JUNE 23-24, 2004 • SALISH LODGE & SPA • SNOQUALMIE, WA

Mesh Networking Summit 2004

MAKING MESHES REAL

Microsoft Research

Microsoft
Your potential. Our passion.

Mesh Networking

http://research.microsoft.com/mesh

Victor Bahl
Senior Researcher
Systems and Networking Group
Microsoft Research

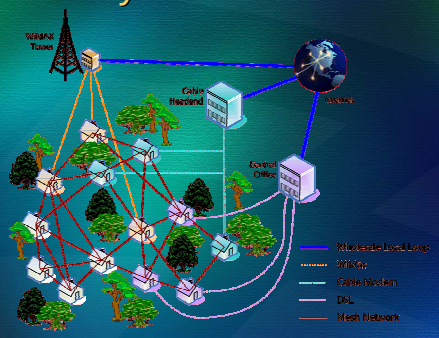
Team Introduction

Executive Sponsor
- Craig Mundie, CTO & Senior Vice President Microsoft

Microsoft Research
- Victor Bahl (Project Lead), Richard Draves, Jitu Padhye, Lili Qiu, Alec Wolman, Brian Zill

The Venice Incubation
- Jeff Erwin (Project Lead), Pierre De Vries, Ian Ferrell, Jason Ginchereau, Steve Kelly, Alexander Popoff, Karen

Community Network



Community Network Applications

Internet use increased social contact, public participation and size of social network. (social capital - access to people, information and resources)

Keith N. Hampton, MIT (author of "Netville Neighborhood Study")
URL: http://www.asanet.org/media/neville.html

- Shared Broadband Internet Access
- Neighborhood watchdog (e.g. video surveillance)
- Neighborhood TiVO
- Medical & emergency response
- Distributed backup
- Neighborhood eBay, portals
  - Bits produced locally, gets used locally
  - Social interaction

Mesh Formation: Problem Formulation

Question

How many homes in the neighborhood have to sign up before a viable mesh forms?

Answer depends on
- Definition of "viable"
- Wireless range
- Neighborhood topology
- Probability of participation by a given houshold

Example Scenario

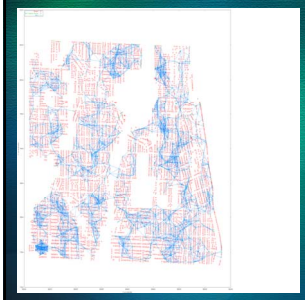
Viable mesh: group of at least 25 houses that form a connected graph

Topology: A North Seattle Neighborhood. 8214 houses, 4Km x 4Km

Wireless range: 50, 100, 200 and 1000 meters

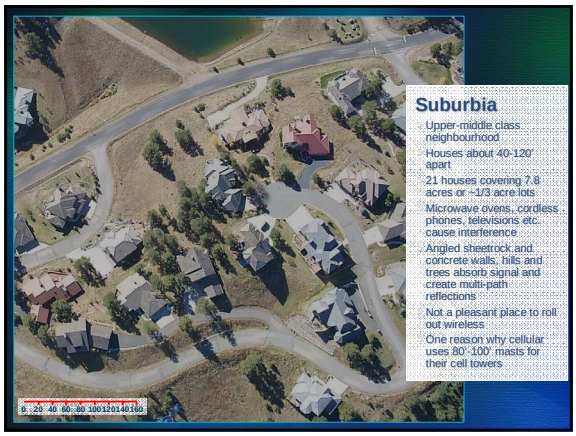
Houses decide to join at random, independent of each other. We consider 0.1% to 10% participation rates.

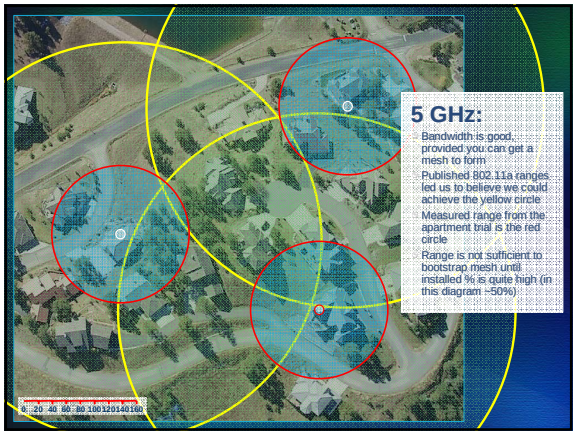
Mesh Formation



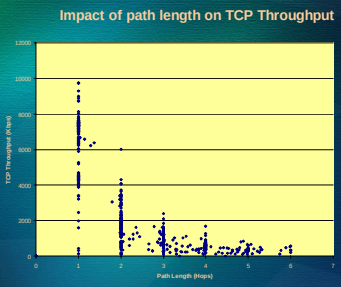
- 5-10% subscription rate needed for suburban topologies with documented wireless ranges
- Once a mesh forms, it is usually well-connected
  - i.e. number of outliers are few (most nodes have > 2 neighbors)
- Need to investigate other joining models
- Business model considerations will be important

