Imperial College London

April, 2021

Indoor Occupancy Tracking in Smart Buildings Using Passive Sniffing of Probe Requests

Published in the IEEE ICC Workshop (2016)

By Vattapparamban et.al

Outline

- Related work
- WiFi probe requests
- Experiment
- Results
- Summary

Related work (1)

- Occupancy tracking can be implemented via:
  - Video processing and camera systems
  - Occupancy sensors throughout the building
- These options require installation of new equipment,
  - Costly to deploy.
- Alternatively, we can use wireless signals to uniquely match building's occupants.
- Many proposed solutions based on existing WiFi infrastructure,
  - They require a connection between user equipment and WiFi APs
- No detailed studies that report building occupancy tracking using WiFi probe requests.

Motivation

- Buildings are among the largest consumers of electricity
- An important portion of the electricity consumption of buildings is used for heating, ventilation, and air conditioning (HVAC).
- Occupancy tracking can help in achieving significant energy savings in smart buildings
  - Dynamically scheduling HVAC activity based on real-time building occupancy levels at different areas

Related work (2) - Why Probe Requests?

- Location analytics
- Search and Rescue
- Privacy and Security

Location analytics

To improve marketing, business teams use probe request information:

- To learn how frequently and when shoppers visit a store.
- For advertisement purposes.
- To estimate required number of personnel for peak hours.

Cisco Meraki APs are used as sniffers to capture probe requests from users.

- This data is then sent into a cloud server,
- A database is generated that involves location analytics and patterns of shoppers.
- To maintain privacy, only a hashed version of the MAC address is stored in the database

Search and Rescue

- Examples:
  - A WiFi-equipped drone actively broadcasts request-to-send (RTS) frames (100 per second) to trigger transmission of probe requests from a victim WiFi device.
  - This information is then used to coarsely estimate the location of the WiFi device
- The proposed work differs because they capture the probe request for occupancy monitoring purposes.
  - Privacy is maintained in the sense that the addresses can be anonymized

Security and Privacy

- More probe requests are sent when devices are in active mode (screen on) and not connected to any network, which can be used for tracking individual users based on Received-Signal-Strength (RSS) information.
- Other studies show that the maximum probing frequency is observed to happen when a device attempts to connect to a known network in its area.
- For a commercially deployed MAC randomization mechanism, it is possible to re-identify anonymized probes
- An attacker can automatically send beacon and probe response frames for every received probe request, to direct the clients to his own network.

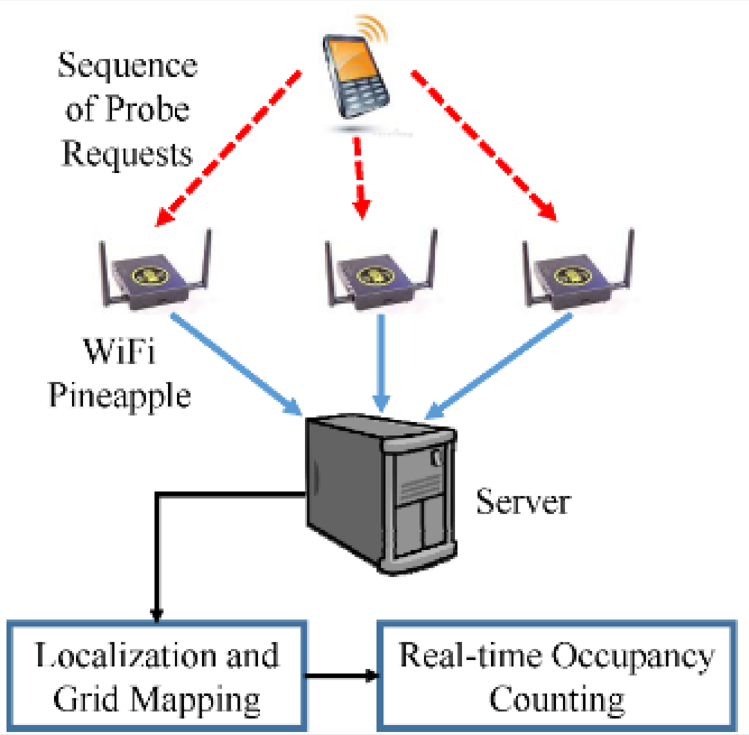
Contribution

- WiFi probe requests are used for occupancy counting and tracking
- WiFi Pineapple equipment are used for passively capturing ambient probe requests from WiFi devices
  - No connectivity to WiFi devices is required
- This information is used to localise users within coarsely defined occupancy zones

