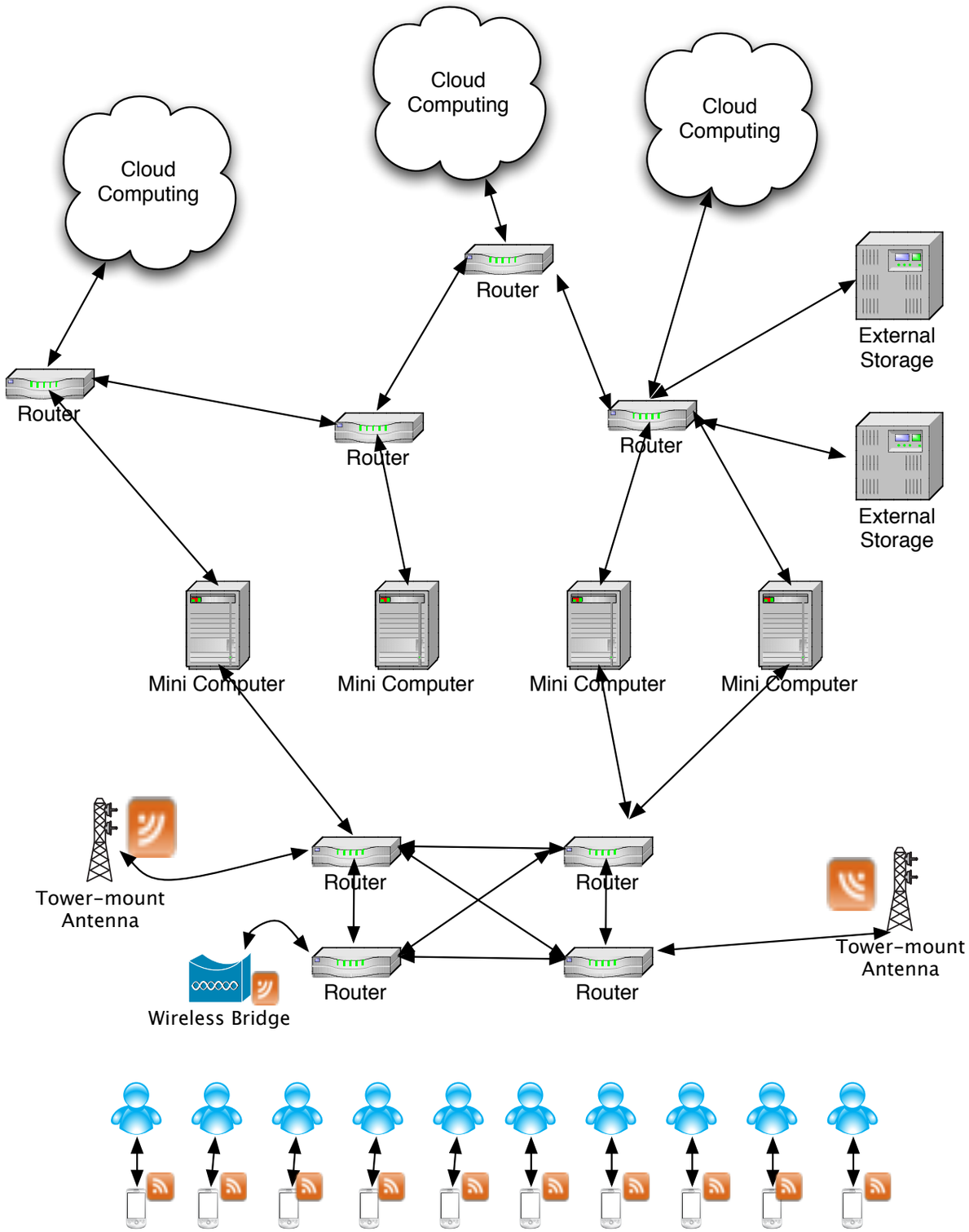
Secure Cloud Computing With Brokered Trusted Sensor Networks

Profs. Steven Myers, Apu Kapadia, XiaoFeng Wang and Geoffrey Fox

School of Informatics and Computing
Indiana University, Bloomington

Computing & Network Model

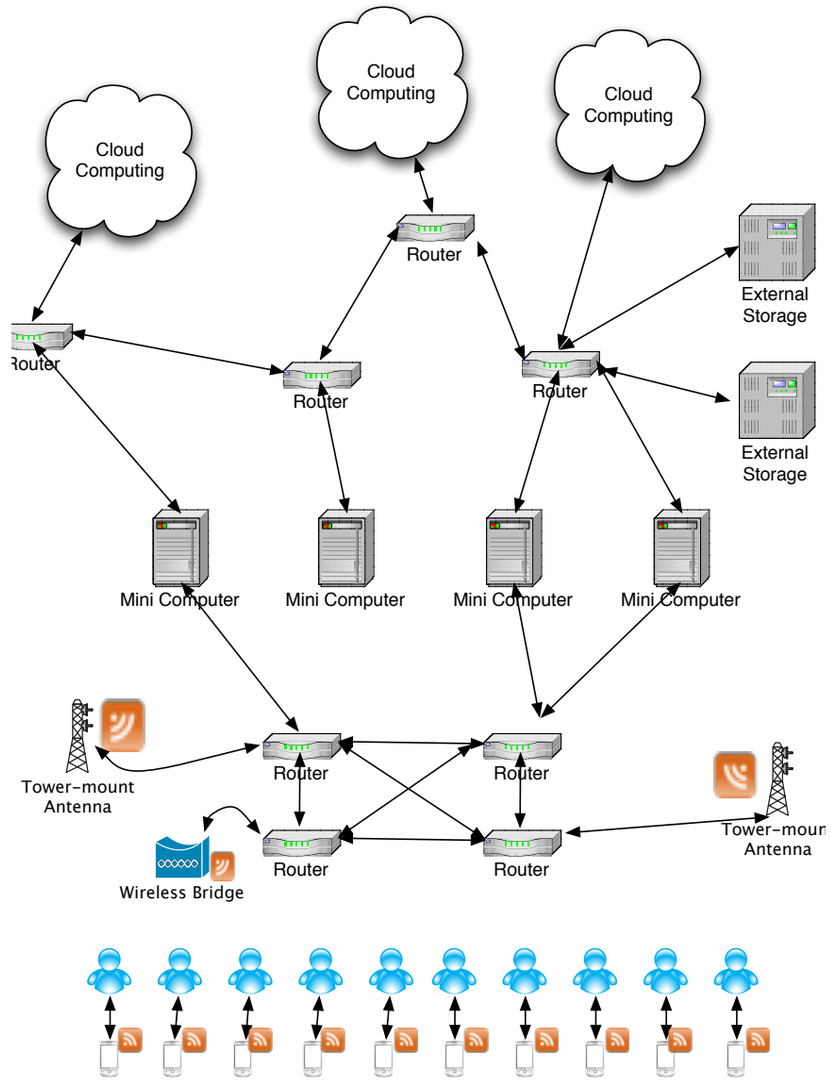


Sensor Model: (Not a Mote)

- Android G1 Development Phone.
- Version 1.6 Android OS
- Sensors
  - WiFi 802.11b/g
  - Bluetooth
  - Temperature/Thermometer
  - Accelerometer
  - GPS
  - Touch Screen
  - Camera (3.1 MP)
  - Audio
- QualComm 7201 528MHZ
- 64MB Ram
- MicroSD Slow Storage
- Currently NO SIM CHIPS

