μ-Operators, User-Provided, Community, and Cognitive Networks in Open Spectrum Access

George C. Polyzos

Mobile Multimedia Laboratory

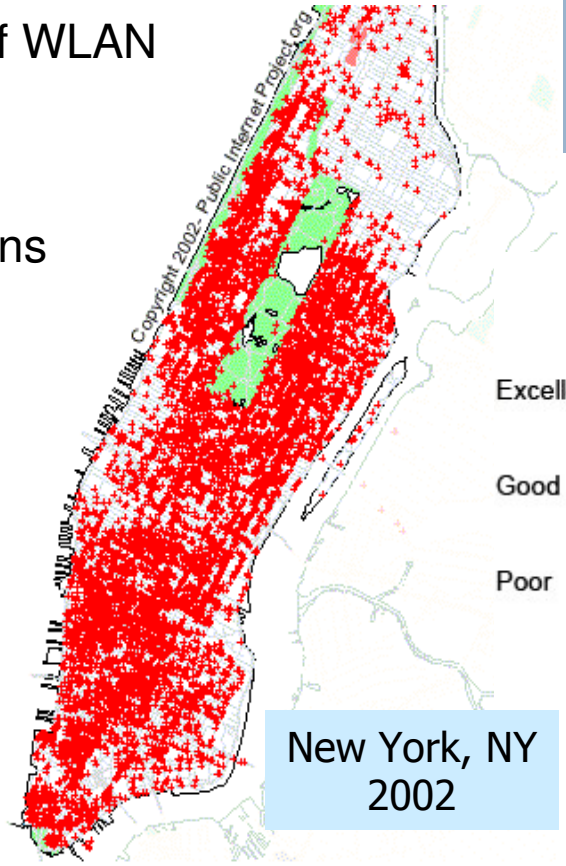
Department of Informatics/Computer Science
Athens University of Economics and Business
47A Evelpidon, 11362 Athens, Greece

polyzos@aueb.gr, http://mm.aueb.gr/
Tel.: +30 210 8203 650, Fax: +30 210 8203 325

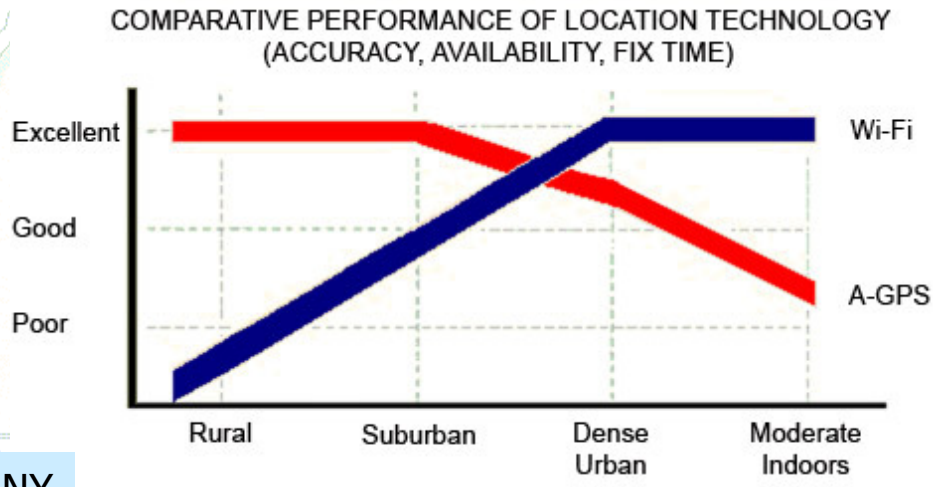
ICCCN 2009, San Francisco, CA, August 2009

Numerous Wireless Nets in Metropolitan Areas…

- So many Wi-Fi's that…
  you can base a business on their existence…
- The case of Skyhook Wireless, Inc.
  - Wi-Fi Positioning System: a GPS-like service
  - Relies on database of WLAN beacon signals
  - 70% of US, CDN, & Australian populations
  - by the end of 2007:
    - top 50 metropolitan areas in Europe &
    - top 15 cities in Asia



New York, NY
2002



Wireless Community Networks (WCNs)

WCN History

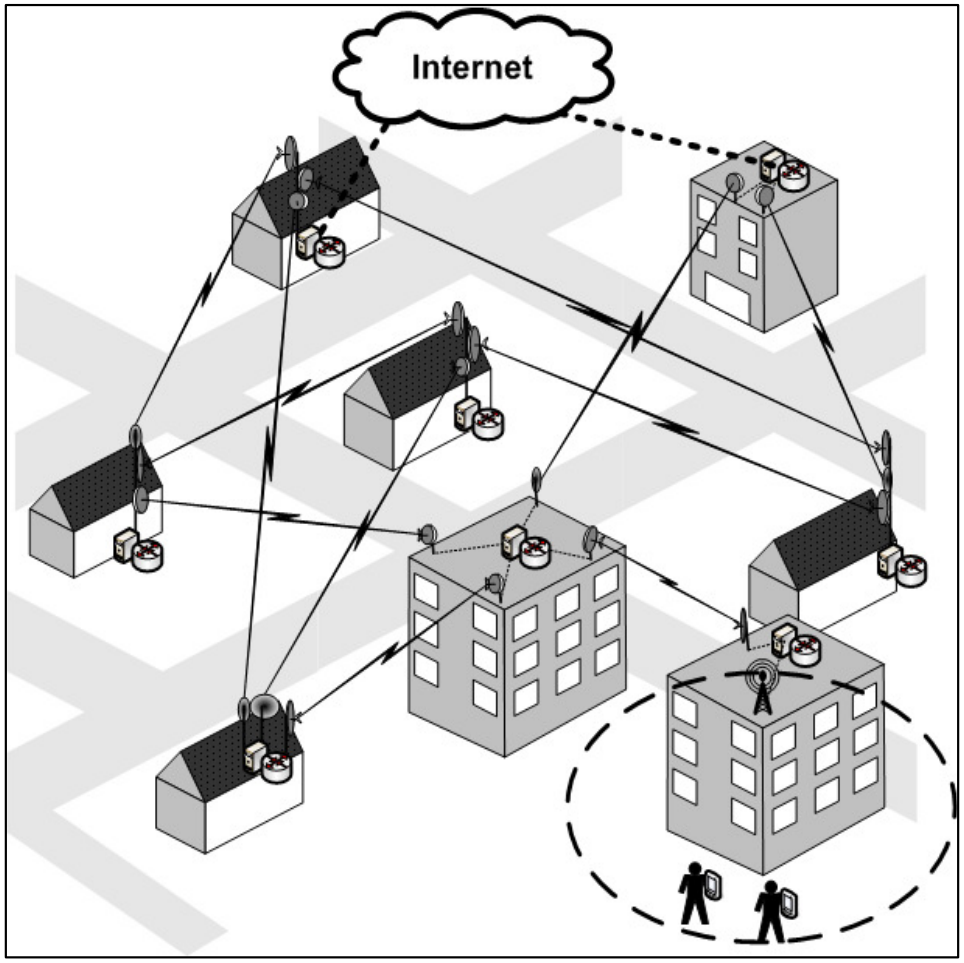
- Birth [late 90s, early 00s]
  - Fixed broadband: expensive and scarce
  - Experiments with Wi-Fi-based long distance links
  - First WCNs:
    - SeattleWireless (2000)
    - NYCWireless (2001)
    - Athens Wireless Metropolitan Network (2002)
  - In Greece: community-wide broadband services in the dial-up era!

