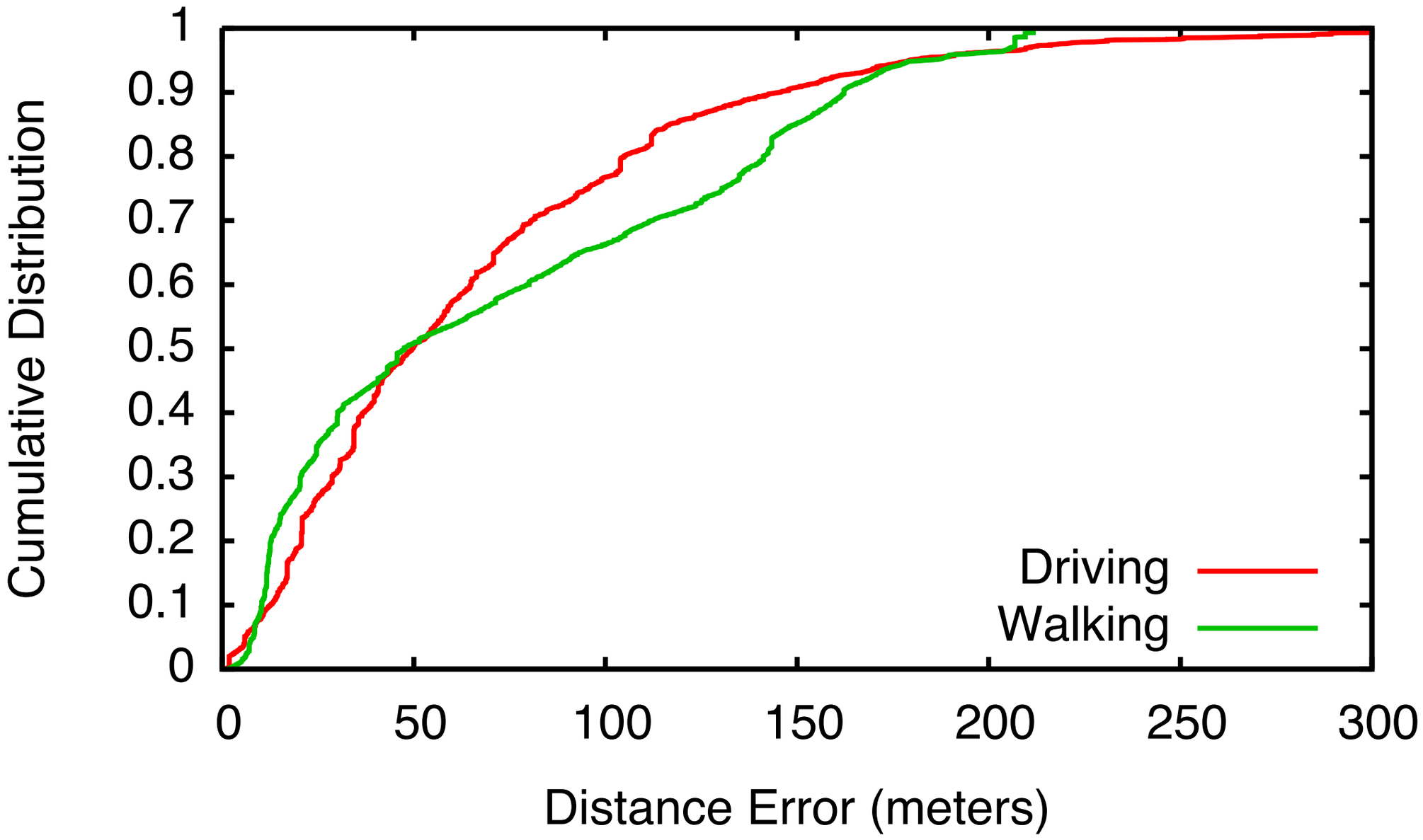
Experimental setup

- 12 hour deployment of 7 monitors along 2.8 km city street
- Drove and walked several times with some smartphones and GPS

