Attestation

Center for Embedded Networked Sensing

Jonathan Yang

Urban Sensing

- Utilizes software and network technology to enable mobile devices such as smart phones to act as credible sensors in environments.
- Smartphones gather sample data with sensor and send to database. Data can be used for various studies.
- Example: Sound level mapping campaign for LA
  - Phones gather data samples, which include decibel level of sound. Samples are kept in database.
  - Helpful towards urban planners and developers.
  - Helpful for monitoring quality of life in city

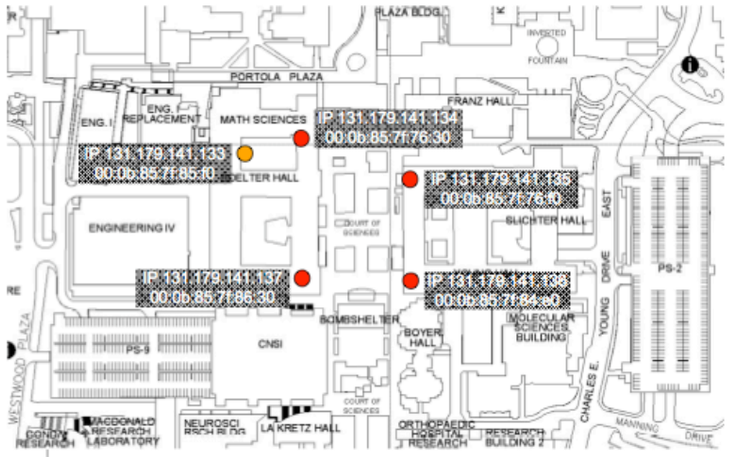
Attestation Concept

- Location credibility equally as important as gatherer's identity.
- Phones use GPS to measure location.
- Data from phone is sent to database via Wi-Fi.
- GPS location of the access points are known.
- Attestation is the network ability to attest to the location measured by the phone is within a certain radius from the access point location.
  - Used as an added layer of correctness and credibility.
  - Not designed to prevent hackers.

Network Infrastructure

- Two identical wireless mesh networks on UCLA campus.
- Each mesh has a root access point which is wired to the router.
- Network hardware donated by Cisco.
  - Devices use proprietary protocols for communication.
- Key network software
  - Campaignr : Application on the smart phones that gathers sensor data. Sends packets to database via Wi-Fi.
  - Perff : Database which collects sensor data for the various campaigns.

Network Map



CENS

CENS IP INFO
Static Network:
131.179.140.64
255.255.255.192
APs:
131.179.141.133-137
DHCP Network:
131.179.141.128
255.255.255.128
DHCP Client Pool:
131.179.141.138 -254

3845 GW
131.179.140.6
VLAN
141.129
remap--cens
140.6
SMF
3551B Boelter – 1473 Melnitz

WLC
131.179.141.130 (Mgmt)
131.179.141.131 (AP Mgr)

Location Appliance
131.179.141.132

Future
Urban Sens. Proxy /FW
Future

CENS
144, 148

CS Border

REMAP

REMAP IP INFO
Static Network:
131.179.140.0
255.255.255.192
APs:
131.179.141.5-10
DHCP Network:
131.179.141.0
255.255.255.128
DHCP Client Pool:
131.179.141.11-120

140.x
DNS, WCS
131.179.141.5:8443
WLC
131.179.141.2 (Mgmt)
131.179.141.3 (AP Mgr)
Location Appliance
131.179.141.4

VLAN
141.1
cens--remap
140.5
3845 Router
140.1
tft--remap

MMF Melnitz Rm 1473-1469B
1471-1427 – E Melnitz 116-211-11

remap--tft
140.2
Nortel
E.Melnitz

UCLA Backbone

Internet

Portable

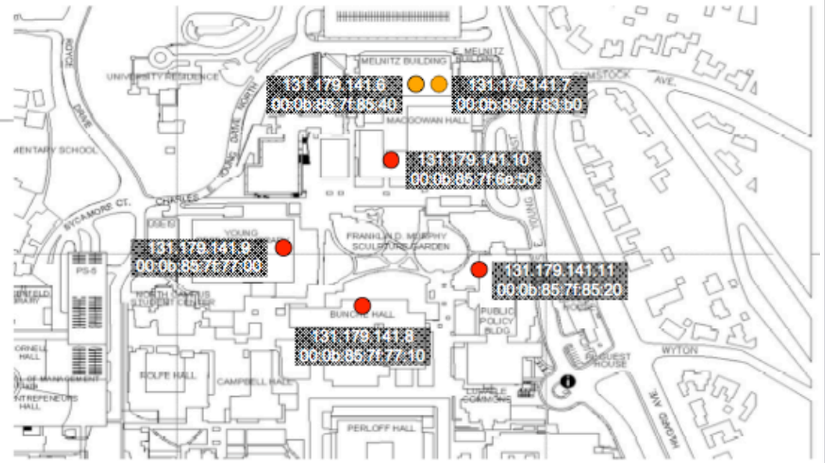
Future

APs: 140.x
Mobile Nodes: 141.x & 142.x

3845 Router

Location Appliance
131.179.142.x

WLC
131.179.142.x (Mgmt)
131.179.142.x (AP Mgr)