- Growth factors
  - Low broadband penetration
  - Enthusiasm in the academic community
    - Universities deploy/participate in WCNs for experimentation
  - New Wi-Fi standards: 802.11a
    - Higher throughput, less interference → more interfaces per node
    - Replaced 802.11b at the backhaul

Wireless Community Networks: Technologies & Architectures

- Technologies
  - Based on Wi-Fi / IEEE 802.11
  - Modifications for PtP links
  - Open hardware and software platforms
    - Hand-made hardware (antennas)
- Architectures
  - **Mesh** based
  - **Hotspot** based

WCN Architecture: Mesh-based

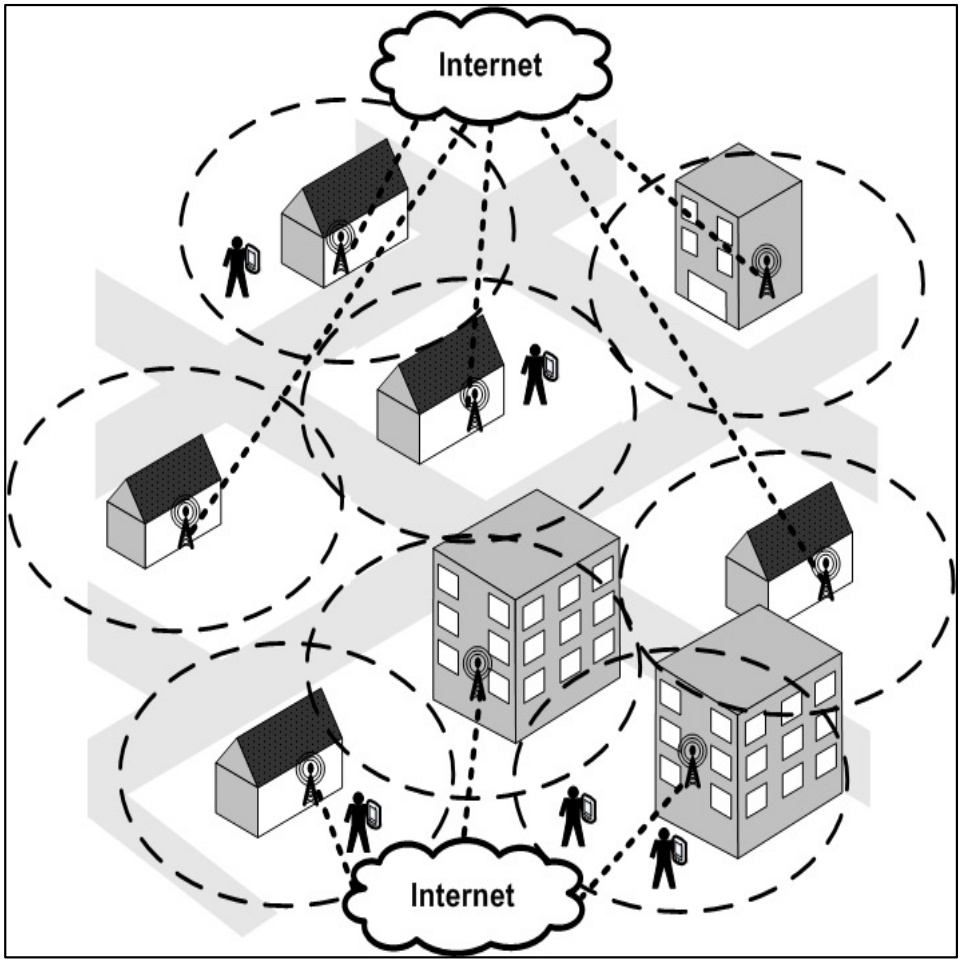


Mesh architecture

- All-wireless backhaul
- Community owned network
- Access points (optional)
- Internet connection sharing -- WCN-to-Internet gateways (optional)
- Focus on network autonomy

WCN Architecture: Hotspot-based

- Community-owned(?) WLAN Access Points
- APs attached to fixed wired broadband lines
- Focus on Internet access