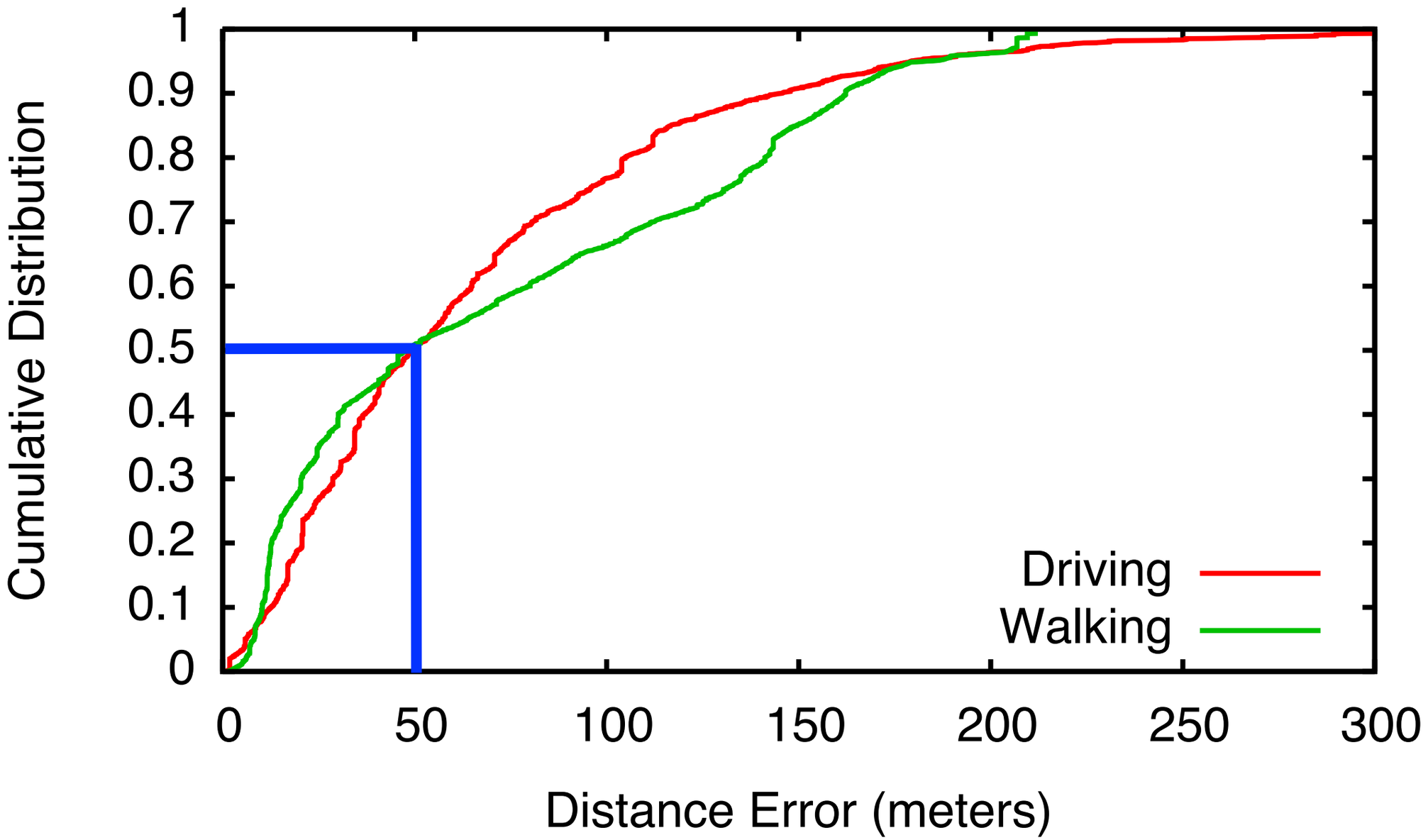
Movie time!


3/28/2012 2:09:44 pm
2:09 pm
2:18 pm
90
E Balbo Ave
S Halsted St
S Michigan Ave
mon6
mon4
mon2
mon1
mon7
mon5
mon3
Dan Ryan Expy
S Canal St

Distance error



Distance error



How many cars do we detect?

12 hour deployment
7000 unique devices
37000 ADT according to DOT

How many cars do we detect?