WiFi Probe Requests (1)

- Probe requests are signals that are continuously broadcast from devices with WiFi technology (e.g., smartphones, laptops).
- When a WiFi client wants to get connected to a WiFi network:
  - 1. Scan for beacon frames, which are frames broadcast by WiFi routers to tell about their presence to WiFi clients
  - 2. Send probe requests. A WiFi client itself can initiate a connection to a WiFi router instead of waiting for a beacon frame from the router.

WiFi Probe Requests (2)



- Such requests contain the unique MAC address of the device, as well its type, brand, manufacturer, and model.
- The probe requests are not encrypted, and can be passively captured and decoded with the help of wireless sniffers.

WiFi Probe Requests (3)

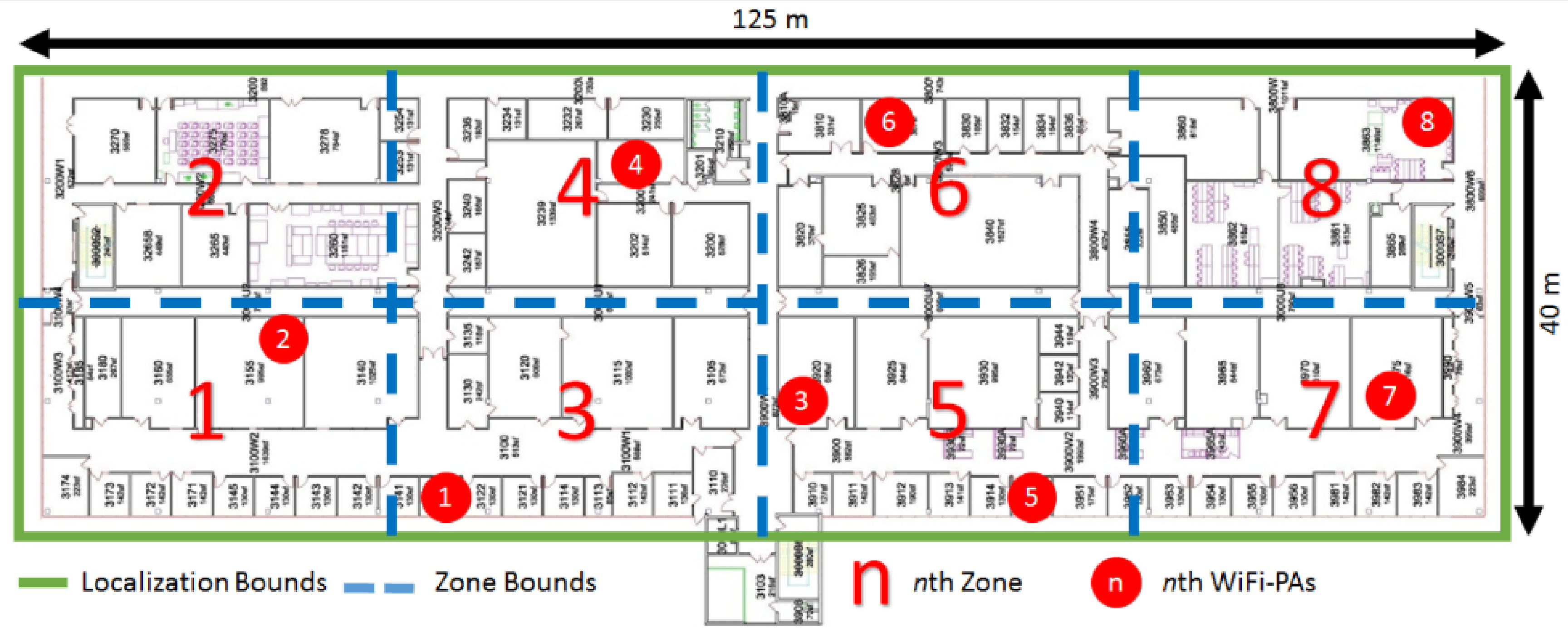
Probe requests are bursty in nature as they are broadcasted in the air in search of WiFi networks

- To get connected or
- To get a list of available networks.

