Swansea University
Prifysgol Abertawe

Localization to Enhance Security and Services in Wi-Fi Networks under Privacy Constraints

Presenter: Gareth Ayres

Authors:
Gareth Ayres, Rashid Mehmood.*(Civil and Computational Engineering, **Swansea University**)*
Keith Mitchell2, Nicholas J P Race. *(Computing Department, InfoLab21, **Lancaster University**)*

Conference: EuropeComm2009, London.
Date: 12 August 2009

JANET UK

- Janet UK (UK Education and Research Network)
- www.ja.net

- Research carried out as part of the Janet UK Location Awareness Trial
- http://www.janet.ac.uk/development/network-access/location-awareness/index.html

Definition of Key Terms

- Localization to Enhance Security and Services in Wi-Fi Networks under Privacy Constraints:
  - **Localisation**: Determine physical location of a node
  - **Security:** Access Control, Authorisations
  - **Services:** Location Based Services (Context Aware)
  - **Wi-Fi:** 802.11g Wireless Networks
  - **Privacy:** Protection of nodes (hence human) location data

Introduction to the Problems

- Challenges:
  - Wi-fi becoming more and more pervasive
    - Number of Access Points increasing
      - Homes, Institutions, Industry
    - Mobile users move around more
      - Smaller lighter devices
    - No physical boundaries
      - Wireless leaks
  - Location based Services popularity increasing
    - Privacy of users under threat
    - Difficult to predict usage patterns
    - Infrastructure not designed to cater for mobility

Introduction to the Solutions

- Solutions:

- Fine-grained localisation system (indoors)
  - Geographic firewall
    - A LBS that provides Security and Containment as a Service

- Coarse-grained localisation system (per Building)
  - Allows Visualisation:
    - Predict usage patterns
    - Aid network infrastructure deign
    - Helps provide user privacy
  - Building Level Location based Services

Overview of Infrastructure

- Overview of Wireless Infrastructure:
- Wireless Hardware:
  - Cisco WiSM's
  - Light Weight Access Points (LWAPP)
  - Linux Servers
    - Java, C#.NET, PHP, MySQL, Apache
- Locations:
  - Main Campuses Coverage
  - Some halls of residence

GEOFIREWALL

- Aim:
  - Access Control of wi-fi nodes in a geographic containment area.
  - Defeat Leakage Problem.

  - Example:
    - block access to a particular lecture room during an exam
    - Or block specific protocols in that room (Chat/IM)
    - Without affecting other used of those AP's.

- Solution:
  - Geofirewall consists of:
    - Location Data Gathering
    - Location Based Security Policies
    - Access Control