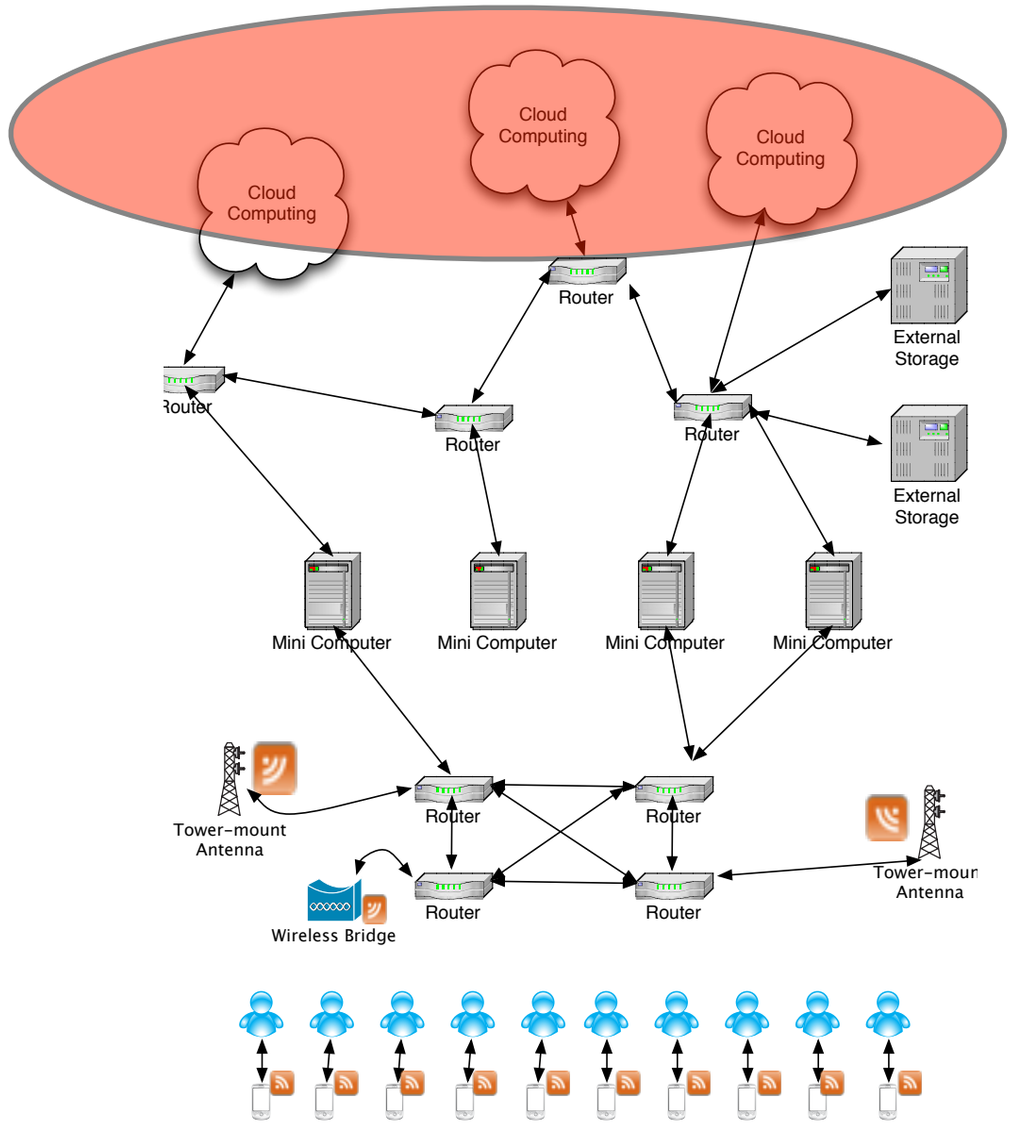
Security Threats

1. Cloud or Grid
2. Communication Channels
3. Client
4. Sensor
5. Environment



Security Threats

1. Cloud or Grid
    1. Information Theft
    2. Malware
    3. Covert Channels (shared CPU/ Resrouces)
    4. Proof of Computation?