Frequent transmission of probe requests introduces an opportunity to:

- Track occupancy of building by passively sniffing
- Counting probe requests

Experiment (1)



Experiment (2) - Details

- Only WiFi probe requests are captured.
  - All the other packers were filtered out
- The data captured include:
  - Time stamps providing the time at which the data were captured
  - MAC address of the WiFi enabled device
  - The signal strength of the WiFi device.
- The bursty nature of probe requests requires pre-processing of the data to make it ready for wireless location estimation.

Pre-processing (1)

- The RSS data **is resampled in time** due to its bursty nature.
  - We can have several probe requests from the same user within few hundred milliseconds, followed by a silent period that may last several seconds.
- To have uniformly sampled RSS captures, we **average the received RSS values** within one second intervals.

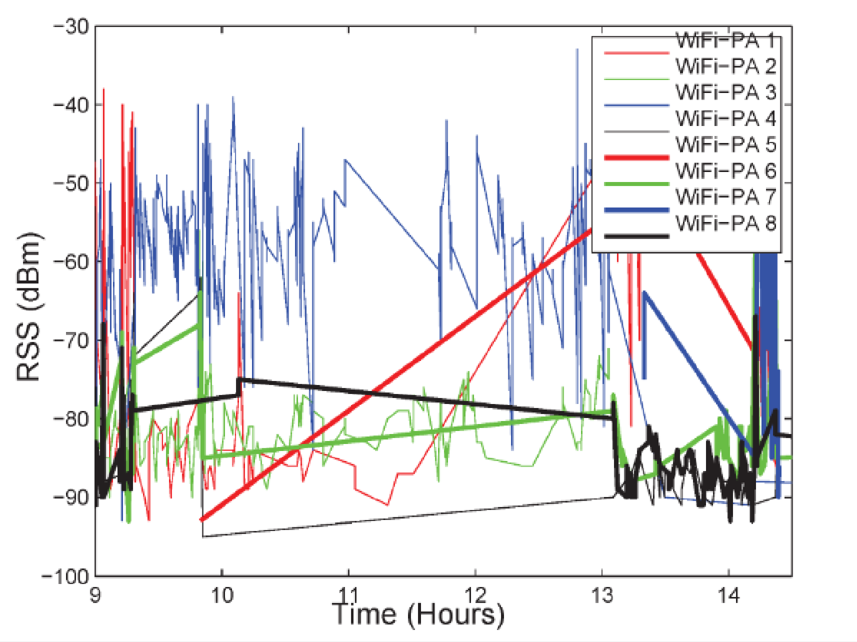
Pre-processing (2)

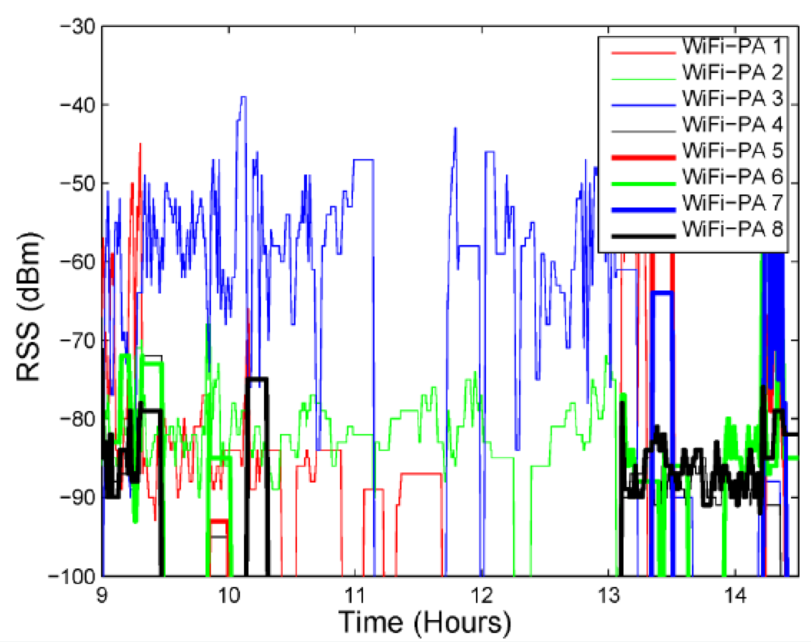
- The **interpolation stage involves** a sample-and-hold filter.
- This keeps the probe requests RSS value at a certain WiFi-PA for a fixed time window.
  - If **a new probe request is received**, the **RSS value is updated** with the information obtained from that probe request.
  - If **no probe request is received** within 300 seconds, **the value** of the RSS from that particular MAC address **is labelled as unavailable.**