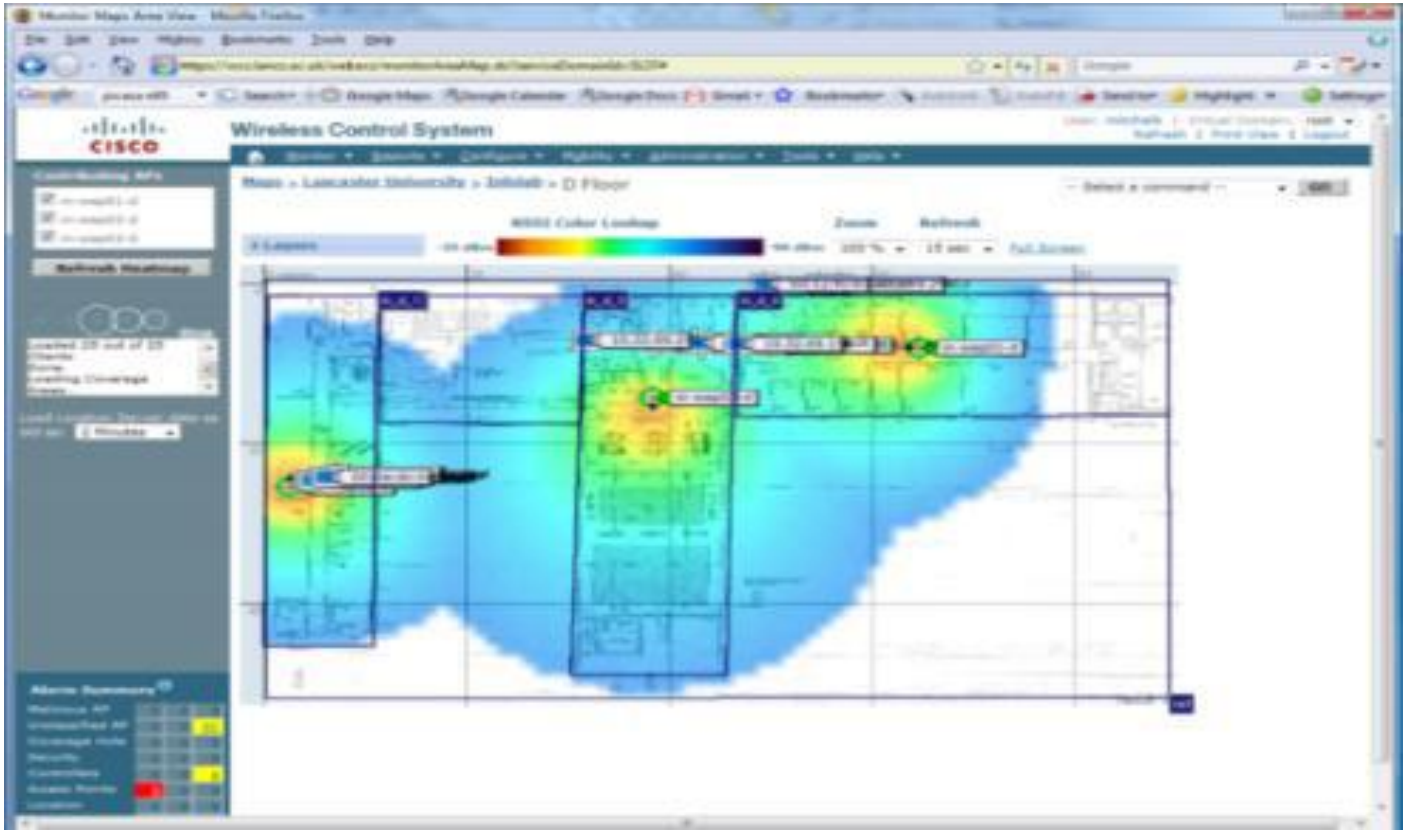
GEOFIREWALL: ARCHITECTURE

- Location Data Gathering
  - Custom Application in C#.NET
  - Communications with LA API using SOAP/XML
  - Request, Response, Notification
- Location Based Security Policies
  - Application provides a list of rooms available
  - Defines a room and time period to disable access
  - Spawns the LocoTrak service
    - Returns list of wireless nodes in that room at that time
    - Uses last 2 minutes worth of nodes
    - LocoTrak then forwards list of nodes to geofirewall
    - LocoTrack runs thread runs for duration of time period

