Architectural Considerations for Location-Aware Networking

Marco Gruteser
WINLAB @ Rutgers University
Relevance of Location Information: A Vehicular Network Example

- VANETs a likely driver for deployment of location-based networking technologies
  - Compelling application scenarios: Vehicular collision avoidance (~40,000 deaths/yr in US)
  - FCC approved spectrum for Dedicated Short Range Communications
  - Challenging requirements: high velocity, low-latency environment, privacy, security, reliability

- Sensor information relevant in geographical context
  - Location is a natural addressing mechanisms
  - Location can scope interactions

- Network optimizations
  - MAC, Routing, Security
Location-Aware Protocol Stack

Application: Search, Sensor Aggregation, Proximity Detection, Geofencing

Location Service (e.g. Quorum-based, GLS, Homezone)

Transport (e.g. Geocast, Mobicast)

Network (e.g. GPSR, DREAM, LAR)

MAC (directional antenna protocols)

Application-specific representations

Location Fusion

Localization (e.g. Wifi Radar, GPS)

Overlay Services

- Location-aware technologies affect all traditional network layers
- Challenges
  - A coherent architecture
  - Supporting local interactions across domains (geocast from cell-phones to vehicles)
  - Privacy
Representing Location

- User-oriented applications: Symbolic representations
  - Postal addresses, road intersections, room and building numbers

- Sensing-oriented applications: High-precisions geoid models

- Network and MAC Layers
  - Considerations
    - Complexity of distance computations
    - Storage overhead
  - Easy in cartesian projections such as Universal Transverse Mercator, except when crossing zone boundaries
  - More difficult in ellipsoid models such as latitude, longitude

- Unified worldwide coordinate system or patchwork of local grid coordinate systems?

- Required level of accuracy?
  - For specification of points
  - For specification of regions (#edges in polygon?)

Source: GFZ Potsdam
Distilling Application Requirements for a location service

- Requirements are distilled/refined by studying and building many applications
  - No coherent architecture because requirements are unclear
  - Too few applications built because of insufficient system support

- Sample “Socket extensions” for location services
  - Determine own position
  - Locate any remote Host (e.g., for geographic routing)
  - Track Remote Host (e.g., for remote navigation applications)
    - Location-update events with specified frequency
  - Query hosts in geographic area (e.g., emergency evacuation)
  - Monitor hosts in geographic area (e.g., geofencing)
    - Application trigger indicating that remote host has entered/left geographic region (polygon) – needed for geofencing

- Additional network primitives
  - Geocast, Delay-Tolerant Geocast, Mobicast
  - Stream-oriented geobinding

- Support Functions
  - Coordinate system conversions
  - Interfaces for mapping and resolving symbolic names to geographical coordinates
Privacy Concerns: Identification Through Location

Identification based on public records, subpoenas not necessary

Aerial imagery (Google Earth/Terraserver)

Geocoded Address Database (TIGER/LINE):

John Doe
1234 Main St
Anywhere, US
(515110X 4300483Y, 13Z)

[515110X 4300483Y 13Z]
Privacy Architecture Components

- Applications
- Location Service
- Network
- MAC

Access Control
On-Device Localization
Silent Periods Disp. Addresses

Location Cloaking

Accuracy reduction

Coarse resolution throughout Internet
Medium resolution shared throughout local network
Maximum resolution shared with 1-hop neighbors

NSF WMPG Workshop, Aug 2-3, 2005
Privacy Architecture Components

- Applications
- Location Service
- Network
- MAC
  - On-Device Localization
  - Access Control
  - Location Cloaking
  - Silent Periods Disp. Addresses

- Coarse resolution throughout Internet
  - Medium resolution shared throughout local network
  - Maximum resolution shared with 1-hop neighbors

Accuracy reduction

NSF WMPG Workshop, Aug 2-3, 2005
Issues

- Accountability
  - Pervasive computing scenarios raise privacy concerns
    - provide increased sensor coverage
  - Solutions often in direct conflict with the effort to increase accountability in the Internet
    - To address spam, worms, etc.

- Overlay location service that connects islands of ad hoc services (?)
  - No clear unifying candidate among routing/transport protocols: sensing systems will choose from a larger set of possible protocols based on application requirements
  - Location service should provide a unifying grid-based coordinate system and offer facilities for translation among other systems

- User privacy and accountability are key requirements for location architecture
  - Consider access control and accuracy reduction techniques