Increasing range is key for good mesh connectivity

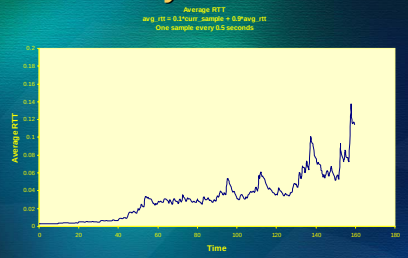




802.11a in a Multihop Network

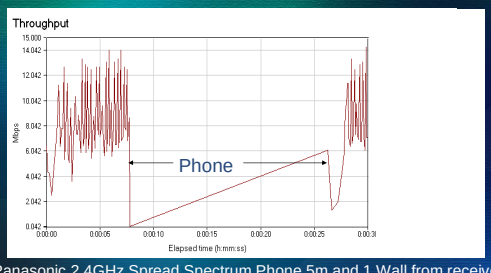


Round Trip Delay versus Node Density



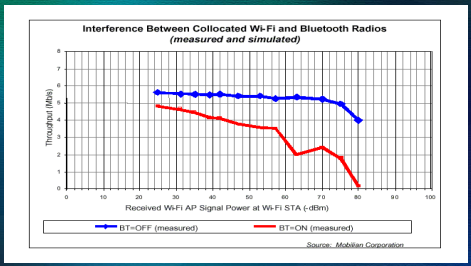
A new 100Kbps CBR connection starts every 10 seconds, between a new pair of nodes. All nodes hear each other.

Collision between ISM devices



Panasonic 2.4GHz Spread Spectrum Phone 5m and 1 Wall from receiver

Colliding standards



Performance worsens when there are large number of short-range radios in the vicinity

Conclusion

Meshes are viable
existing technologies are inadequate

To make it real

Identify and solve key problems
build and deploy a mesh prototype

Problem Space

Range and Capacity [Talk by Jim K; Poster by John D. & Ranveer C.]
- Electronically steerable directional antenna or MIMO for range enhancement
- Multiple frequency meshes
- Multi-radio hardware for capacity enhancement via greater spectrum utilization
- New data channel MAC for higher throughput
- Tools for predicting & analyzing network viability & performance

Multihop Routing [Talk by Rich D.; Poster & Demo by Jitu P. & Brian Z.]
- L2.5 on-demand source routing. Routes selected based on link quality
- Route selection with multiple radios

Security and Fairness
- Guard against malicious users (and freeloaders)
- EAP-TLS between MeshBoxes, PEAPv2 or EAP-TLS between clients and MeshBoxes
- Priority based admission control, Secure traceroute

Self Management & Self Healing [Talk by Lili Q.; Poster by AP]
- Desirable: avoid network operator - minimal human intervention
- Watchdog mechanism
- Data cleaning and liar detection
- Online simulation based fault isolation and diagnosis

Problem Space (Cont)

Smart Spectrum Utilization
- Spectrum Etiquittes
- Agile Radios, cognitive radios
- Cognitive software & applications

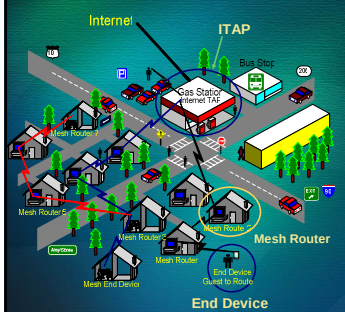
Analytical Techniques
- Information theoretic tools that predict expected capacity with practical constraints, based on experimental data

Digital Rights Management (DRM)
- Broadband access will become popular with expanded digital content.
- Increase the value proposition for end-users/subscribers

Ease of use (Plug and play, HCI)
- Make the user experience pleasant
- QoS protocols over wireless meshes to improve content delivery

Proof of Concept via rapid prototyping and testbed deployments

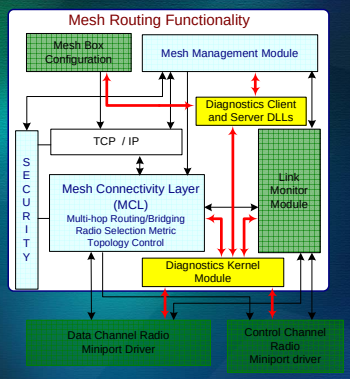
Scenario: Neighborhood Wireless Meshes



End Device
- Connects to a Mesh Router
- Standards Compliant Network Interface

Mesh Router / MeshBox
- Routes traffic within the mesh and to the neighborhood Internet Gateway
- Serves as access point for End Devices