GEOFIREWALL: ACCESS CONTROL

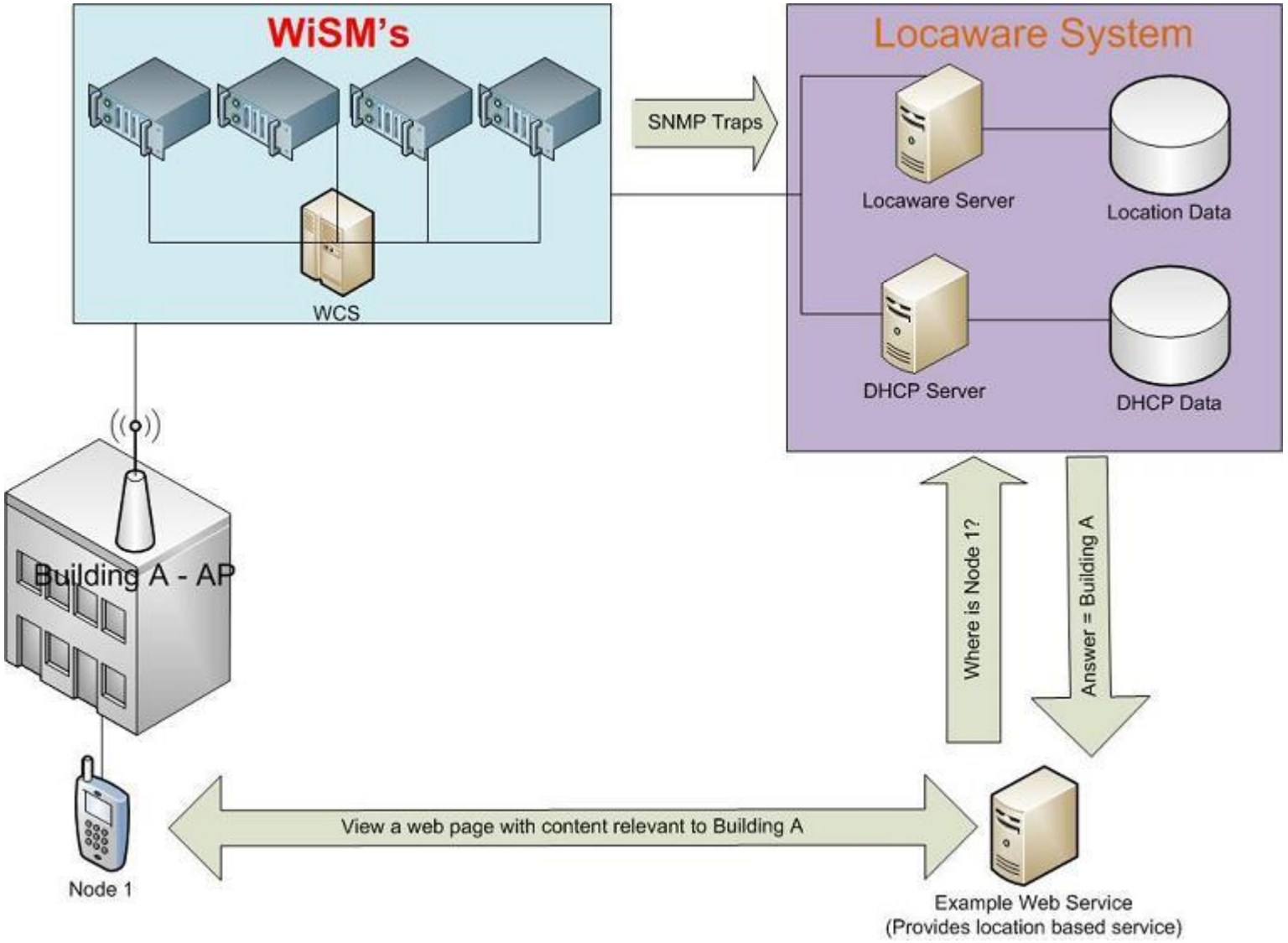
- Access Control. 3 possibilities:
  - Mac filters on WLC and de-auth packets
    - Easy to spoof MAC
    - No user feedback
  - Use existing role based firewall and captive portal
    - Requires full re-auth to regain access
    - Easy to spoof MAC
  - Dynamic configuration of IPTables
    - Scalability of 100's of rules
    - Facilitates a easy captive portal effect for HTTP traffic for feedback