DSL
62.121.238.243

CENIC

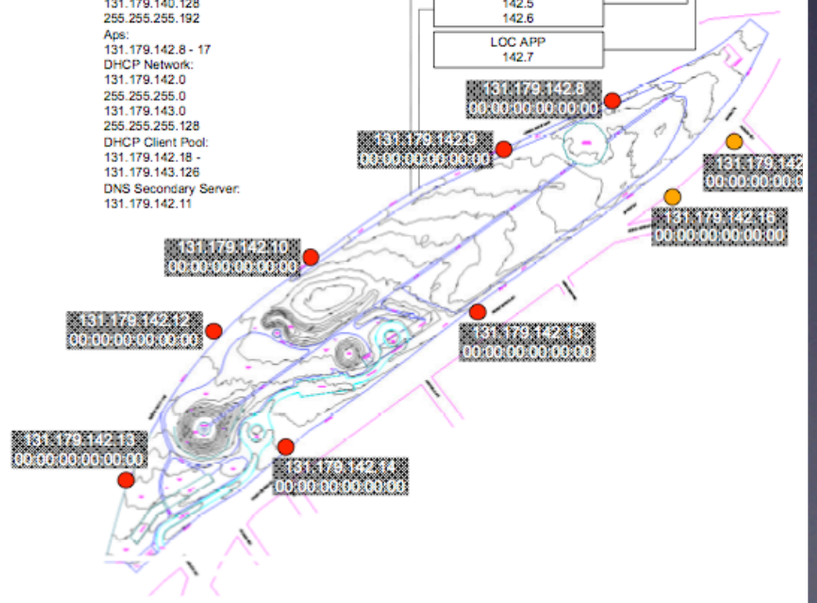
DS3 (provided by Qwest)

3845 GW
62.121.238.243
255.255.255.248
VLAN
142.1 wifi--las

IP WCS (Ox) 142.11, DNS
IP WLC 142.2 142.3 (AP Mgr)
IP Location Appliance 142.4
WLC 142.5 142.6
LOC APP 142.7

LA State Historic Park

LASHP IP INFO
Static Range:
131.179.140.128
255.255.255.192
Aps:
131.179.142.8 - 17
DHCP Network:
131.179.142.0
255.255.255.0
131.179.143.0
255.255.255.128
DHCP Client Pool:
131.179.142.18 -
131.179.143.126
DNS Secondary Server:
131.179.142.11



KEY
- Urban Sensing Net Traffic
- Site-To-Site VPN
- CS Private Traffic
- Wired Connection
- Future

MetWi Network Diagram

metwi.ucla.edu
SSID: MetWi

MetWi IP Space:	131.179.140.0/22 (metwi.ucla.edu)
Static Space:	131.179.140.0/24
Reserved for router-to-router connections:	131.179.140.0/28
DHCP Space[1]:	131.179.141.0 – 131.179.143.255

1. DHCP Space is partitioned between locations. At each location, the first (~)10 addresses have static assignments to wireless management devices and access points.

Attestation Approach

- GPS location of access point is associated with AP's MAC address.
  - Linking to IP would be too volatile.
- All packets sent from Campaignr must utilize one AP to reach the database.
- Verification calculation is achievable once the MAC address of the AP used for connection is known.
- Due to link layer protocol, the MAC address of any network node is in the packet only when the packet is being transmitted through the node.

One Possibility

- The mobile device must know the MAC address of the AP in order to send the packet.
- Use Campagnr to include the MAC address into the sensor data payload.
- Reasons why this approach was not taken:
  - Very difficult to program on Symbian OS.
  - Did not want to break existing functionality in Campaignr.

Extracting the MAC Address

- Due to Cisco proprietary protocol, it was unclear to which device could see the AP MAC address in the packets.
- Port mirrored traffic from multiple devices to a separate computer.
- Used Wireshark to analyze packet data.
- Concluded that the router was the only device that could obtain the AP MAC address.

Attestation Design

- Information about packet known by Perff
  - Source and Destination IP / port
  - Packet checksum
  - Packet timestamp
- Intercept packets at router and filter relevant traffic.
- Create a separate database with information about packet known by Perff as well as the MAC address of AP used by the packet.
- Perff can find matching packet entry in this database and obtain MAC address of AP.

Herbivore

- Herbivore is a program that intercepts router traffic and creates the separate database.
- Runs on a dedicated machine with network traffic mirrored from router.
- Uses *pcap* library in C to sniff packets on the network.
- The packets have eight separate layers and desired information is located in innermost layers.
- Must parse packet one layer at a time to extract needed fields.
- As of the end of the winter quarter, application was still in development.

Acknowledgements

Deborah Estrin
Jeff Burke
Jason Ryder
Vidyut Samanta
Ryan Dorn
Richard Guy
Derek Kulinski

Questions