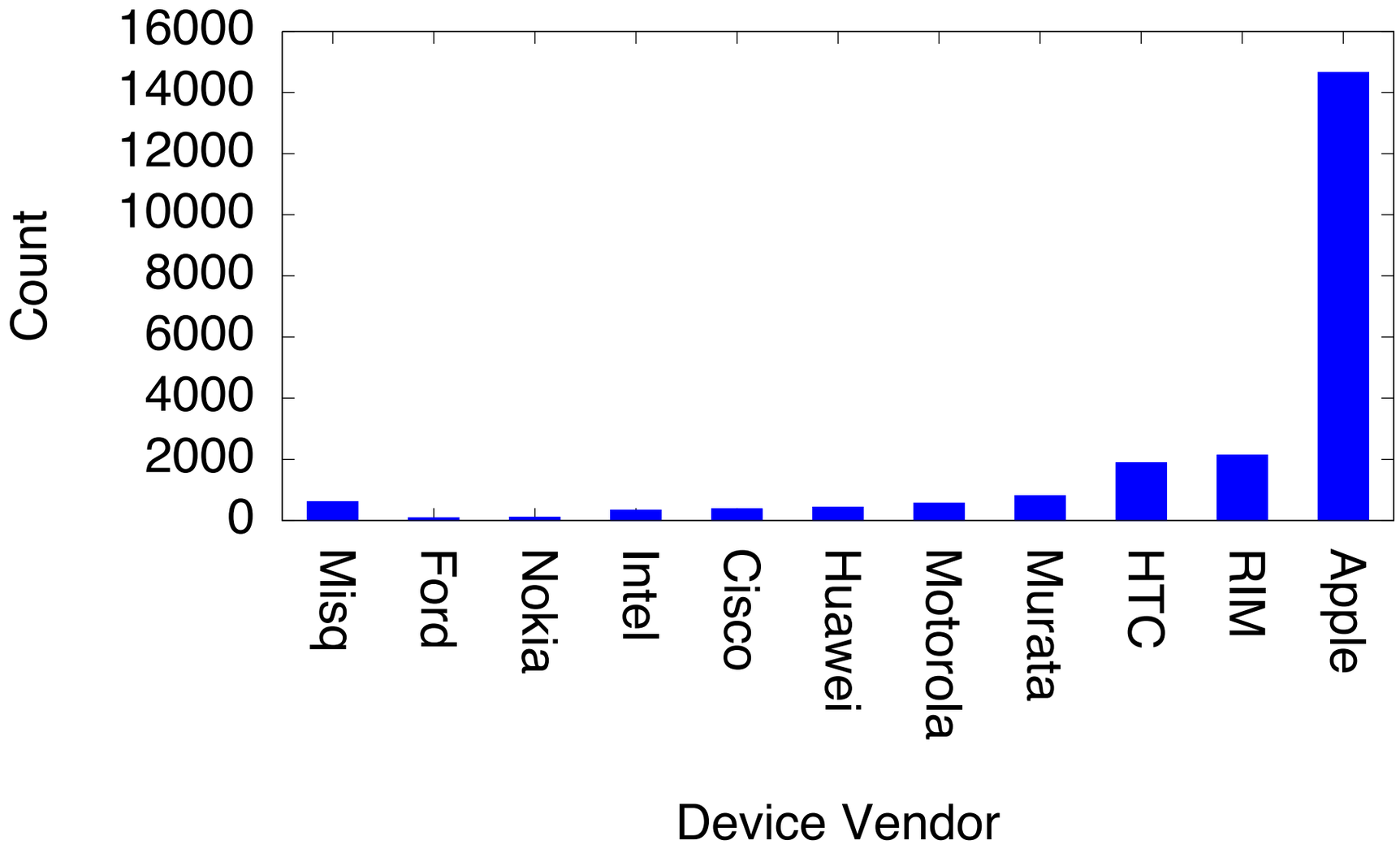
12 hour deployment

7000 unique devices