Imperial College London

Raw measurement vs Processed data

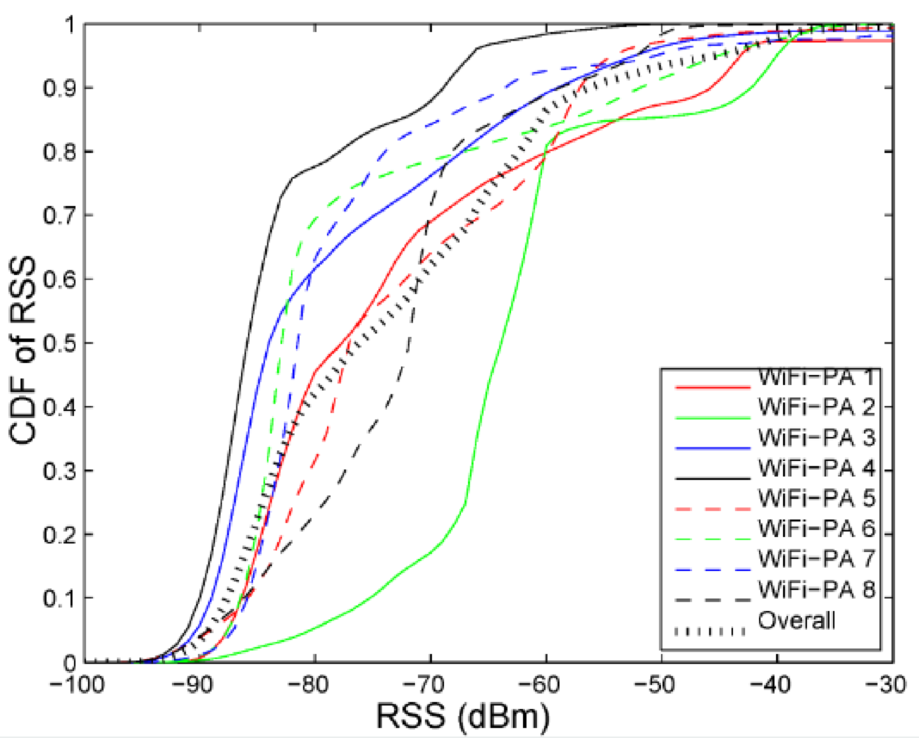
- Raw measurements (left) vs processed data (right) of RSS.





Cumulative distributions of RSS

- RSS values smaller than -100dBm or larger than -30dBm is regarded as outliers



Device Localization (1)

- **True distance** between the user and the i*th* reference node is given by:

$$d_i = \sqrt{(x_0 - x_i)^2 + (y_0 - y_i)^2}, \qquad (1)$$

- The **path-loss model** for the RSS is given by:

$$P_r = P_0 - 10n \log_{10}(d/l_0) + X_\sigma, \qquad (2)$$

- The **distance** between transmitter and i*th* WiFi – PA is estimated as:

$$\hat{d}_i = 10^{(P_0 - r_i)/10n}. \qquad (3)$$

Device Localization (2)