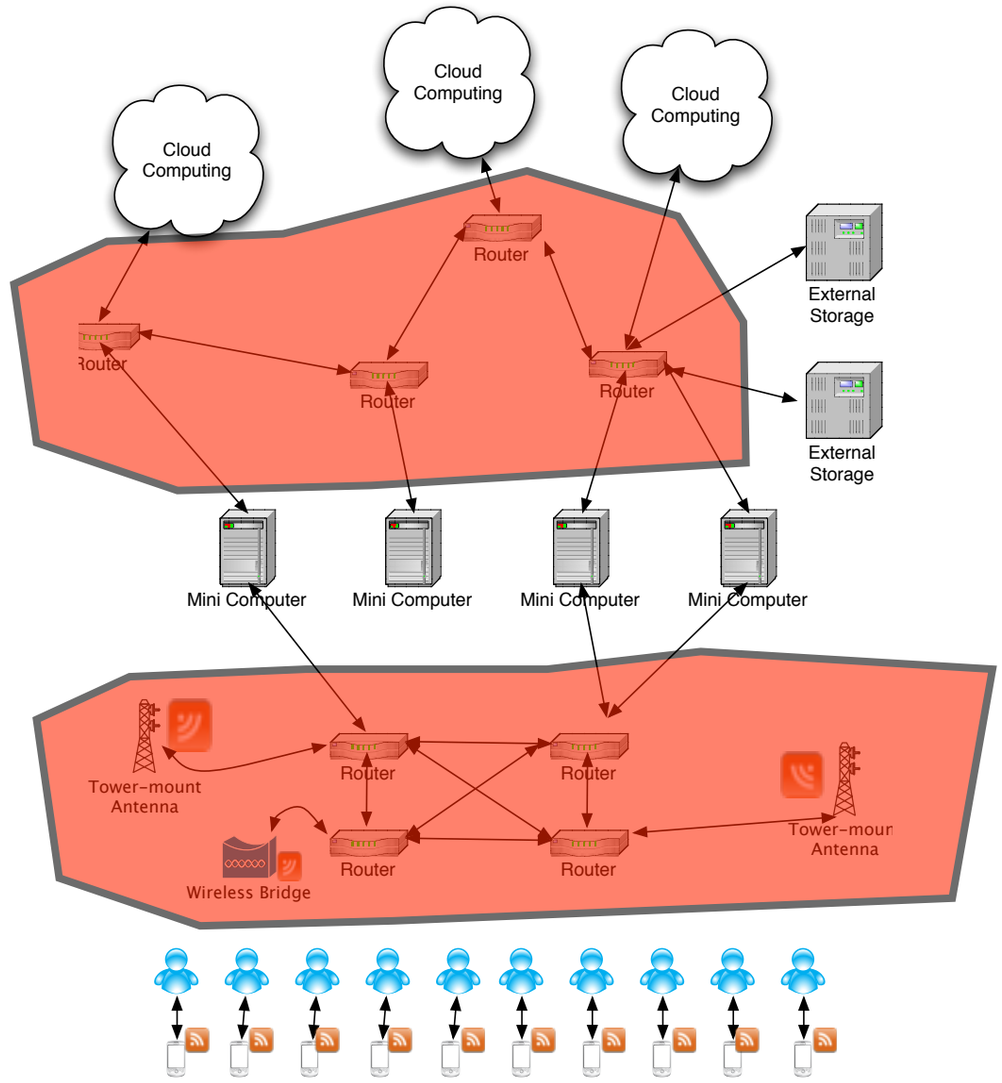
Security Threats

2. Communication Channels

    1. Eavesdropping

    2. Manipulation of packets

    3. Denial/Delay Of Service

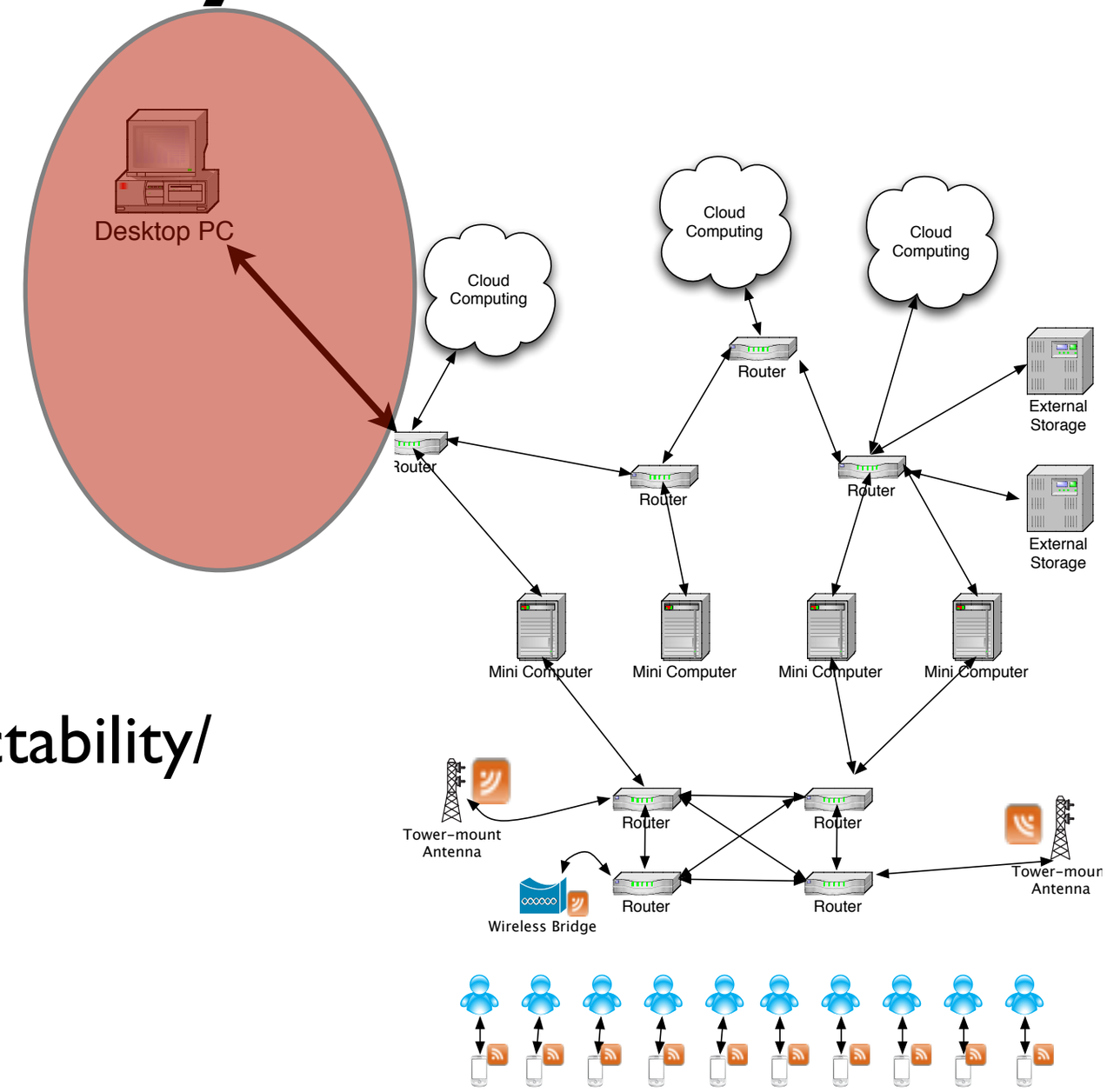


Security Threats

3. Client

    1. Malware

    2. Human Predictability/ Fallibility



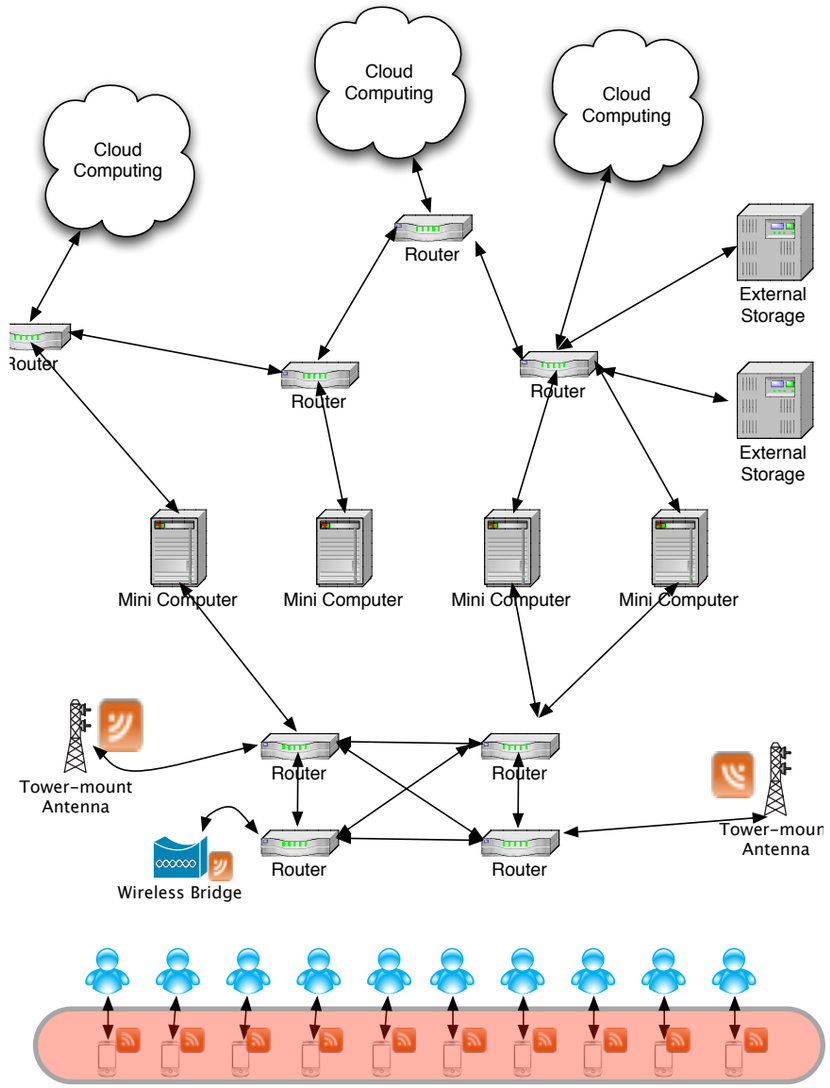
Security Threats

4. Sensor

    1. Malware/Viruses

    2. Sensor data lost or stolen

    3. Human Predictability/ Fallibility

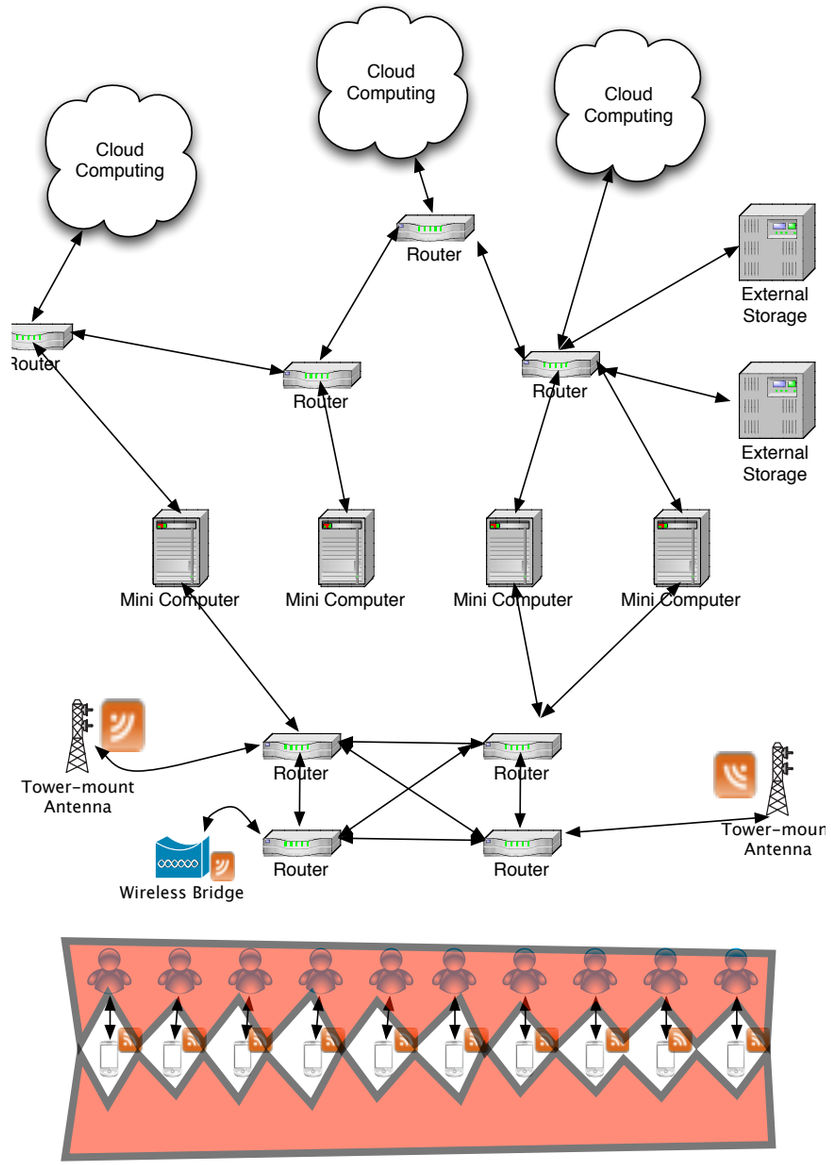


Security Threats

5. Environment

    1. Sensor stolen or repositioned