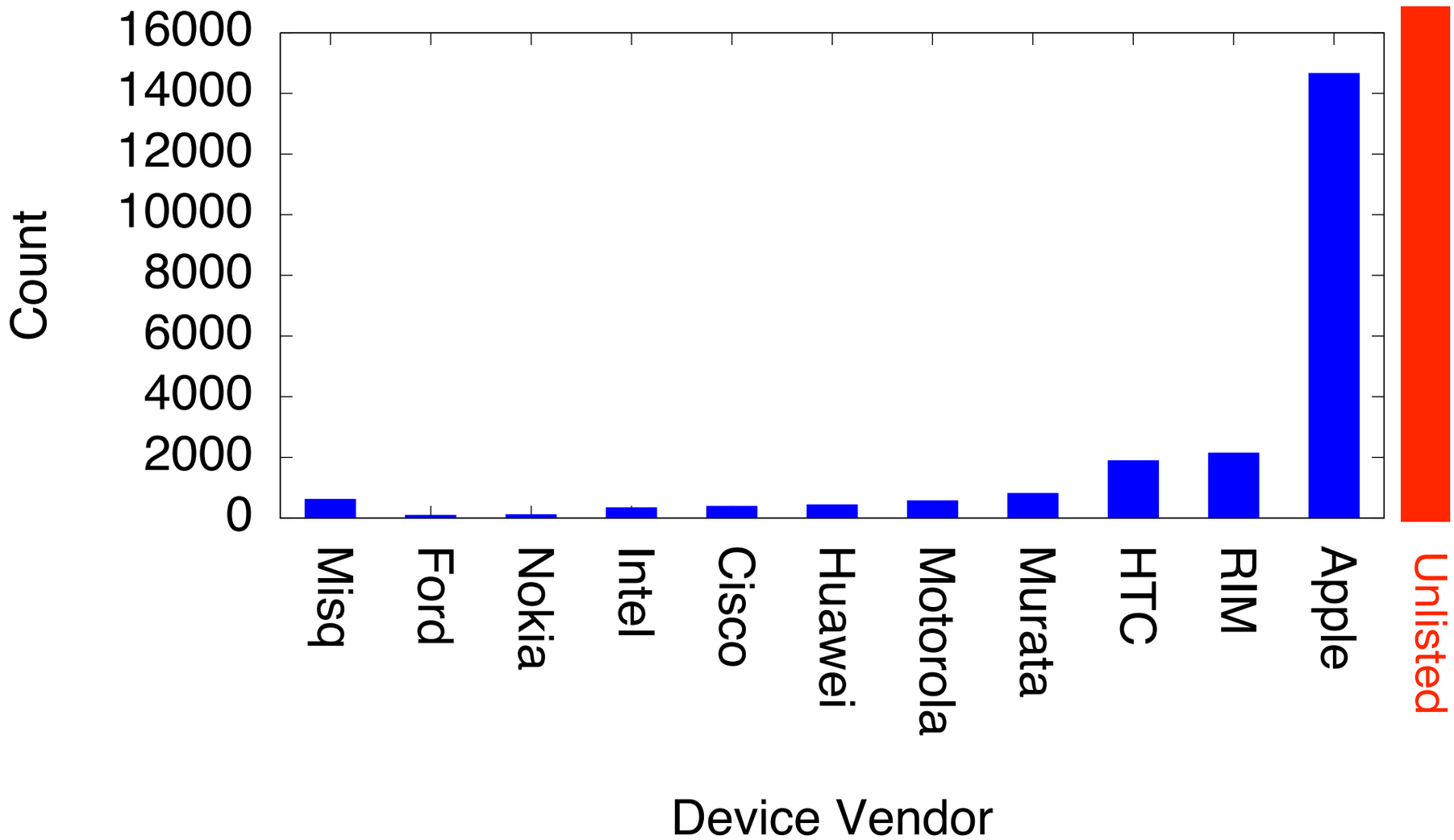
37000 ADT according to DOT

19%

A mystery for you...



A mystery for you...



