



Future Internet Architecture and Protocols: Mobile/Wireless Requirements

Breakout Session

Participants: Victor Bahl, Marco Gruteser, Dave Johnson,
Jim Kurose, Shalini Periyalwar, Ramesh Rao, Ram
Ramanathan, Peter Steenkiste, Nitin Vaidya and others

Example “grounding” questions

- Can IP evolve to meet emerging mobile requirements, or is there a real need for new architectures and protocols?
- If not IP, can we outline a possible end-to-end protocol architecture concept?
- What are the pros and cons of multiple custom overlays vs. a single multi-purpose protocol?
- How would a proposed new network deal with router mobility? Link impairments? Link adaptations and control? Is a cross-layer approach necessary/sufficient?
- How is location to be integrated into the networking framework, or should it be an overlay?
- How is content or context awareness to be incorporated, or should it be an overlay?
- What are the lessons learned from previous similar efforts -- e.g. ATM, active networks? On what not to do for a new network?
- What are the security implications of the above and of any ideas you have in mind?

Problems: Disruptive Features

- Mobility
 - Endpoint as well as router as well as cluster of endpoints/routers
 - Security (distributed trust) e.g. ad hoc vs infrastructure modes
 - Presence (location), geographic service, tracking positions
 - Anonymity
- Identity vs addressing discrimination (e.g. of sim cards)
- Spectrum of tolerance to delays
 - Delay-tolerant networks/ carry and forward
 - Intermittance-tolerance (TCP/Apps don't time out)
- Phy/Link adaptation and agility
 - Wireless endpoints and routers
 - Where to do the adaptation (e.g. when room gets up and moves)
- Tension between control and automation
 - Framework in which we can study that

Problems(Contd)

- Designing for unpredictable phy layer technologies
- DoS attacks indirect, doesn't need to be injected into your network
- Management issues
 - Sheer numbers
 - Intangibility
- Business perspectives for wireless infrastructure
- Simplifying infrastructure and distributing functionality DNS -> semantic addressing, self protecting, healing, configuring
- At level in the stack is discovery done
- Agile radios imply agile links

- Hooks in the architecture to accommodate legal regulations (??)

Problems (contd)

- Endpoints don't speak IP in sensor nets
- Nodes managed as one entity -- virtual node
- Actuator nodes
- Dynamic opportunistic spectrum and secondary leasing
- QoS provisioning is an n-party thing

Architectural Impact

- IP level support for mobility. Mobile IP can be made better (DNS based, semantic addressing?)
 - Flexible layering having at one or more levels
- User defined anonymity settings
- Resource discovery as you move from one location to another
- Manage complexity through localized actions
- Better instrument the Internet so that we can decompose end to end and make available for automated processing and reasoning and response
- Actuator: Timing, bandwidth, prioritization, mixing command and data

Impact (contd)

- Policy framework for experimentation with wide area wireless networks
 - Provisioning dynamism calls for dynamic control constrained by many things including policy
- Location awareness at all layers of the stack
- Location privacy at all layers of the stack
- Identifying security breaches without looking at packet
- Flexibility and cross-layer approaches
- On demand creation and management of links/topology
- New transport protocols

BorderGW vs Overlays vs Clean slate

- All of these are relevant
- They should evolve together, innovation could happen as underlay under overlay
- Overlays vs clean slate difference may be in performance

Summary of recommendations

- Mobility, broadly defined, must become fundamental to the next generation Internet architecture
 - Within and across heterogeneous networks
 - Endpoint as well as router as well as (multi-homed) cluster of endpoints/routers
- Ability to exploit location information should be incorporated at several layers
 - geographic service, tracking positions, geocasting
- Security, privacy should be addressed by a flexible framework that allows for selectable tradeoffs
 - Wireless networks have new implications in terms of tradeoffs

Summary (continued)

- Manageability
 - Simplifying infrastructure and distributing functionality, semantic addressing, self protecting, healing, configuring
 - Instrumentation of network components across all layers, decomposition of information for automated processing and reasoning and response
 - Large sensor/actuator networks
- Adaptive and efficient resource usage
 - But must be balanced against management and control complexity
 - Dynamic spectrum-agile resource usage
- Flexible layering
 - Cross layer techniques and rethinking what belongs to which layer