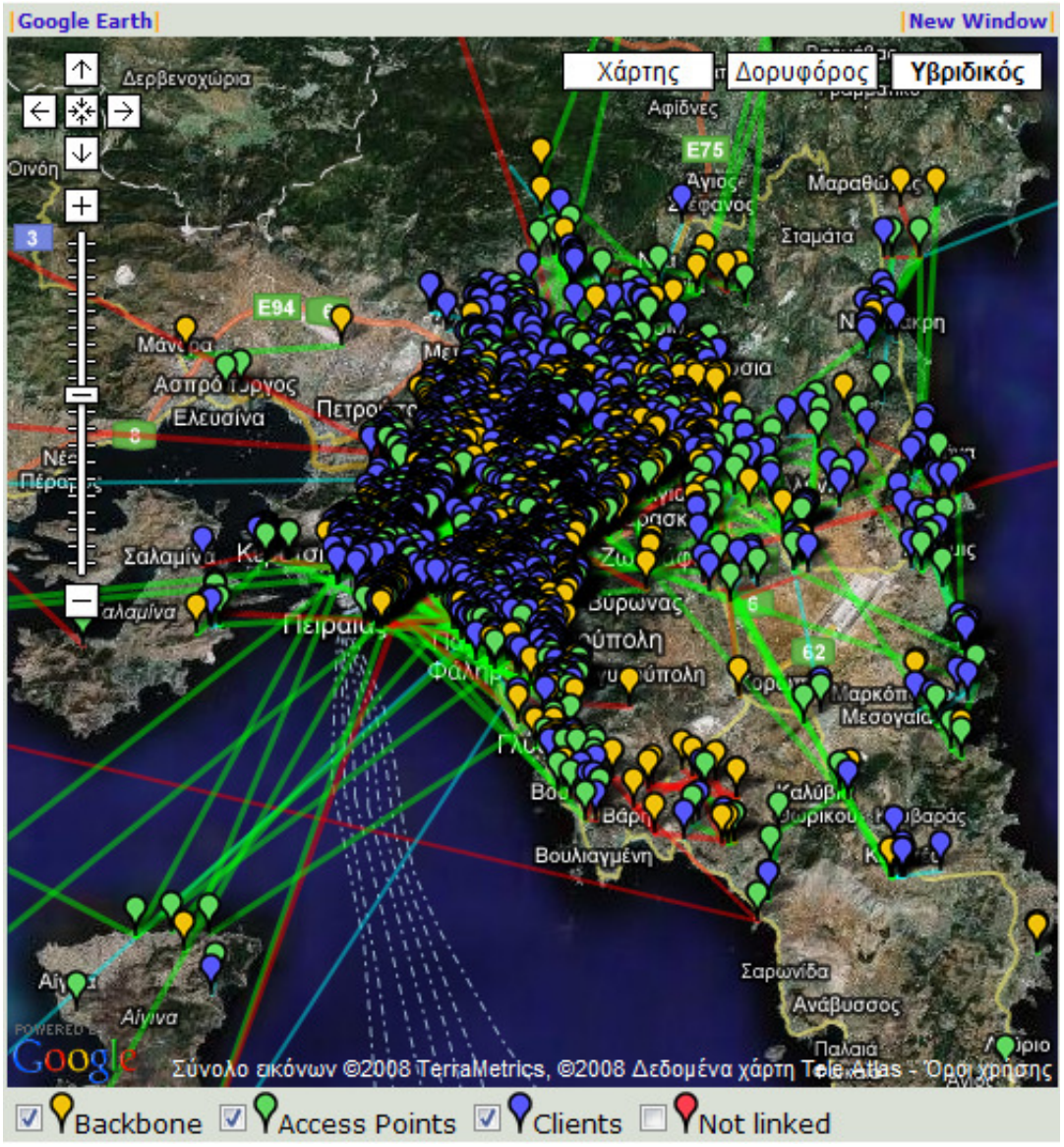


Hotspot architecture

Wireless Community Networks…

Seattle Wireless	**Seattle, US**	**75 nodes**	**Mesh**
AWMN	**Athens, GR**	**2331 nodes**	**Mesh**
CUWiN	**Urbana, US**	**48 nodes**	**Mesh**
Berlin's Freifunk	**Berlin, DE**	**316 nodes**	**Mesh**
NYCWireless	**NYC, US**	**149 nodes**	**Hotspot-based**
Wireless Philadelphia	**Philadelphia, US**	**15 miles^2**	**Hotspot-based**
FON	**Worldwide**	**~210 000 registered APs**	**Hotspot-based**

Athens Wireless Metropolitan Network

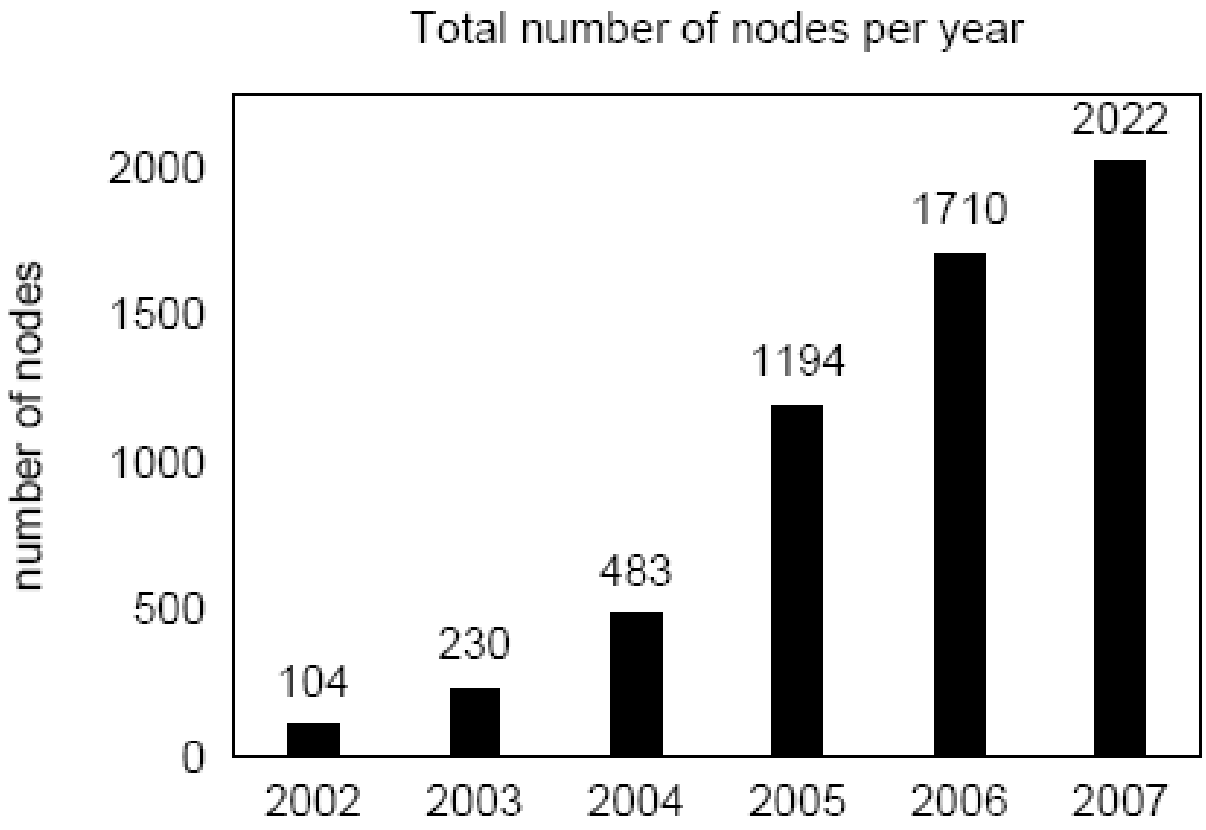


- **among the largest, globally**
  - **2331 active nodes**
  - **2786 links**
  - **791 active services**
- **Node #66 @ MMlab**

Study of AWMN Evolution

- Data come from
  - Information stored in WiND database
    - Wireless Node Database
    - available on the Internet
    - stores data about nodes, links, services
  - Measurements that we made from our AWMN node (aueb|mmlab, #66)
    - measurements were repeated on 5 different days and at different times
- We investigate differences between the two sources