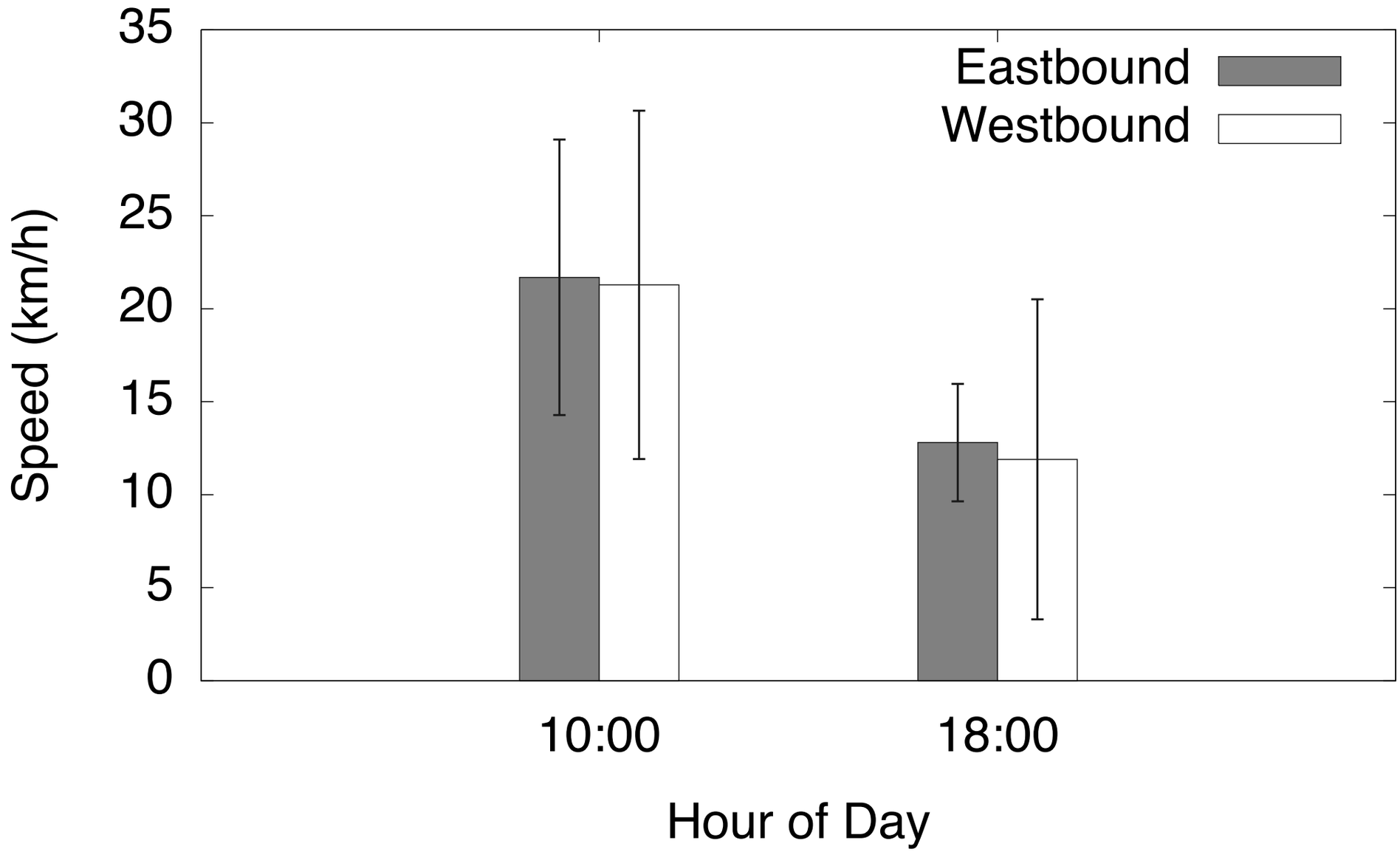
Conclusions

- Smartphone Wi-Fi is chatty and trackable
- HMM Trajectory estimation from detections
- Several probing techniques
  - Potentially increases detections
  - Certainly increases received packets
- Good tracking accuracy
  - Enables real world applications