- Subtracting all approximations of RSS from different WiFi – PAs, we obtain:

$$\underbrace{\begin{bmatrix} -x_1^2 - y_1^2 + x_k^2 + y_k^2 \\ -x_2^2 - y_2^2 + x_k^2 + y_k^2 \\ \cdots \\ -x_{k-1}^2 - y_{k-1}^2 + x_k^2 + y_k^2 \end{bmatrix}}_{\mathbf{y}} =$$

$$\underbrace{\begin{bmatrix} -2x_1 + 2x_k & -2y_1 + 2y_k & \frac{a_1(r_1 - r_k)}{5} \\ -2x_2 + 2x_k & -2y_2 + 2y_k & \frac{a_1(r_2 - r_k)}{5} \\ & \cdots & \\ -2x_{k-1} + 2x_k & -2y_{k-1} + 2y_k & \frac{a_1(r_{k-1} - r_k)}{5} \end{bmatrix}}_{\mathbf{H}} \underbrace{\begin{bmatrix} x_0 \\ y_0 \\ \frac{1}{n} \end{bmatrix}}_{\mathbf{x}} \qquad (5)$$

where $k \geq 4$, and the k-th WiFi-PA is selected as reference for linearization. The final solution for $(x_0, y_0, \frac{1}{n})$ is given by:

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{y}. \qquad (6)$$

Real Time Occupancy Tracking

- At every second:
  - A linear least squares technique is used to obtain location estimates of each WiFi user.
  - They are further refined using a weighted k-nearest neighbour (WKNN) location tracking algorithm.
  - The final estimate is mapped to the nearest zone point with distance threshold.

Occupancy Tracking – Results (1)

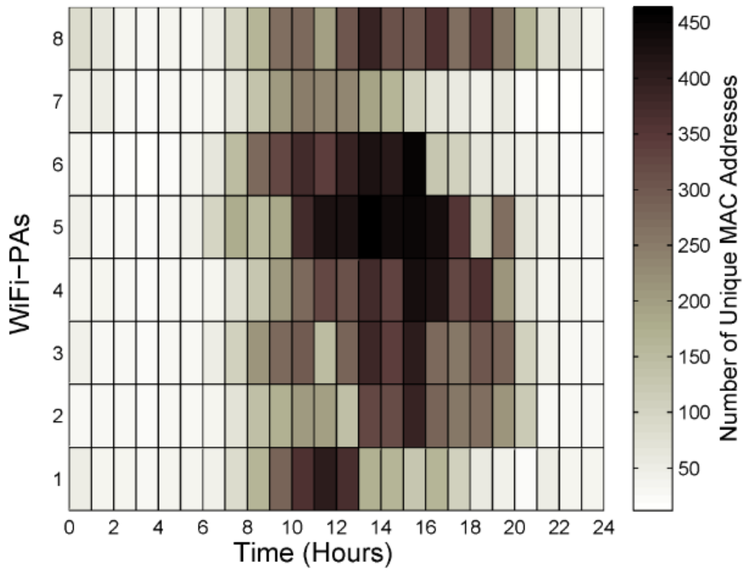


Fig. 6: Number of probe requests captured from each WiFi-PA.

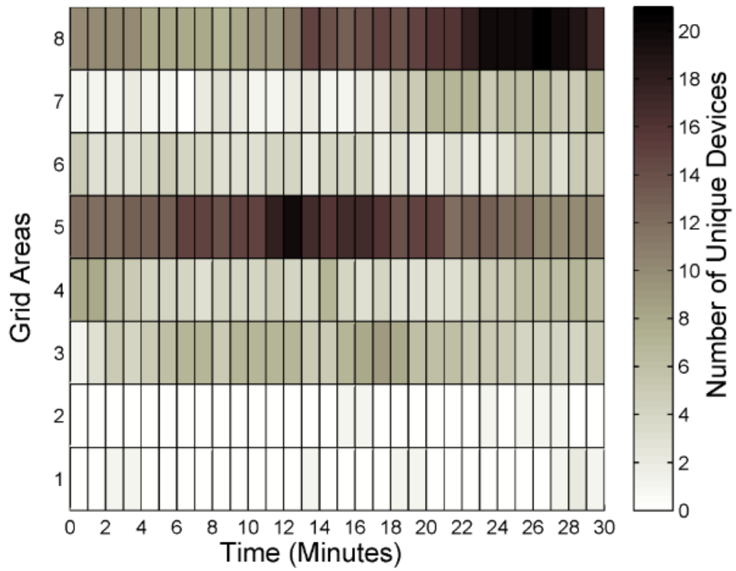


Fig. 8: Number of total people in gridded areas between 12 PM to 12:30 PM.