    2. Environment modified to provide artificial sensor readings



Protecting Sensors From Environment

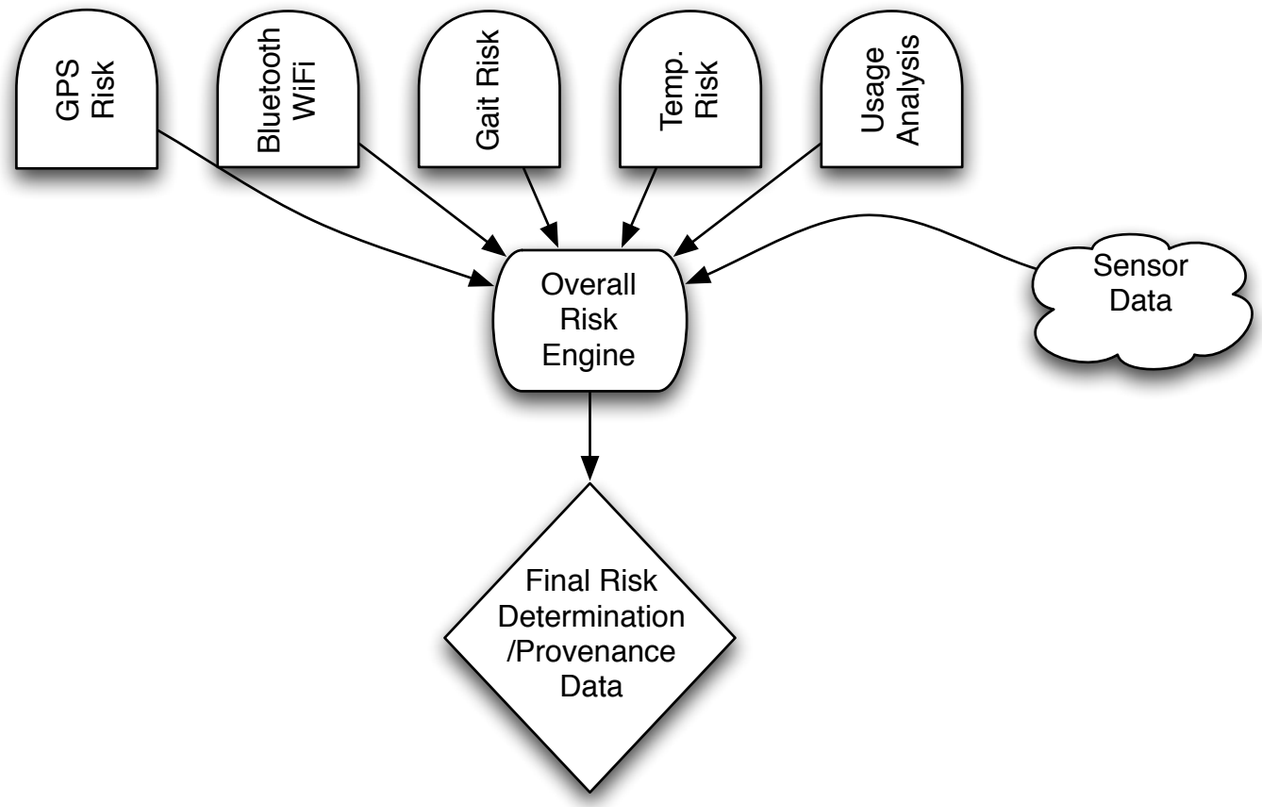
Goal: Prevent/Detect Theft or Movement of Sensors

Idea: Use Sensor Information to Determine Risk that Phone is misplaced/stolen

Examples

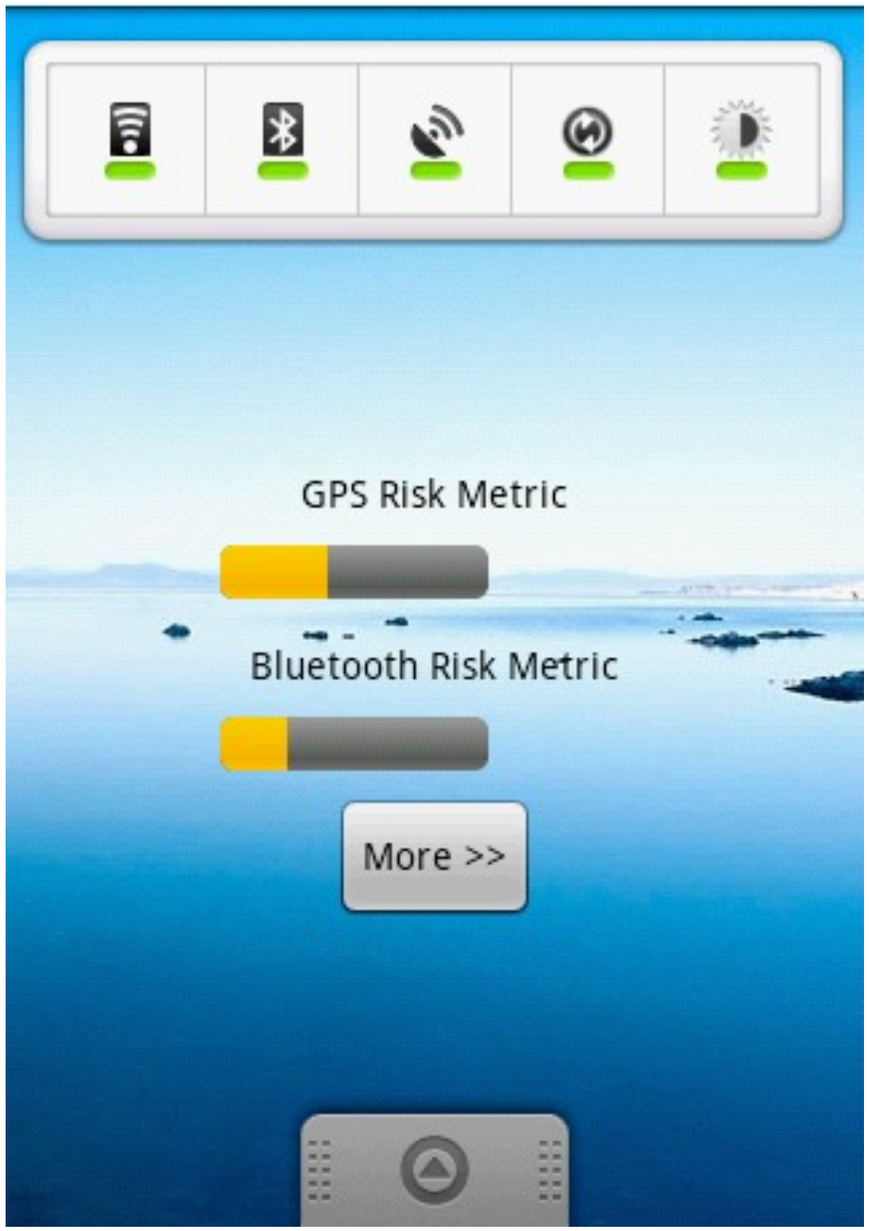
- If I have my phone in my office at 3pm vs 3am, what are the risks?
- If my phone knows my wife's phone and my earpiece are present, what are the chances of theft?
- If the phone is in motion and gate of walker is equivalent to owners, what are the risks?
- Phone was authenticated to, and been in constant use since then.