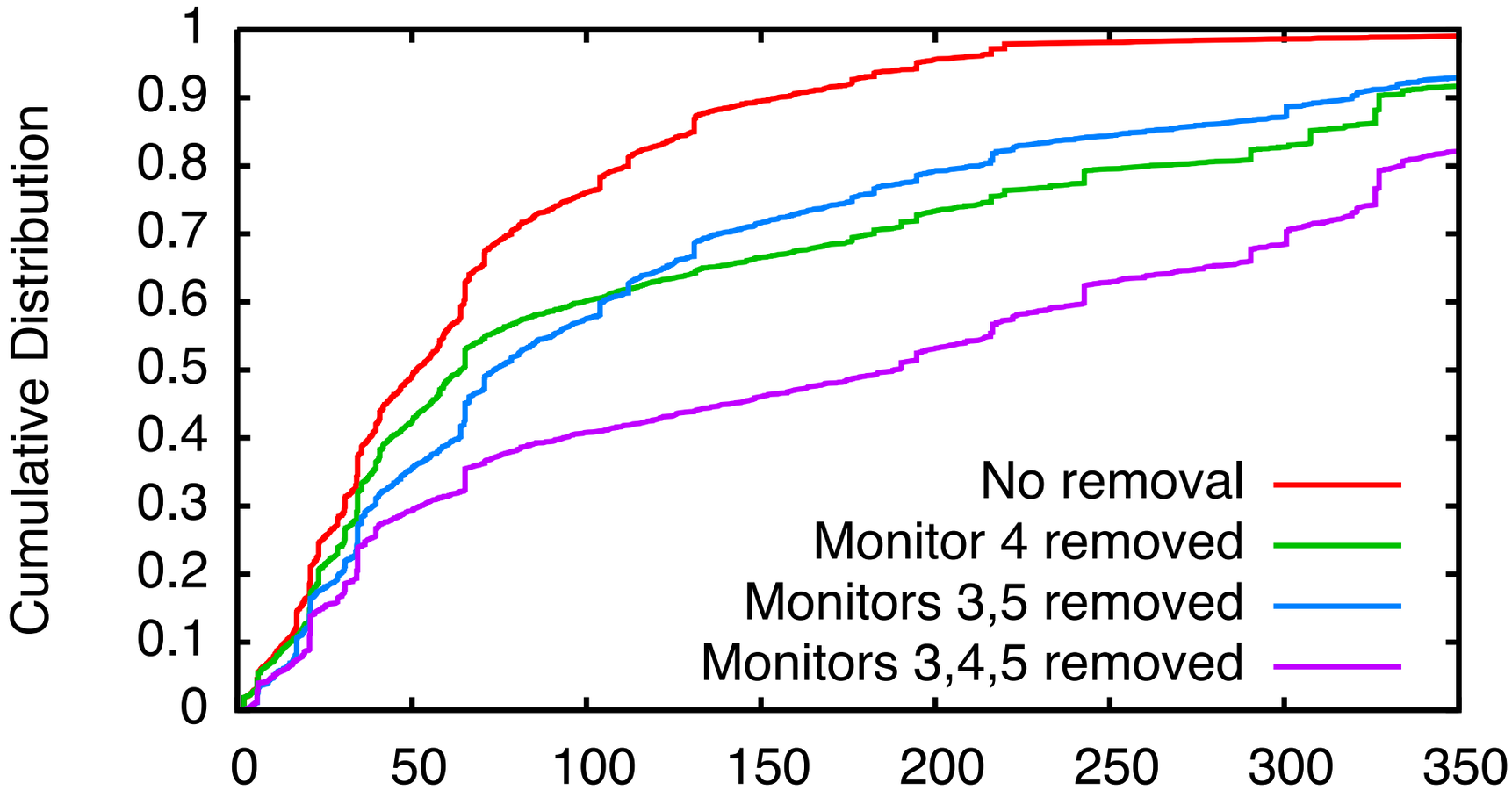
Thank you!

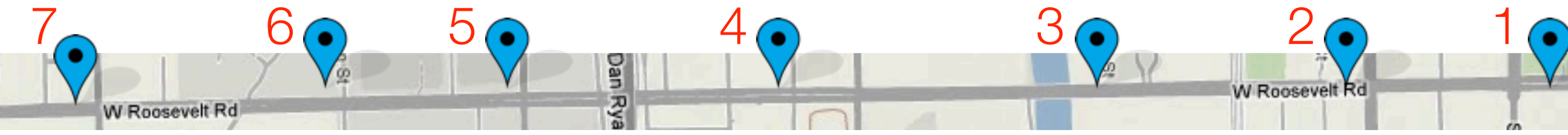
Questions?