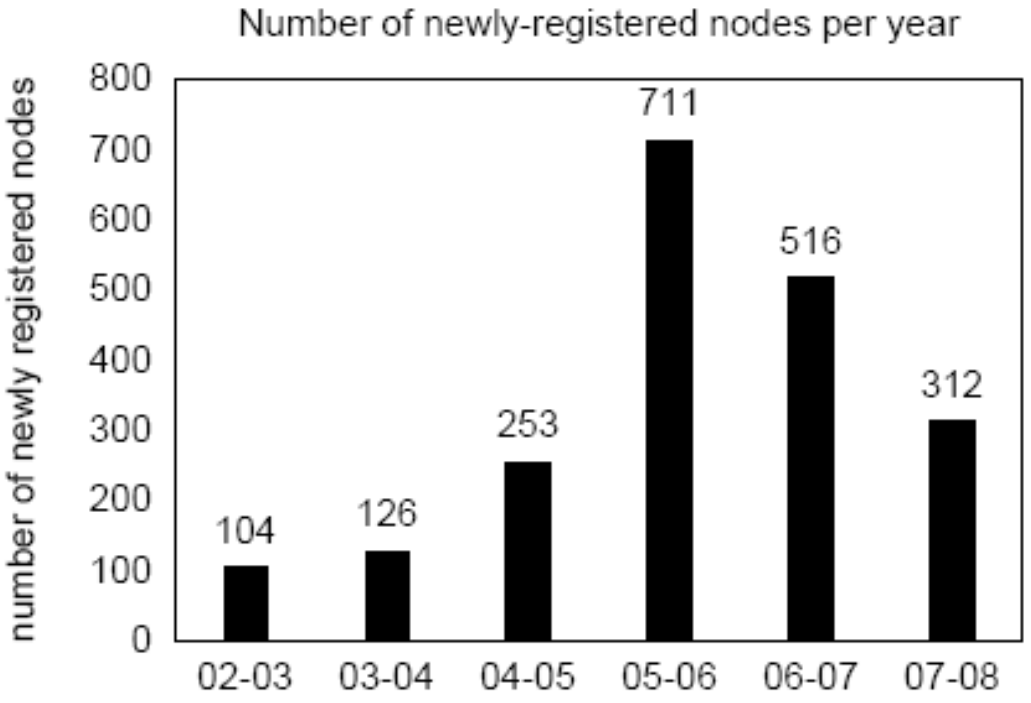
Evolution in participation over the years

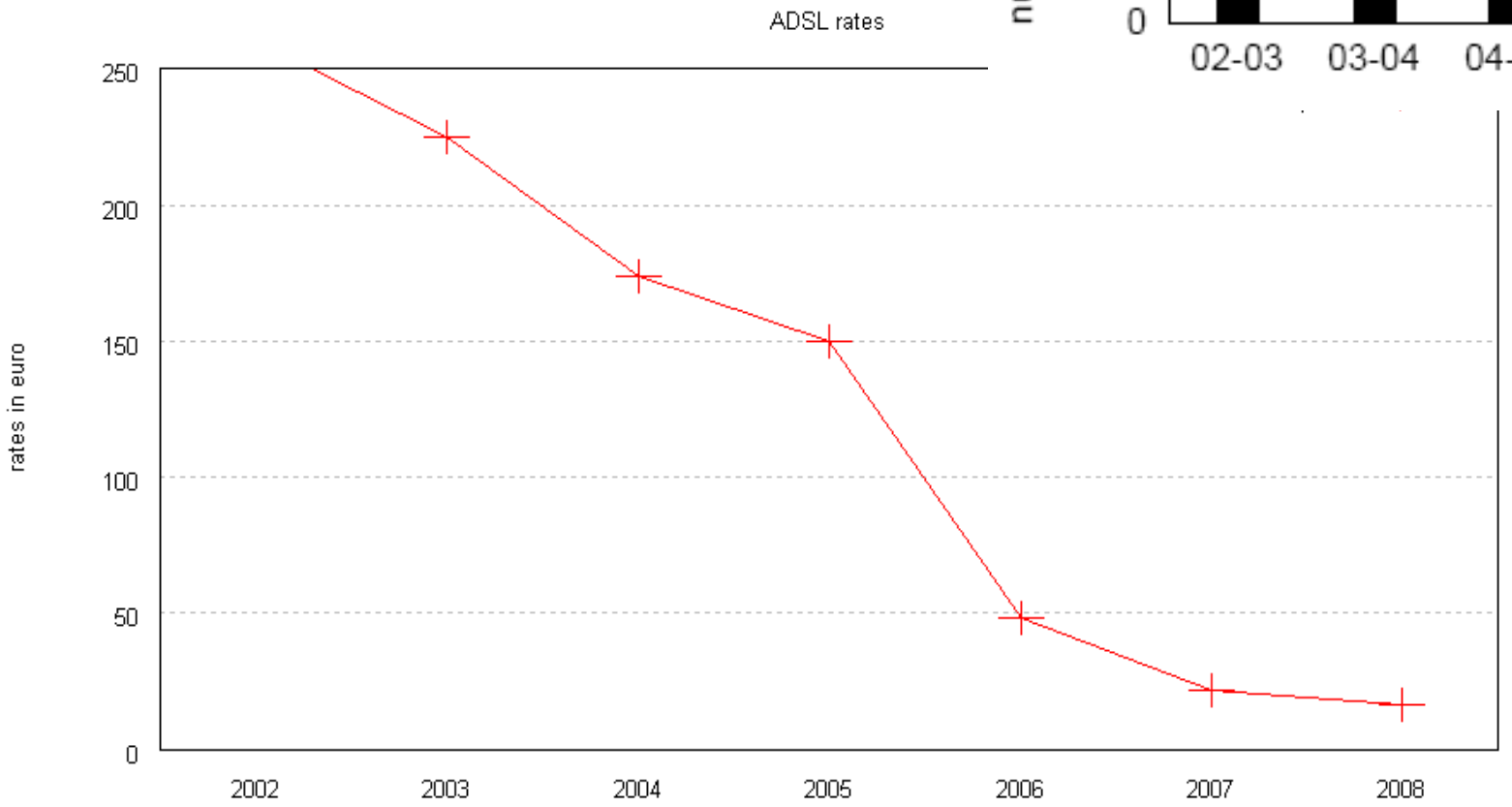


- The size of AWMN has always been increasing

Newly registered nodes per year

- They started decreasing after 2006
- ADSL price decreased significantly during the same period