Architecture

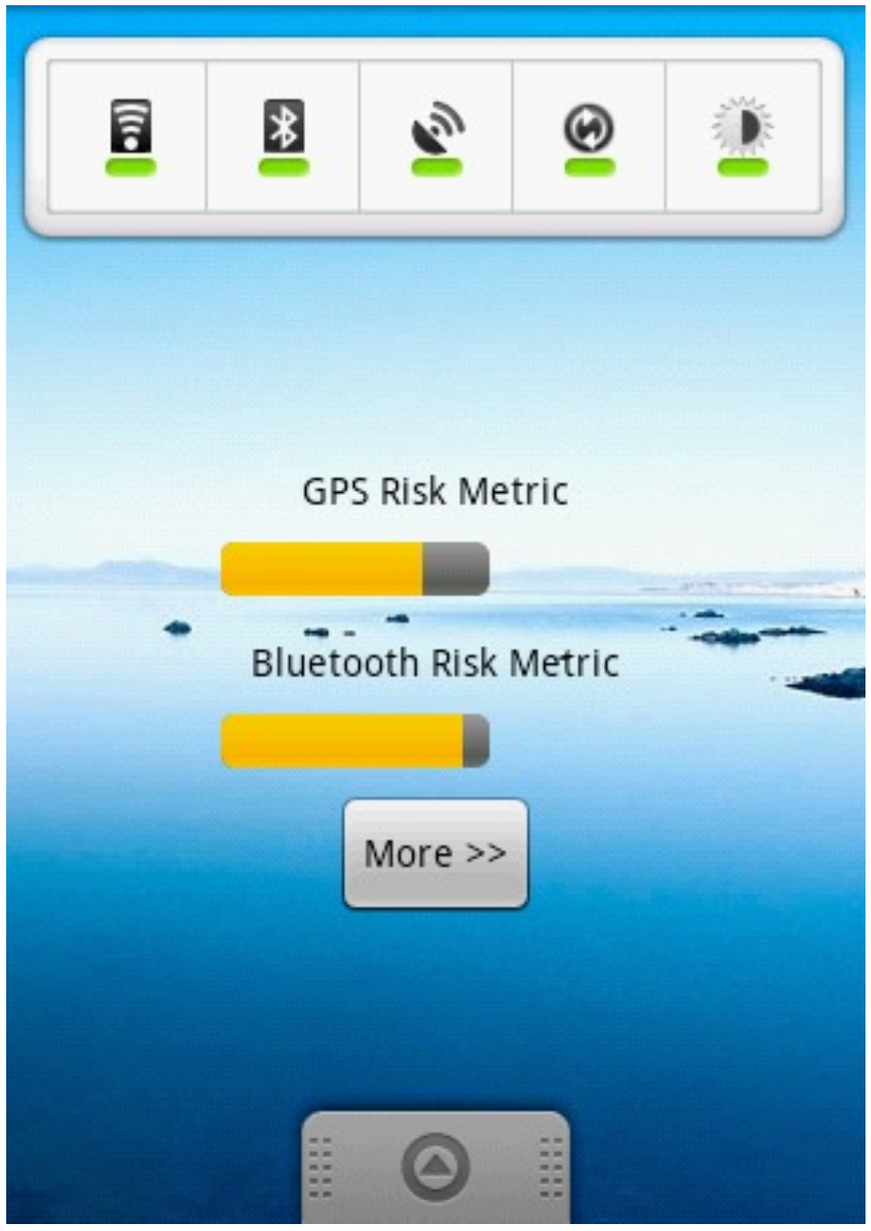


- If final risk is low sensor data reported as is, possibly with Provenance Data.
- If risk is high, force authentication of phone before reporting data or mark with high-risk provenance data.