Neighborhood Internet Gateway
- Gateway between the mesh nodes and the Internet



Research Results

Spectrum Etiquette

- P. Bahl, A. Hassan, P. Vries, Spectrum Etiquettes for Short Range Wireless Devices Operating in the Unlicensed Band - A Proposal, White paper, Spectrum Policy: Property or Commons, Stanford Law School

Multi Radio Meshes

- A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou. **A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks**. BroadNets 2004 (also Technical Report, MSR-TR-2003-41, June 2003)

Determining Mesh Capacity

- K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu. **Impact of Interference on Multi-hop Wireless Network Performance**. ACM Mobicom, San Diego, CA, September 2003

Mesh Self Management

- L. Qiu, P. Bahl, A. Rao, and L. Zhou. **Fault Detection, Isolation, and Diagnosis in Multi-hop Wireless Networks**. Technical Report, MSR-TR-2004-11, December 2003

Research Results (cont.)

Single Radio Mesh Performance

- R. Draves, J. Padhye, and B. Zill. **Comparison of Routing Metrics for Static Multi-Hop Wireless Networks**. ACM SIGCOMM 2004 (also Technical Report, MSR-TR-2004-18, March 2004)

Single Radio Mesh Performance

- R. Draves, J. Padhye, and B. Zill. Routing in Multi-radio, Multi-hop Wireless Mesh Networks, To appear in ACM MobiCom 2004

Multi Radio Mesh Routing & Performance

- L. Qiu, P. Bahl, A. Rao, and L. Zhou. **Fault Detection, Isolation, and Diagnosis in Multi-hop Wireless Networks**. Technical Report, MSR-TR-2004-11, December 2003

Capacity Enhancement

Problem

Improve throughput via better utilization of the spectrum

Design Constraints

Require only a single radio per node
Use unmodified IEEE 802.11 protocol
Do not depend on existence of control channel

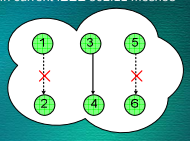
Assumption

Node is equipped with an omni-direction antenna
- MIMO technology is OK

Multiple orthogonal channels are available
Channel switching time is 80 usecs.
- current speeds 150 microseconds

Capacity Enhancement

In current IEEE 802.11 meshes

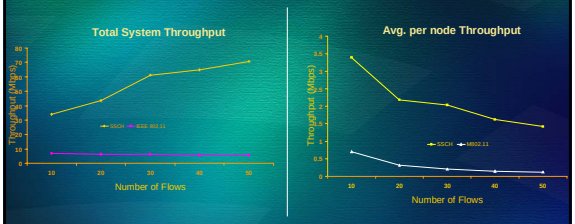


Only one of 3 pairs is active @ any given time

With MSR's SSCH enabled meshes

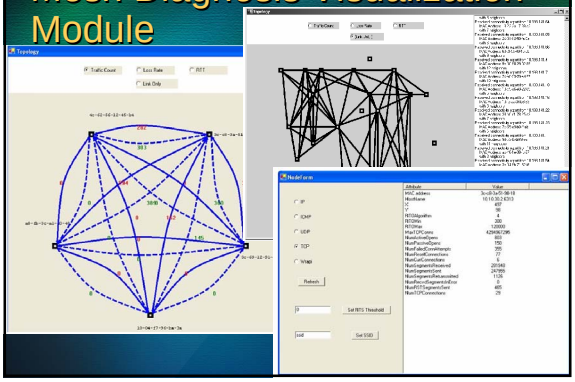
Performance

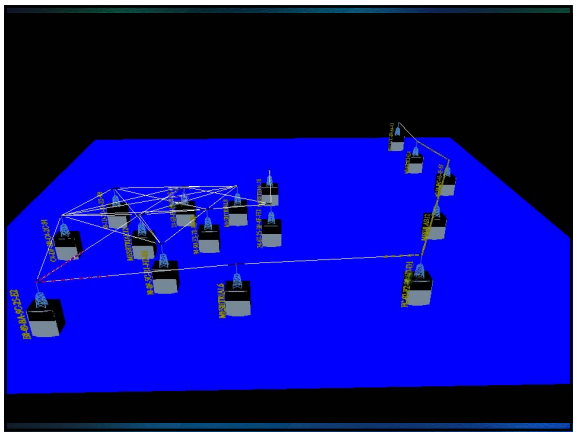
100 nodes, IEEE 802.11a, 13 channels, every flow is multihop



Significant capacity improvement when **traffic** load is on multiple separate flows

Mesh Diagnosis Visualization Module





Testbeds

Details

- 23 to 30 nodes
- Inexpensive desktops (HP d530 SF)
- Two radios in each node
  - NetGear WAG or WAB, Proxim OriNOCO
  - Cards can operate in a, b or g mode.