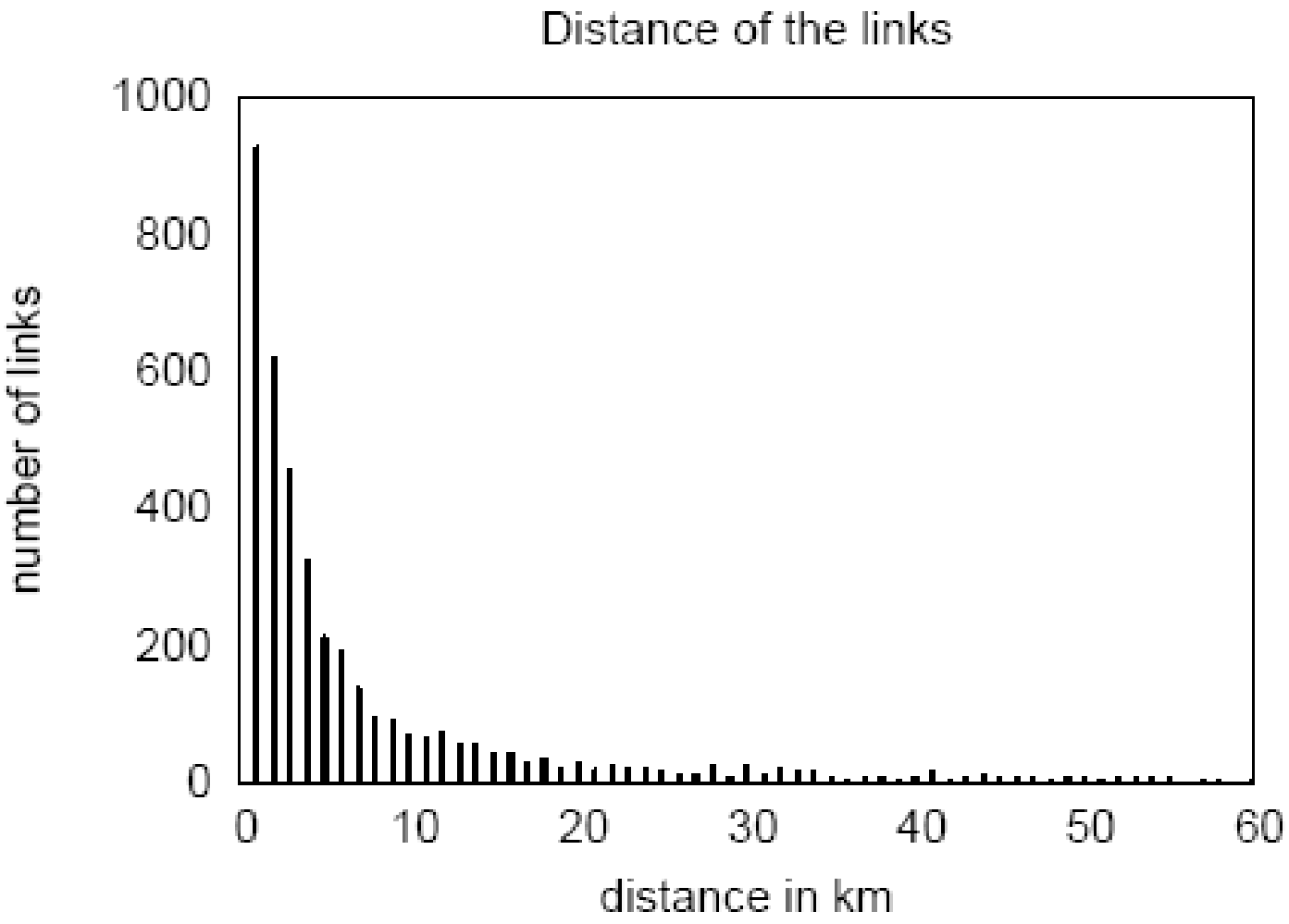




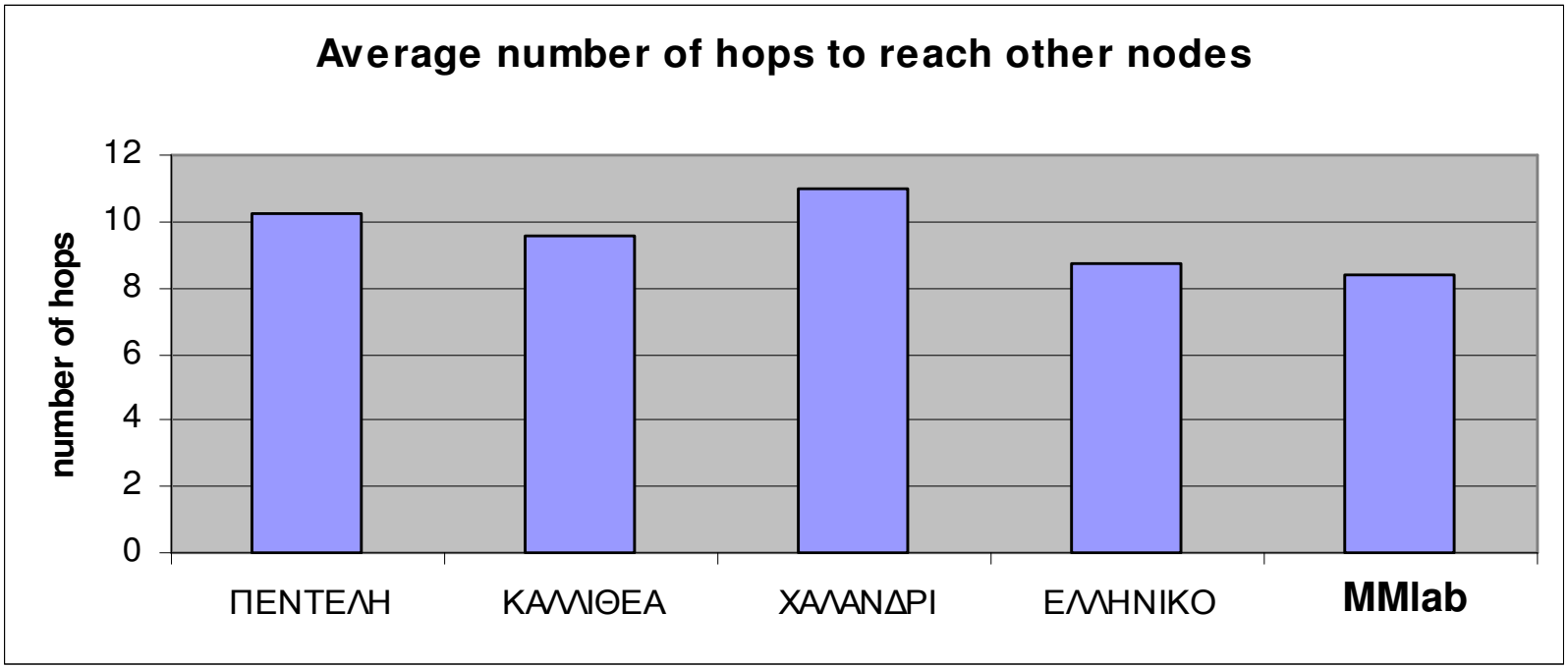
- Expensive broadband connections were one of the major factors that encouraged the creation of AWMN

Distances of the Links

- Most links have distance of about 1km
- Shortest link 8m
- Longest link 124km (!)
- Power is within bounds (20dBm)
- Some links extend to neighboring cities