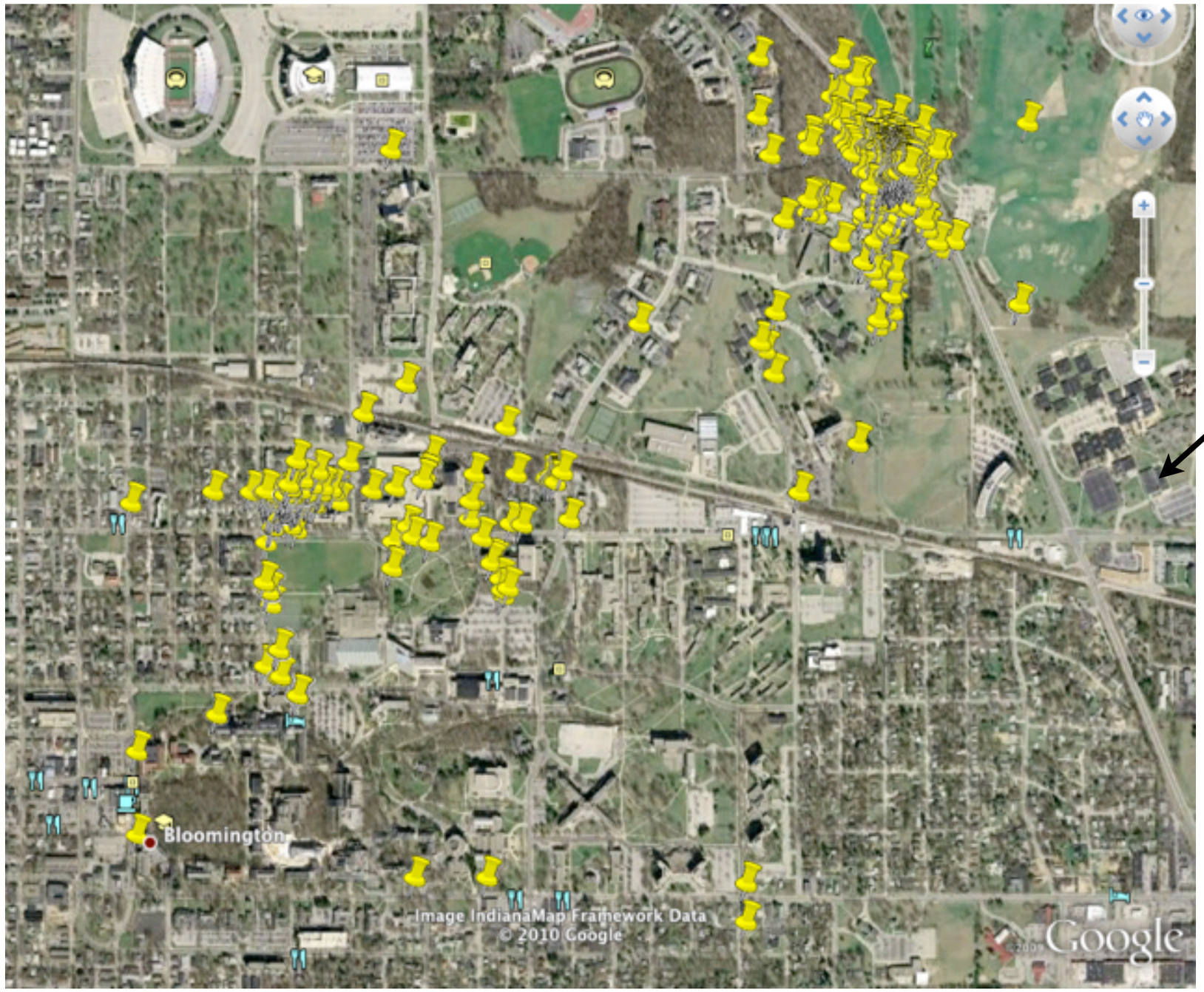
Widget showing low risk



Widget showing high risk

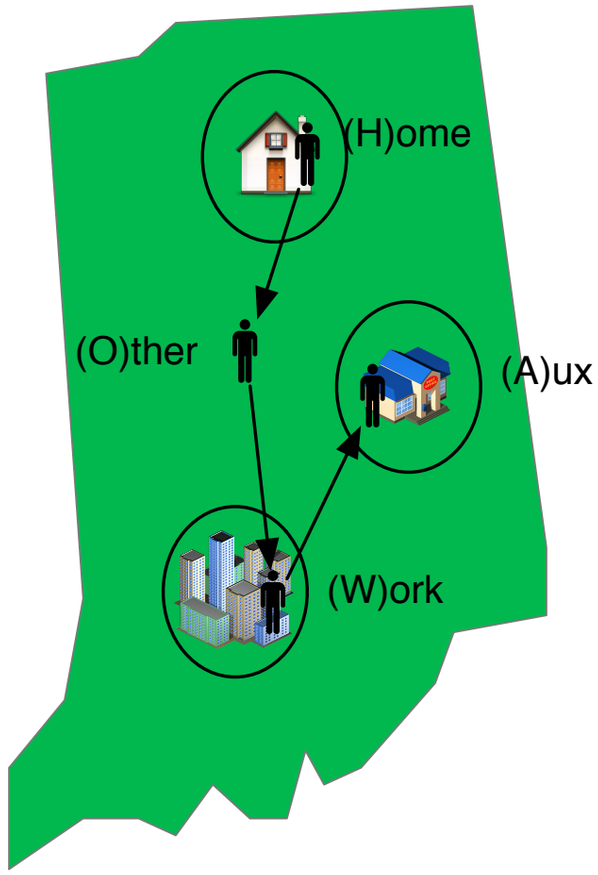


GPS Sensor Risk



You are here

Record Phone's Posn.



Location recorded every 30-Min. for 24 Hrs. producing the string

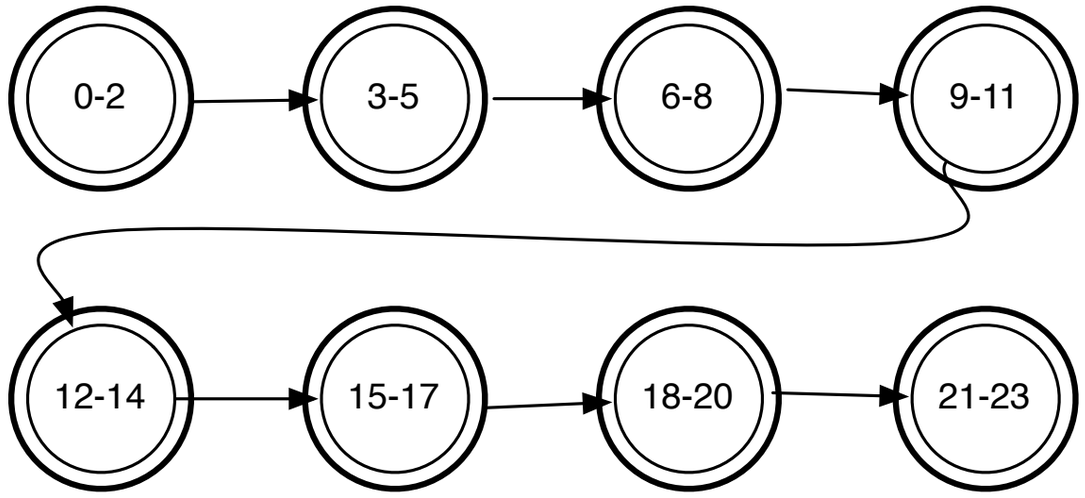
HOWAAA.....

String is parses starting on each letter into triplets for 3rd order HMM

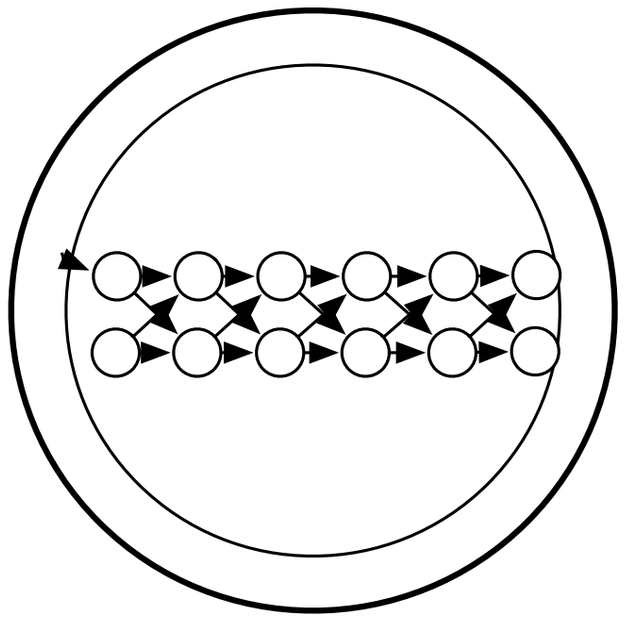
H O W	O W A	W A A	W A A	A A A

O O O O O

Convert to common location string for HMM Learning



A hierarchical HMM model is used to learn users schedules. At the outer layer we in essence have a node for each 3 hour block of time in the day.

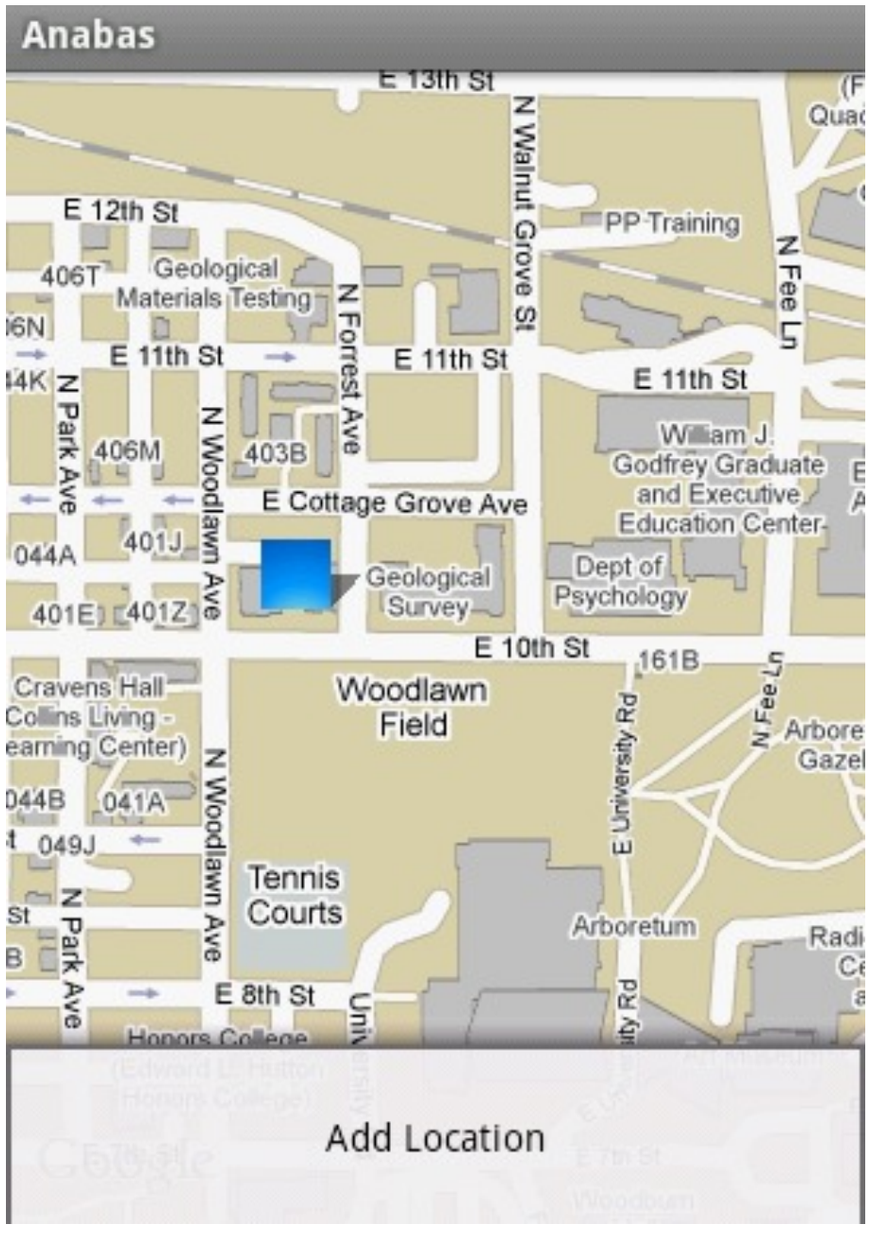


Each node contains within it a 3rd order multi-state HMM to learn the schedule over the corresponding hours.

