

## Session II: *Wireless/Mobile/Sensor Network Requirements* - Moderator Mario Gerla

- Wireless Sensor networks for Environmental Monitoring – a Driver for Adaptive and Programmable Network and Distributed System Services (Deborah Estrin)
- Mobile/wireless Networking Scenarios/Requirements (Mario Gerla)
- Thoughts on Requirements Placed on the Network by Mobile Platforms (Kevin Kahn)
- Scaling Wireless Networks (Srinivas Seshan)
- Near-Field Networks (Badri Nath)
- Wireless/sensor net security (Wade Trappe)
- Interfacing embedded sensor networks to the Internet (Phil Levis)
- Discussion time

# What is this session all about?

- Identify new requirements placed by wireless users on the Internet “network layer”
- These new requirements may trigger a “redesign” of the IP stack (or more generally the way we do networking)
- We are not concerned with SOLUTIONS at this point (it is the job of Session III speakers)
- Questions to be addressed:
  - What is the wireless scenario/application you are addressing?
  - What is the problem to be solved?
  - What are the new qualitative requirements on the network layer?
  - What is the impact of these innovations on user performance?

# Break out session

- **We will identify the requirements using three scenarios:**
  - The **individual mobile user**, interacting with Internet resources only
  - The **mobile “constellation”**: the users equipped with several devices/interfaces, interacting with the Internet, with environment (instrumented user) and with each other (opportunistic ad hoc networking). This model applies to individuals while they walk, drive cars, fly planes, ride trains etc.
  - The **“dynamic” sensor fabric**: this concept includes the traditional environment sensor fields as well as the mobile sensor fields (people, car sensor fabrics). This latter scenario is clearly connected with the instrumented constellation scenario

# Requirements

- **The individual mobile user:**

- Identity vs address: ability to route to/from mobiles (mobility management)
- Flexible definition of identity and address, to allow: route to Internet addresses as well as geo addresses and geo regions; multicast and geo multicast
- Location tracking; mobility tracking (by network); location awareness (where am I?)
- delay tolerant delivery; disconnected operation
- Path awareness (source knows path quality and can adjust content delivery)
- Mechanisms that allow QoS negotiation where available
  - prioritization
  - congestion control (must avoid collapse)
- Network management:
  - End user management
  - support for resource management: efficient use of limited resources (opportunistic use - see Srini slides)
- Security and trust;
- Privacy: mobility privacy vs forensic capability
- economic incentives
- Performance implications of above

## Requirements (cont)

- **The “constellation” model:**
  - Individual ID versus constellation device IDs and addresses
  - Dynamic expansion/shrinking of constellation
  - Ability to find and connect to neighbors forming “opportunistic” nets possibly operated with native protocols
  - Ability to do identifier routing locally (with locally significant IDs), and address routing to Internet
  - Constellation instruments must support dynamic discovery of environment sensors
  - Constellations management and membership
  - Seamless handoff across constellation devices
  - Efficient use of multiple outgoing connections (to Internet and other constellation in the opportunistic ad hoc net)
  - Security issues beyond model 1 (isolated mobile): decentralized trust model support
  - Performance implications of above

## Requirements (cont)

- **Sensor networks:**

- Extending view of sensor nets to include mobile platforms (users, cars, robots, etc)
- In network processing support by exposing topology and path info
- Addressing geo regions (for “fused” content) as well as addressing individual nodes for diagnostics etc
- Energy saving routing, fusion, data collection support (from network level standpoint)
- Security issues beyond models 1 & 2
- Performance implications of above
- Example of enabled service: mobile-google “data mining” across the Internet, eg spatio-temporal data mining (what happened at 321 Main Str last night 1:15 AM?)

# Security

**Network will provide privacy and forensic capabilities (and provide a means to manage tradeoffs)**

**Location tracking/information must be trustworthy**

**Resource/network management should be trustworthy and individuals/entities accountable for misuse/greed/non-compliance**

**The wireless network should be robust and flexible enough to provide network connectivity/availability in the presence of adversarial (possibly unintentional) threats**

**Security management/assessment should be transparent and functional across heterogeneous environments (perhaps to facilitate warnings to network administrators)**

**Network control messages must be authenticated and trustworthy**

**Mechanisms or hooks should be available to allow for the assessment and conveyance of entity trust**

**Traffic analysis by adversaries should not be facilitated (e.g. prevent traffic analysis from sniffing)**

**Naming/addressing should be verifiable and authenticated**

# Radio Impact

- **Cognitive radios**
  - How to discover, use them
- **WiMAX**
- **MIMO**
- **Cooperative radios**
- **Path monitoring will include cross layer notification and exploitation**

# Summary

- **Routing to flexible identities and addresses**
  - Identities represent devices, constellations of devices, geo-areas
- **Security/privacy**
- **Delay tolerant delivery**
- **Visibility of path and topology quality**
- **“Identifier based” network management**
- **Physically decentralized local identifier routing**
- **QoS negotiation support mechanisms**

# Report writing

- **Must be completed by mid next week!!!**
- **About 7-8 pages**
- **Outline:**
  - Review of 3 scenarios, to motivate the introduction of REQUIREMENTS (Gerla)
  - Introduce scenarios progressively, with new requirements each time. This allows quite a bit of detail
    - First scenario:
      - Identity vs addressing (Phil)
      - Security (Wade)
      - Management (Badri)
      - Delay tolerant + disconnected ops(Phil)
      - Mobility management (Wade)
      - QoS + path/topo monitoring and feedback (Mario)

# Report (cont)

- Second scenario
  - Constellation: identity hierarchy (Phil)
  - “Infrastructure free” communications (Phil)
  - Ability to find and connect to neighbors forming “opportunistic” nets possibly operated with native protocols (Kevin)
  - Constellations management and membership (Badri)
  - Seamless handoff across constellation devices (Badri)
  - Efficient use of multiple outgoing connections (to Internet and other constellation in the opportunistic ad hoc net)- Srin
  - Security issues beyond model 1 (isolated mobile): decentralized trust model support (Wade)
  - Incentives; economic issues - Anthony Joseph

# Report

- Third scenario:
  - Constellation instruments must support dynamic discovery of environment sensors (Srini)
  - In network processing support by exposing topology and path info (Phil)
  - Addressing geo regions (for “fused” content) as well as addressing individual nodes for diagnostics etc (Badri)
  - Energy saving routing, fusion, data collection support (from network level standpoint) - Wade
  - Security issues beyond models 1 & 2 - Wade
- Section on impact of radios (cross layer concept) - Mario
- Add a scenario with the performance required by applications-Mario
- Summary of requirements at the end - crisp definition of key requirements (Mario)