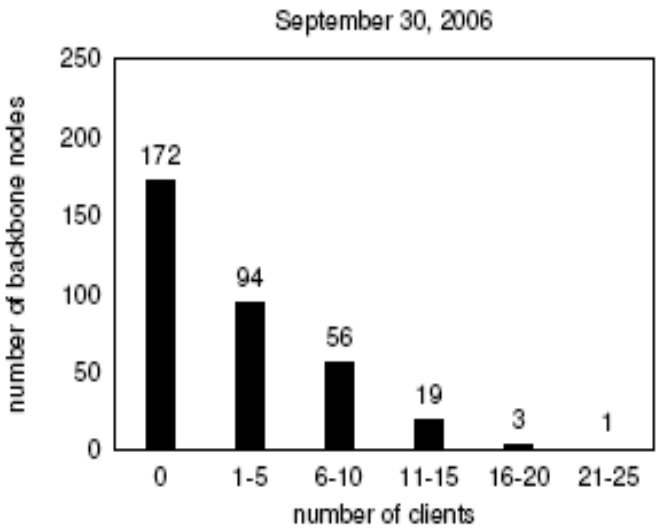
Diameter of the Network

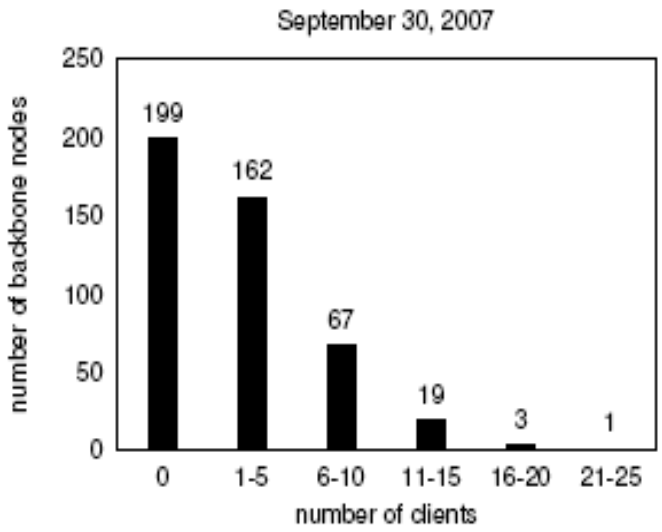


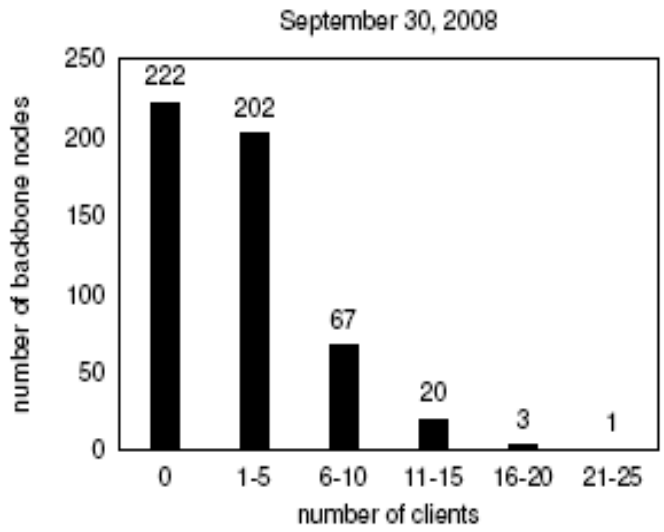
- We ran traceroute commands from 5 different spots in Athens
  - **Diameter based on our traceroute is 9,5**

- Diameter was calculated according to the links registered in WiND
  - Diameter based on WiND is 8,2
  - Maybe more accurate, because it takes into account every link

Distribution of Number of Clients (per Backbone Node)