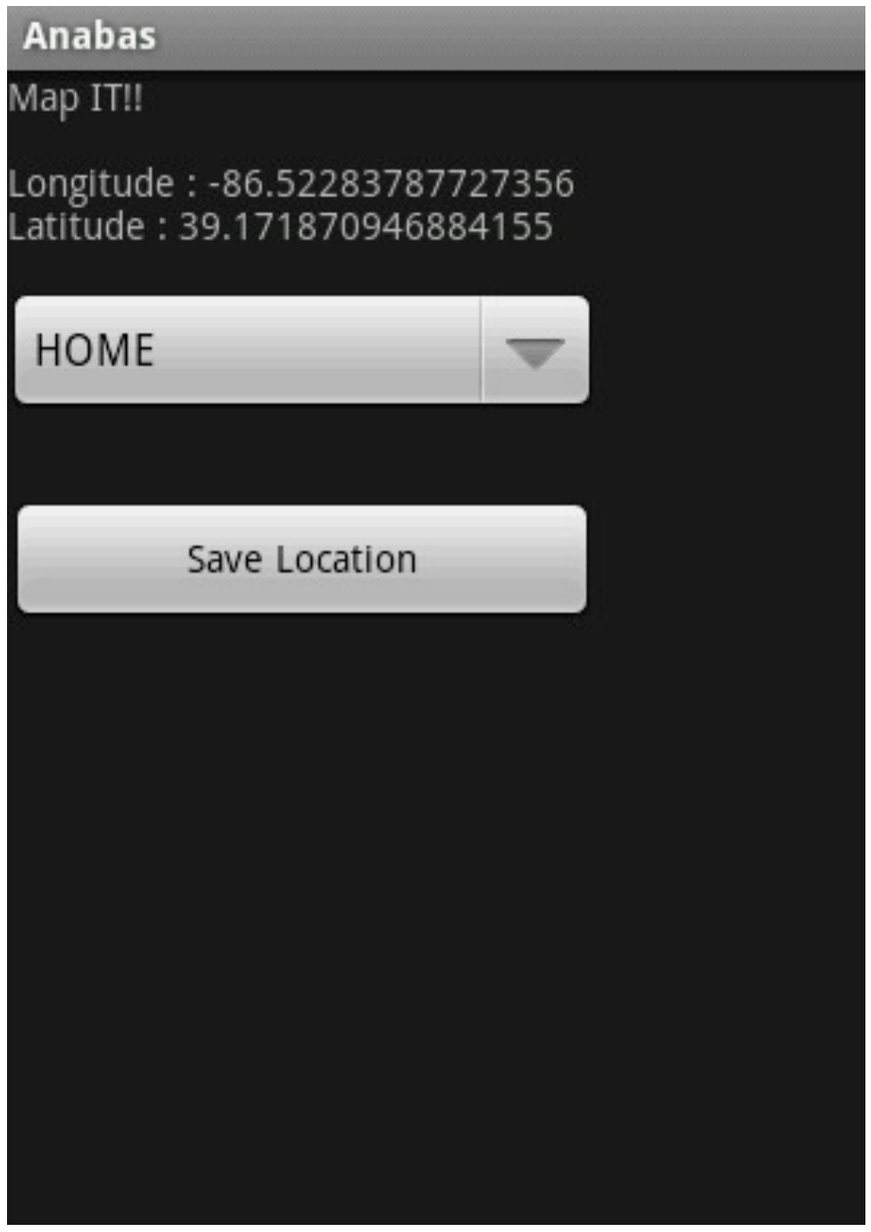
Tradeoff Learning Accuracy vs. Runtime Costs

On clicking Map It! (integrated with GoogleMaps)

Clicking “menu” will give an option to add the location

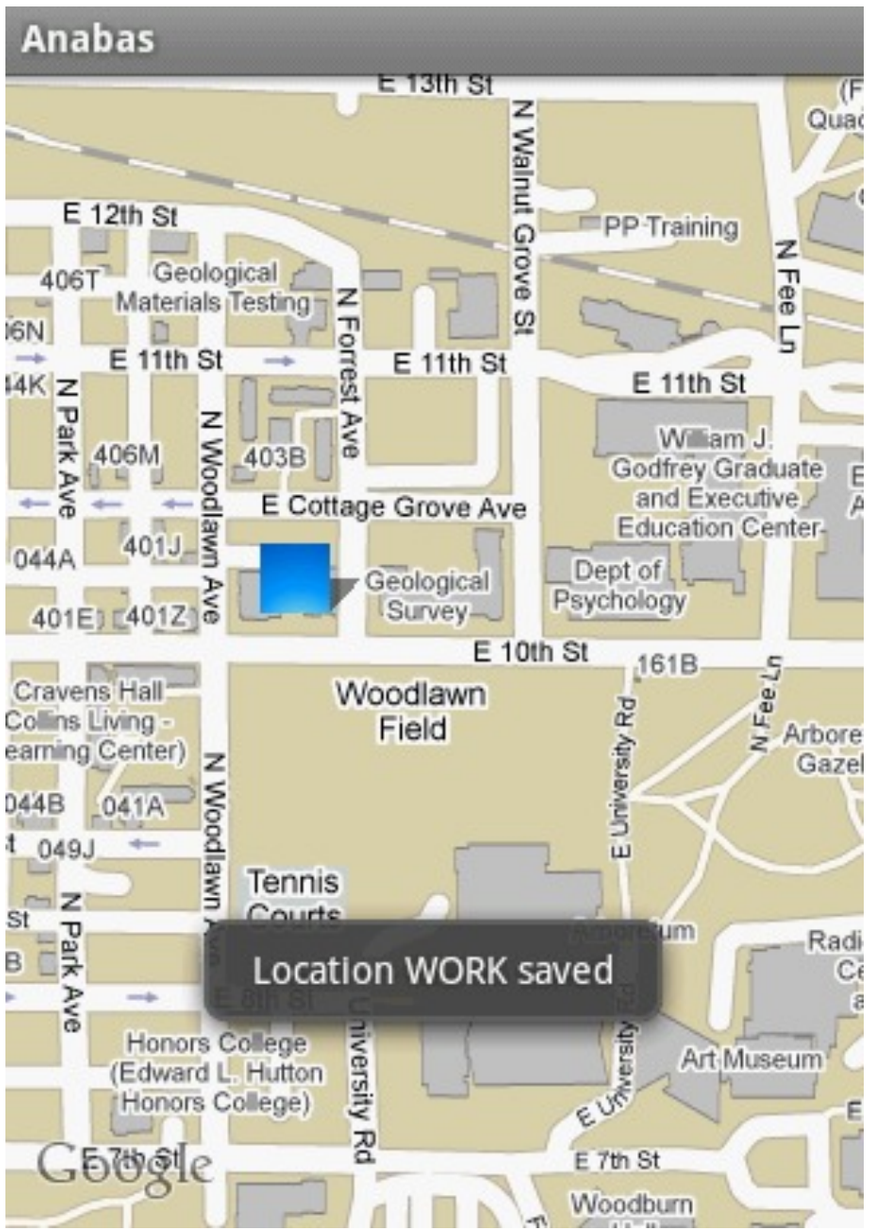


On Clicking “Add Location”