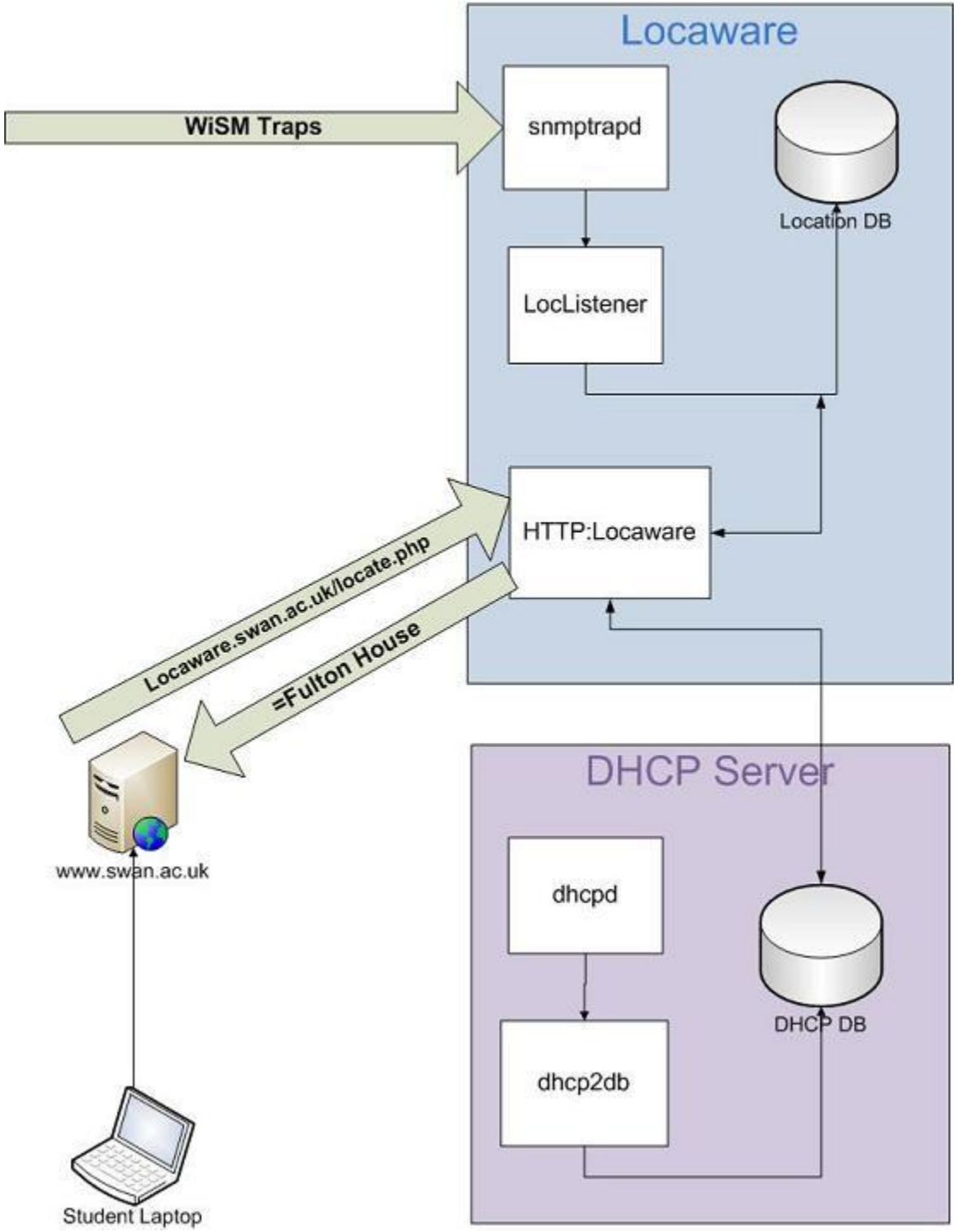
GEOFIREWALL: HEAT MAP



Coarse-Granularity Localisation

- Locaware Server:
  - Cisco WiSM's configured to send association/deassociation SNMP Traps to LocAware server
  - Custom Java software listens for Traps
    - Captures traps
    - Groupings of buildings and AP's defined
    - Groups and traps used for localisations calculations
    - Hashes made of trap info
    - Adds to a database
  - PHP scripts can then be called via HTTP GET to retrieve location information


WiSM's
WCS
SNMP Traps
Locaware System
Locaware Server
Location Data
DHCP Server
DHCP Data
Where is Node 1?
Answer = Building A
Building A - AP
Node 1
View a web page with content relevant to Building A
Example Web Service
(Provides location based service)


Locaware
WiSM Traps
snmptrapd
Location DB
LocListener
HTTP:Locaware
Locaware.swan.ac.uk/locate.php
=Fulton House
www.swan.ac.uk
DHCP Server
dhcpd
DHCP DB
dhcp2db
Student Laptop

Location Based Services

- Easy development of context aware web pages by web development team:
  - Provide a php script to embed in web pages
  - Script gets IP from header and send to Locaware System
  - Location of user is stored as variable in page