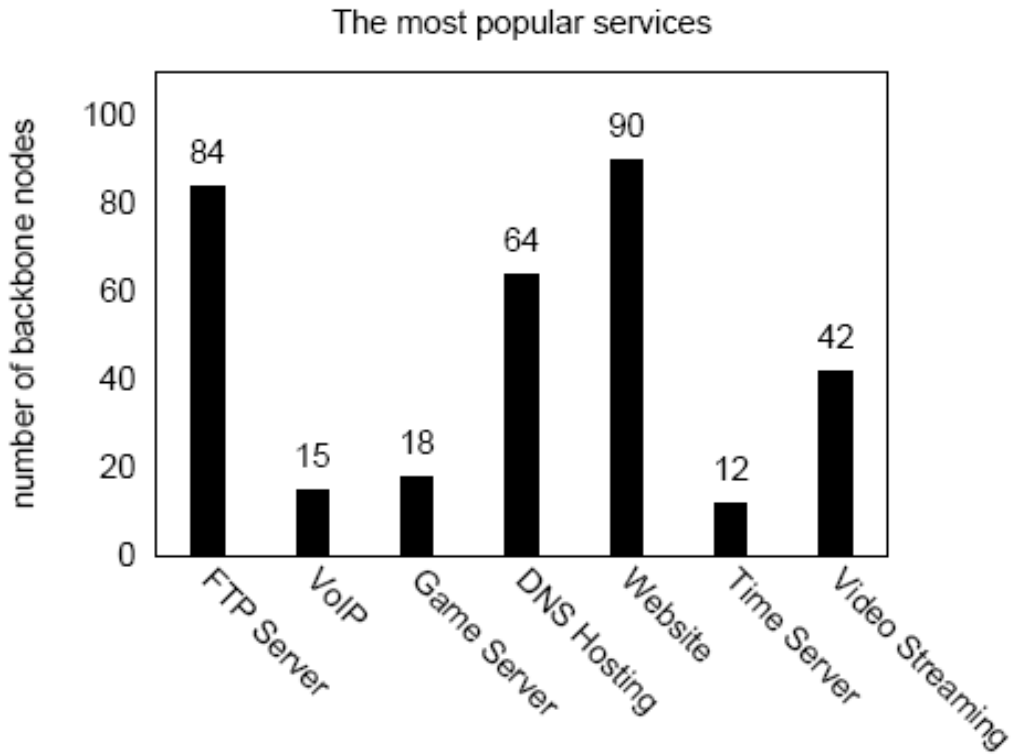


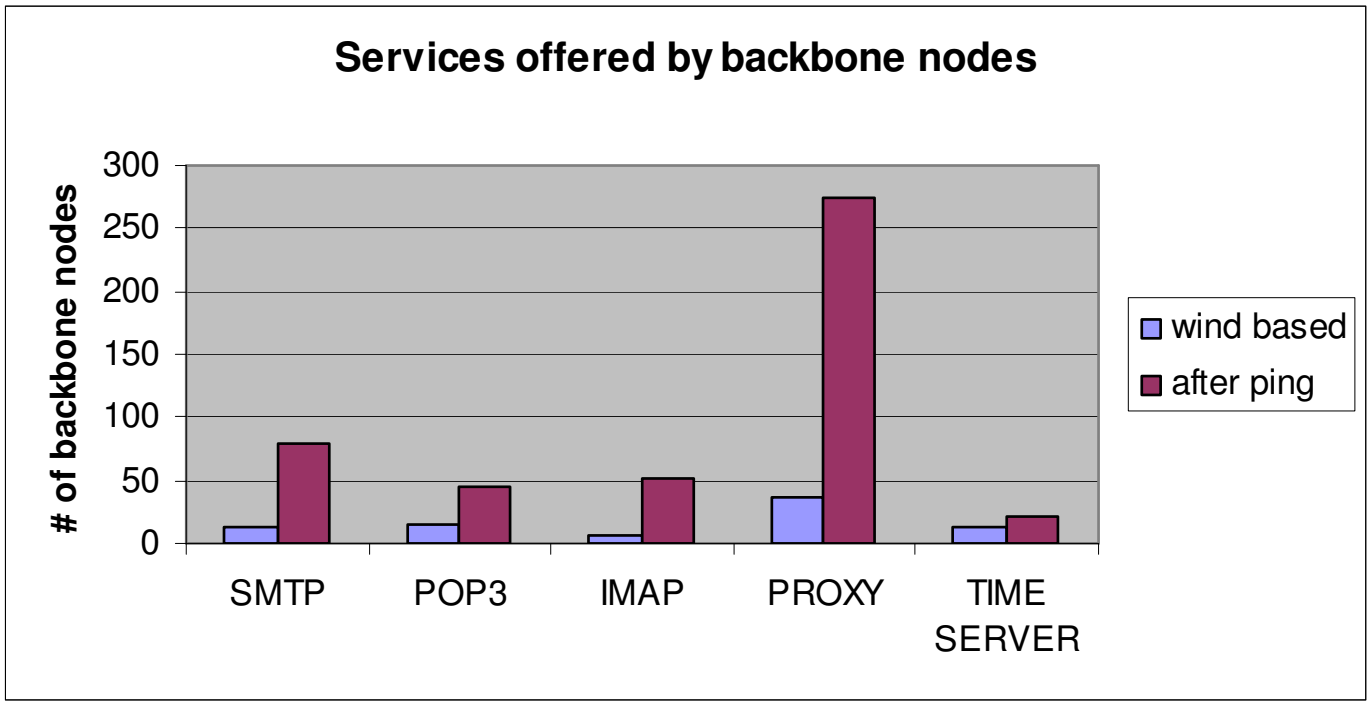


- Many backbone nodes do not support any clients
  - Client nodes seen as not contributing much to the network
  - They increase its size and are potential future backbone nodes

Most Popular Services

- We examined whether some of the registered services are indeed provided
- We noticed that the number of nodes that indeed provide a service is larger than the number registered in WiND





- Proxy service (when a node shares its fixed broadband connection with the rest of the network) is not always for public use

Who runs a WCN?

- **Volunteers**
  - Free interconnection
  - Bypassing wired ISPs
  - Tech-savvy Wi-Fi enthusiasts
- **State initiatives**
  - Municipalities offer Wi-Fi access at low/no cost
  - Athens Wi-Fi, Wireless Philadelphia, The Cloud (London)
- **Private companies**
  - Mediation services for the creation of Wireless Communities
  - FON, NetShare
  - ‘Micro-WISPs’ share Wi-Fi for profit, company may get a share

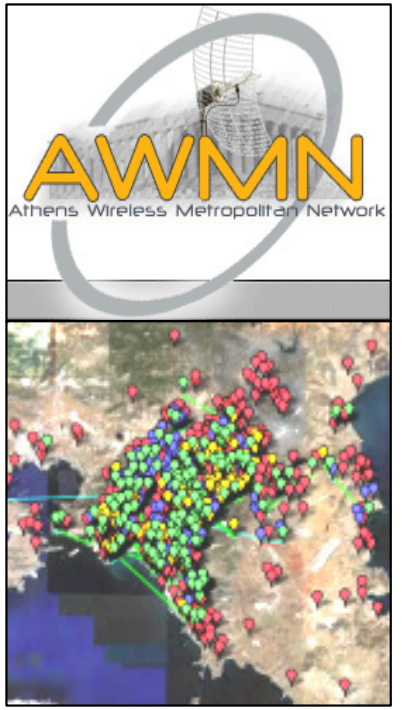
WCN Operation

- Incentives for participation
  - Altruism – “Warm glow” effect
  - Promise of Wi-Fi access when mobile
- Enforcing contribution and compliance
  - Implicit or explicit rules in the community
  - (Fear of) **exclusion**
    - PtP link maintenance: “**tit-for-tat**”
    - Exclusion is easy for mesh → isolate a node by tearing down all links to it
- Building reputation
  - Contributing to collective knowledge/expertise
  - Contributing to the routing process
    - Usually nodes with many interfaces – “hubs”
  - Senior community members have better standing

W(LA)N / Wi-Fi Technology of Yesterday… Tomorrow?

- Access bandwidth: 11-54 Mbps (IEEE 802.11a/b/g)
- Backhaul bandwidth
  - Internet connections: DSL now up to **10s** Mb/s
  - Wireless Community Networks: 54 Mb/s backbone in AWMN
- Wi-Fi phones





- uP W(LA)Ns: An **alternative to** (Telecom) **cellular**?
  - Faster
  - < max. RF power: 100 –200 mW
  - Handovers still an issue
    - but not a problem for **low-mobility** video, audio, browsing

Sharing Wireless Access P2P-style

Wireless Networks & their Backhaul
… have Excess Capacity (when there is no excessive interference)

- Technically, we could share them, however:
  - Direct and indirect costs in sharing
    - unimportant: power, equipment depreciation, BW...
    - **Security** attacks
    - **Legal** issues/exposure
    - Exposure to **radiation**...
  - If WLAN owners rational → no one shares
  - Most private WLANs are secured (closed)

- Need **incentives**

- Payments: a standard approach
  - WLAN aggregators
  - Rely on subscriptions, pay-as-you-go schemes
  - Revenue sharing with WLAN owner
    - Focus on public venues (Boingo, iPass)
    - Focus on residential WLANs (Netshare, **FON**)

… more on FON (http://fon.com)

Our approach: sharing Wi-Fi P2P-style

- P2P Wireless Network Confederation (P2PWNC)
  - A Wi-Fi sharing community
- Rely on reciprocity
  - Users set up their APs for public access
  - Get access to other peers' APs when mobile
  - Access opportunities and QoS proportional to their contribution
- No central authorities
  - Users identified by self-certified public-private key pairs
- Accounting based on the exchange of digital "receipts"
  - Receipt: proof of transaction signed by client
  - Distributed accounting: each peer stores receipts
- Implementable on common WLAN equipment
  - Linux-based AP
  - Smartphones, PDAs

Peer-to-Peer Incentives Literature

i. Tie consumption to contribution, relying on:
   - Central bank, which issues community currency [1]
   - Distributed bank, which keeps track of accounts [2]
   - Tamperproof modules, which enforce reciprocity [3]
   - Simple Tit-For-Tat [4]

ii. Fixed contribution scheme, properties shown in [5]

[1] B. Yang and H. Garcia-Molina, PPay: micropayments for peer-to-peer systems, 10th ACM Conference on Computer and Communications Security (CCS'03), Washington, DC, 2003.

[2] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, KARMA: a secure economics framework for P2P resource sharing, 1st Workshop on Economics of Peer-to-Peer Systems (p2pecon'03), Berkeley, CA, 2003.

[3] L. Buttyán and J.-P. Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks, *ACM/Kluwer Mobile Networks and Applications*, vol. 8, no. 5, 2003.