Speed estimate example

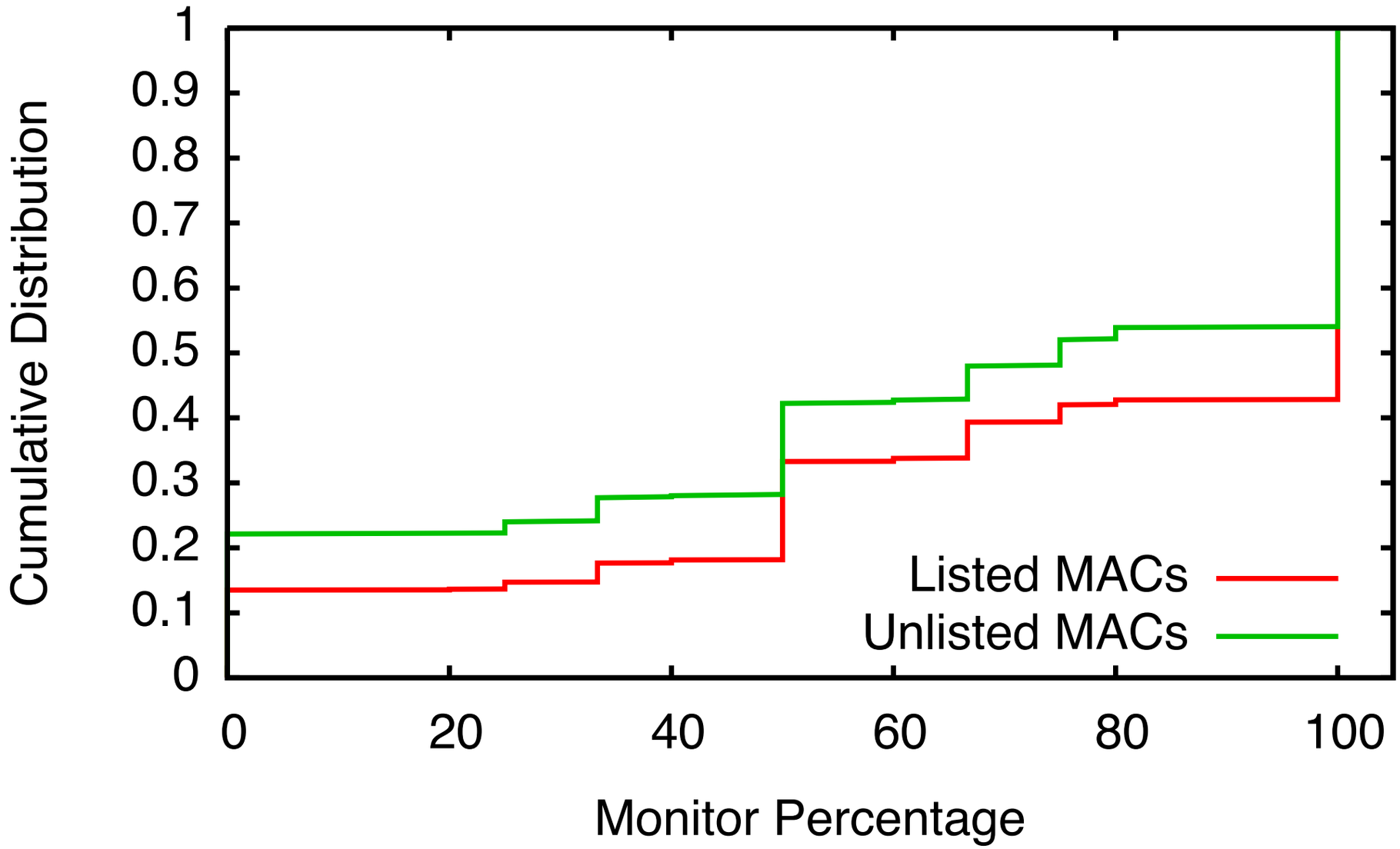


Graceful degradation





Unlisted MACs



Opportunistic AP emulation