Purpose

Verification of the mesh software stack

- Routing protocol behavior
- Fault diagnosis and mesh management algorithms
- Security and privacy architecture
- Range and robustness @ 5 GHz with different 802.11a hardware

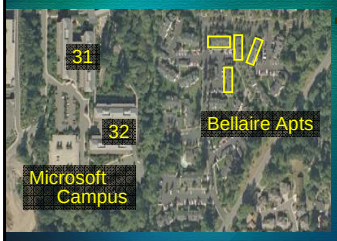
Stress Testing

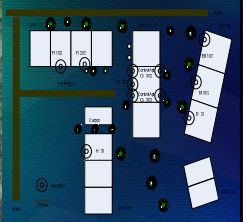
Various methods of loading testbed:

- Harpoon traffic generator (University of Wisconsin)
- Peer Metric traffic generator
- Ad-hoc use by researchers

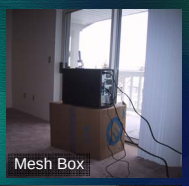
Redmond Apartment Trials

Deployed by The Venice Team





Redmond Apartment Trial



Cambridge UK Trial

Deployed by The Venice Team

Working with *ehome* to create a media sharing demo in collaboration with ZCast DVB trial

10 node mesh

Near Term Goals

- Multi-radio mesh routers
- Directional Antenna enabled meshes
- Multi spectral meshes
- Mesh Connectivity Layer
- Self Managing Meshes
- Large Scale Testbeds

We hope to take this research to the Point of Irrefutability

Thanks!

http://research.microsoft.com/mesh

802.11{a,b,g} in Meshes

Severe throughput degradation as number of hops increase
- Need more Internet connections to cover fixed area ($$$)

Poor fairness properties
- No guarantee that every user will get a fair share (equal) bandwidth

Current software (firmware) for ad hoc 802.11 connectivity is immature
- Frequent disconnects, frequent network partitioning

Bottom Line: Current off-the-shelf WLAN technologies are not suitable for multihop

Slotted Seeded Channel Hopping

Approach
- Nodes hop across channels to distribute traffic
- Senders loosely synchronize hopping schedule to receivers
- Layer 2.5 protocol works on top of MultiNet

Features
- Distributed: every node makes independent choices
- Optimistic: exploits common case that nodes know each others' channel hopping schedules
- Traffic-driven: nodes repeatedly overlap when they have packets to exchange

Prior Work

SEEDEX (MobiHoc '01), TSMA (ToN '97), multi-channel MAC (VTC '00, UIUC '03),

SSCH Algorithm & Performance

Every node has a channel hopping schedule
- 4 pairs of (channel, seed) = (x_i, a_i)

Hop to a new channel every 35 packets, 1536 bytes/packet
- $x_i \leftarrow (x_i + a_i) \bmod 13$ (802.11a has 13 channels)

Parity slot $x_{parity} = a_1$ prevents logical partitioning
- When unsynchronized, still overlap ~$1/13^{th}$ of time → can exchange updated schedules

Synchronize = Change your schedule to match another node's

Common case in sending is know recipient node's schedule
- propagation of schedule information is more frequent than start of new flows
- if wrong, pay latency penalty

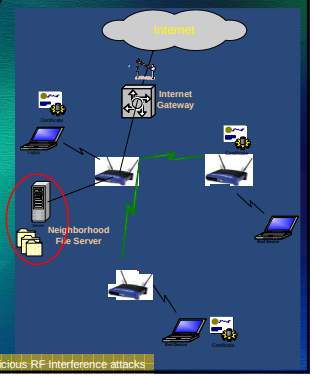
Mesh Security Architecture

Philosophy

Mesh is open to all, however, people who contribute resources to the mesh get priority.

Design Goals
- Guard against faulty or hacked Mesh Boxes
- Defend against disruption (e.g., denial-of-service attacks) by malicious End Devices
- Protect mesh traffic privacy
- Protect access to network resources

Assumptions
- Difficult to hack into a Mesh Box (similar to cable modems)



Regulations handle malicious RF interference attacks

Basic Framework

Certification
- Mesh Routers have built-in public-key certificates for authenticating to each other
- Mesh Router owners use them to issue certificates to End Devices
- Mesh Box accepts certificates issued by any Mesh Box within range
- Access to resources is controlled based on policy and End Device certificate

Encryption & Anonymity
- Traffic between Mesh Boxes is encrypted to foil eavesdroppers
- Misbehaving Mesh Boxes have their certificates "blackballed"
- Traffic from uncertified End Devices is prevented from disrupting certified traffic