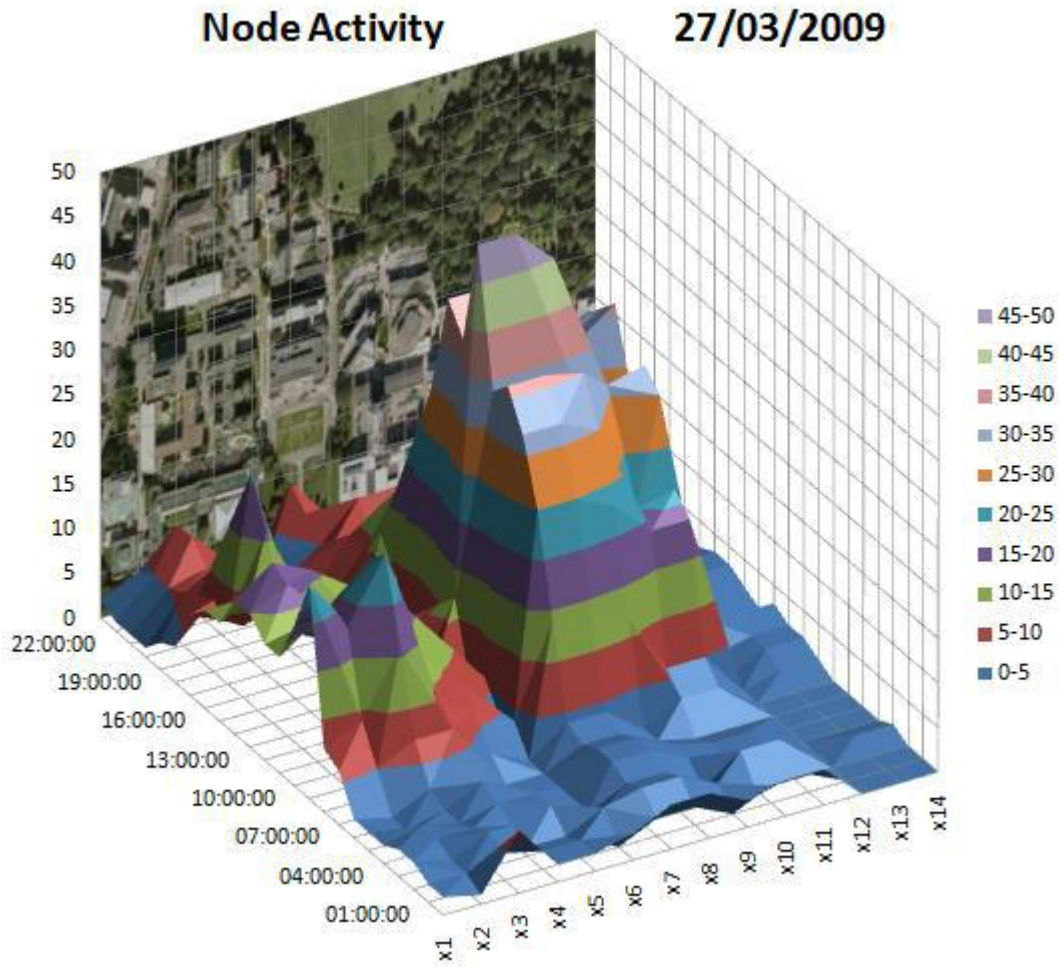
- Examples of use:
  - Google maps mashup of congested areas
  - Enhanced problem reporting
  - Data collection for determination of usage patterns
  - Possibilities:
    - Social Networking based on location
    - Device Auto configuration based on location (printing)