Imperial College London

Occupancy Tracking – Results (2)

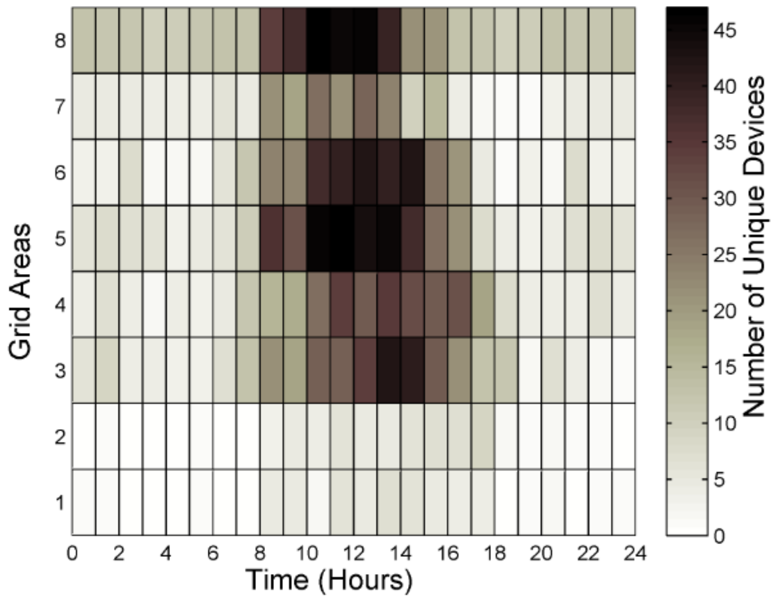


Fig. 7: Detected number of people in gridded areas.

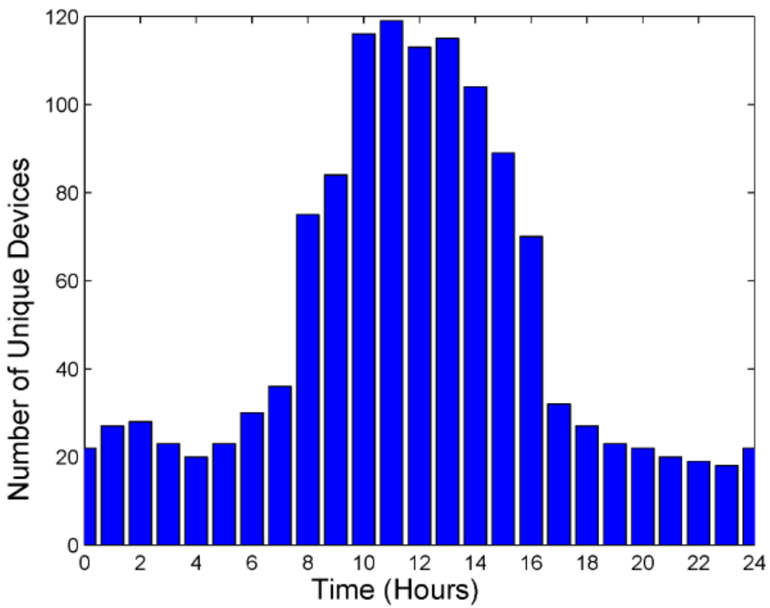


Fig. 9: Number of total people in gridded areas per hour.

Limitations

MAC address randomization may result in over-estimating the number of building occupants

No accurate occupancy tracking if we have a limited number of WiFi - PAs

Summary

By using probe requests, we can track the occupancy level information in different zones inside a building

WiFi-PA equipment can be used for passively capturing ambient probe requests from WiFi devices

No connectivity to a WiFi network is required.

This information is then used to localize users within coarsely defined occupancy zones

Obtain occupancy count within each zone at different time scales.

Imperial College London

Thank you!

Question?