You can select Home, Work, etc

On clicking save, gives you a confirmation

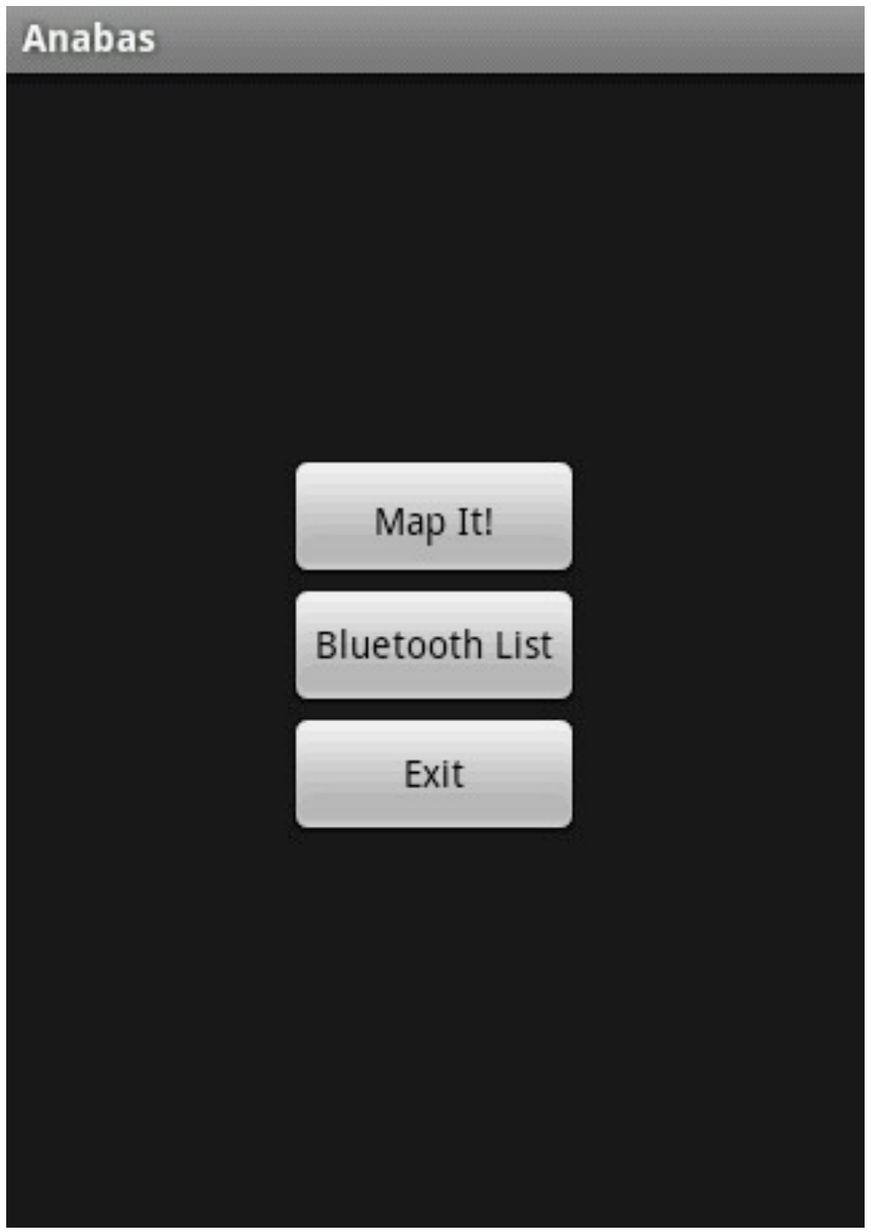


Bluetooth Sensor Risk

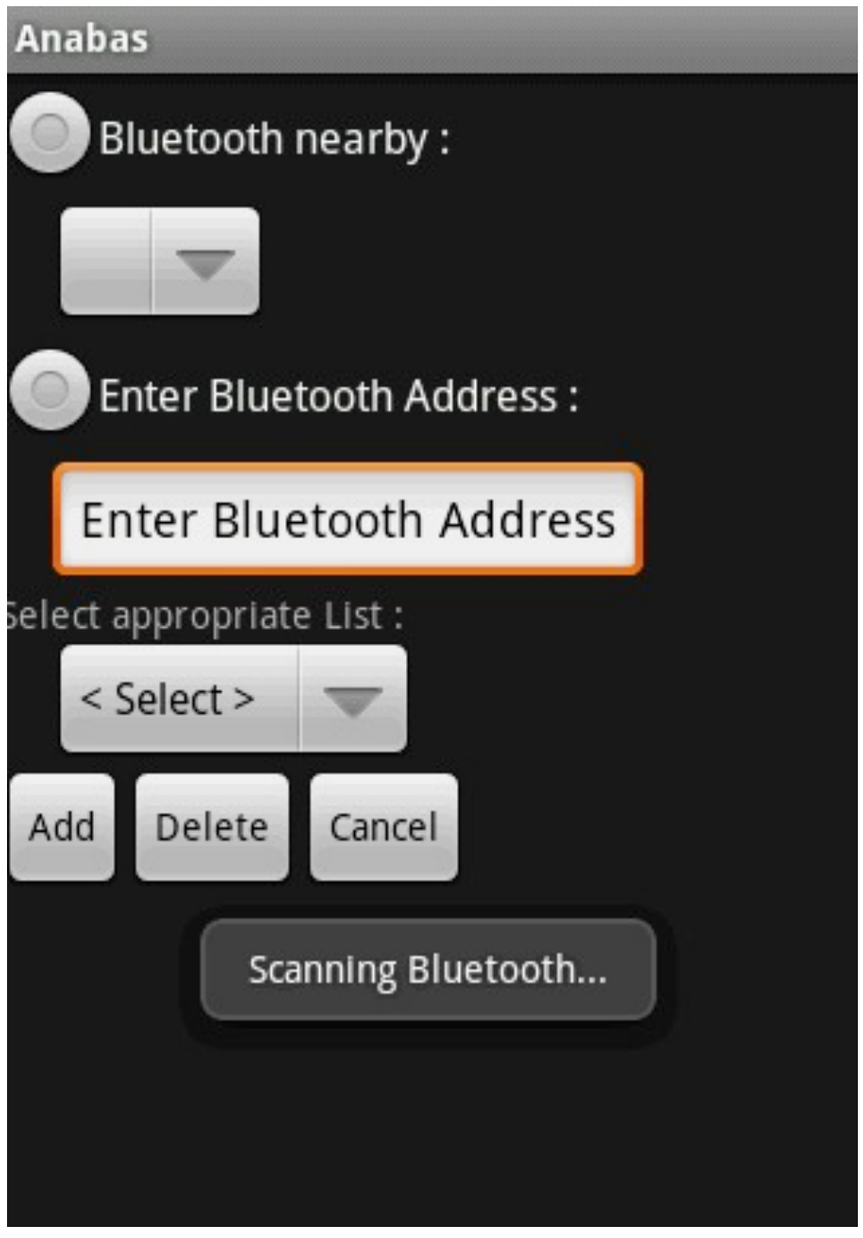
Bluetooth Risk Idea

- Proximity of certain devices suggest low risk (Wife's phone, my bluetooth earpiece, laptop, PS3, etc....)
- Proximity of certain devices suggest high risk (Enemy's phone, competitor's phone, device which has only questionable purposes)

Selection Menu



Bluetooth Menu



Scans and shows bluetooth currently around

Select appropriate list to add the bluetooth into

On Clicking “More >>” on the widget

Going Forward

- Calibrating Individual Sensor Risk
- Overall Risk Engine Structure (right now, simple expectation calc.)
- Other Sensors (phone call surfing patterns, accelerometer gait analysis).