Last 5 Minutes Activity

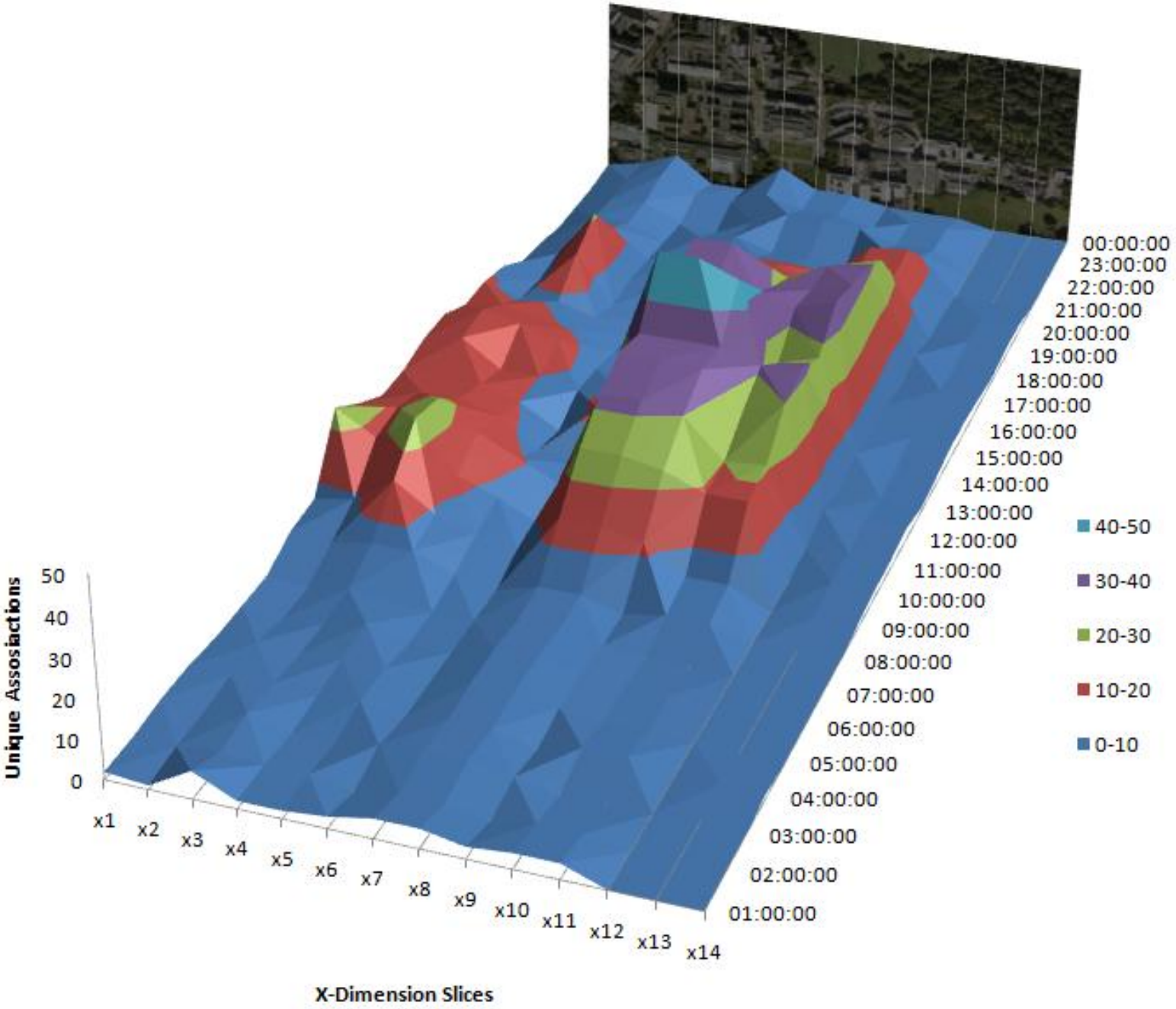
Previous 300 Seconds, Total Nodes Associated=**325**.

Usage Key: 0-1%, 2-5%, 5-7%, 7-10%, 10-13% 13-15%, 15-17%, 17-20%, 20+,

Usage Patterns with Privacy Constraints



Node Activity 27/03/2009



Conclusion

- Location data in the context of wi-fi networks can add lots of additional services and functionality

  - **Visualisation of data important**
    - Network Infrastructure planning
    - Usage patterns
  - **Location Based Services**
    - Some simple custom applications possible
      - Even using coarse-granularity
        - This aids privacy
  - **Geofirewall very useful**
    - Possible to combine AAA with location data for new LBS

Privacy Constraints

- Suggested users value feature rich technology over privacy
  - Privacy needs to be built in regardless
    - Fundamental human right
  - Some tradeoffs between privacy levels and functionality/accuracy
  - Some users reject all LBS technology
    - Opt in/out to be considered

Privacy Constraints

- Granularity, Storage and Presentation
  - Granularity implies location data accuracy
    - which is inversely proportional to privacy?
    - Correlation attacks
      - Inference and Assumptions
  - Storage of location data:
    - How long is location data useful?
    - Data stored in raw or obfuscated form
      - Pseudonyms and Hashing
    - Strict control on access to data
  - Presentation of data through API or Visualisation
    - Dummy nodes – adds noise
    - Mixed Zones – spatiotemporal zones

Questions

- Any Questions?

- **Gareth Ayres, Rashid Mehmood**
- *{g.j.ayres, r.mehmood}@Swansea.ac.uk*

- **Keith Mitchell, and Nicholas J P Race**
- *{k.mitchell, n.race}@lancaster.ac.uk*