[4] R. Axelrod and W. D. Hamilton, The evolution of cooperation, *Science*, vol. 211, 1981.

[5] C. Courcoubetis and R. Weber, Incentives for large peer-to-peer systems, *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 5, 2006.

Peer-to-Peer Incentives: Requirements

1. Central bank
   - Requires a central authority
2. Distributed bank
   - Requires altruists: to form overlay network, to hold accounts
3. Tamperproof modules
   - Requires trusted hardware/software
4. Tit-For-Tat
   - Requires permanent IDs, repeat interactions

Whitewashing [6] and Sybil attacks [7]: problem for all schemes

[6] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, **Free-riding and whitewashing in peer-to-peer systems**, *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 5, 2006.

[7] J. Douceur, **The Sybil attack**, 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), Cambridge, MA, 2002.

Our Requirements

The Peer-to-Peer Wireless Network Confederation scheme:

1. Must assume rational peers—at all layers
2. Must be implementable on common WLAN APs
3. Must not rely on authorities, therefore:
   - ✓ Must not rely on central servers, super-peers
   - ✓ Must not rely on tamperproof modules
   - ✓ Must assume IDs are free and that anyone can join, and must penalize newcomers—proven unavoidable [8], [9]

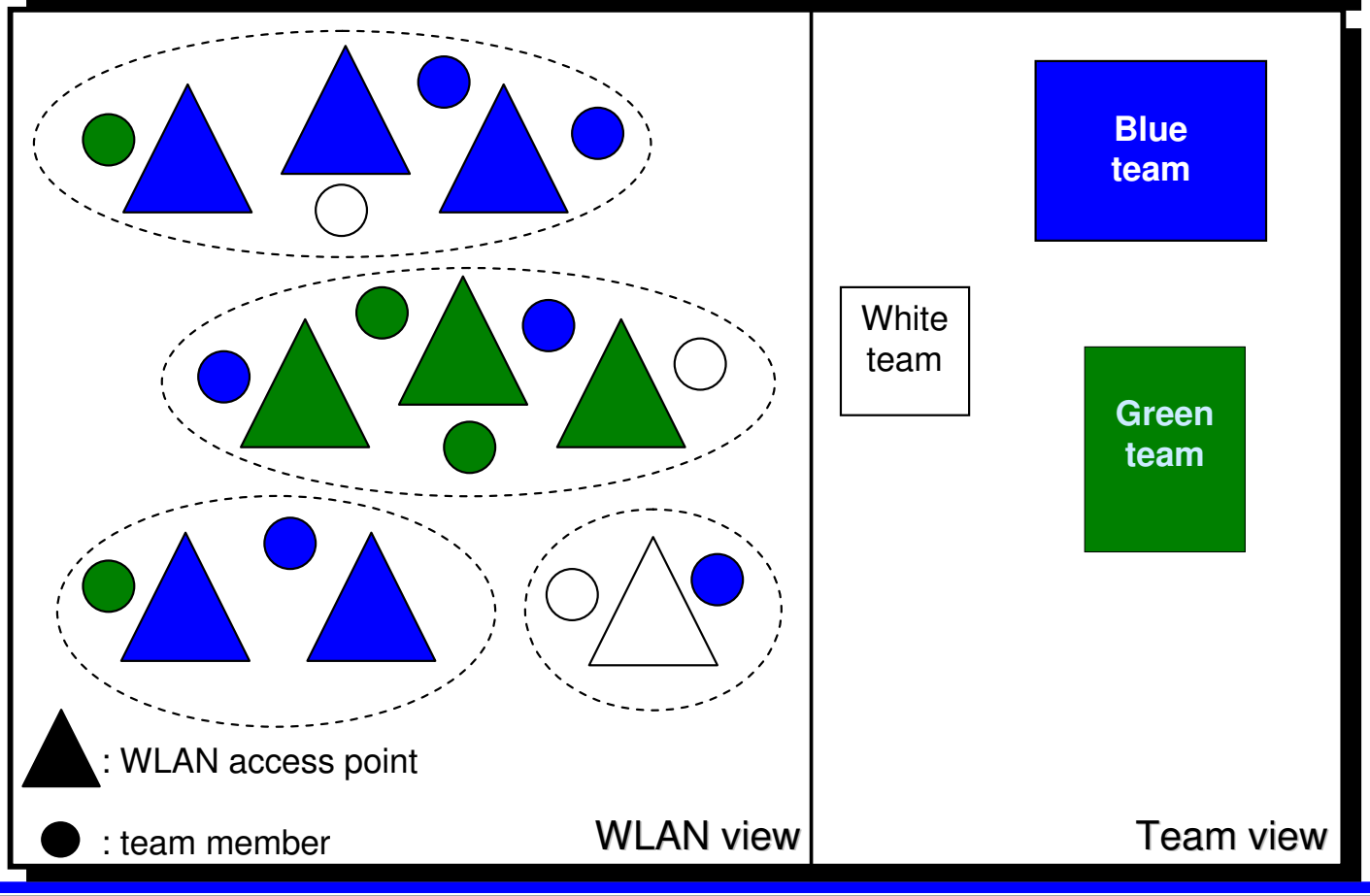
[8] E. Friedman and P. Resnick, **The social cost of cheap pseudonyms**, *Journal of Economics and Management Strategy*, vol. 10, no. 2, 1998.

[9] M. Feldman and J. Chuang, **The evolution of cooperation under cheap pseudonyms**, 7th IEEE Conference on E-Commerce Technology (CEC), Munich, Germany, 2005.

The Basic Idea of the P2PWNC

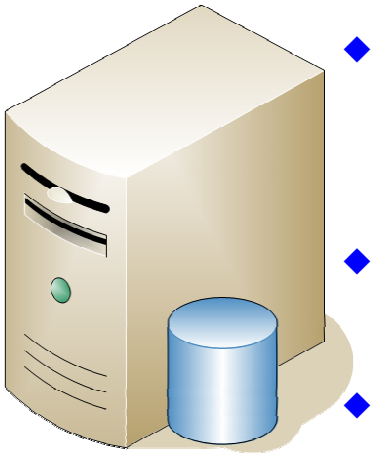
P2PWNC: An incentives-based P2P system

- Teams provide WLAN access to each other
- Teams should provide in order to consume



System Model

- P2PWNC Team/Peer
  - Team ID: public-private key pair
  - Team founder and team members
  - Member IDs and member certificates
    - No PKI required



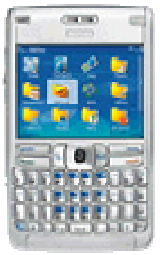
- Team/Peer components
  - P2PWNC clients, storing:
    - Member certificate
    - Member private key
  - P2PWNC APs, storing:
    - Team public key
  - Team server, storing:
    - Team receipt repository

Member certificate

Team public key

Member public key

Team signature



P2PWNC Receipts

P2PWNC receipts

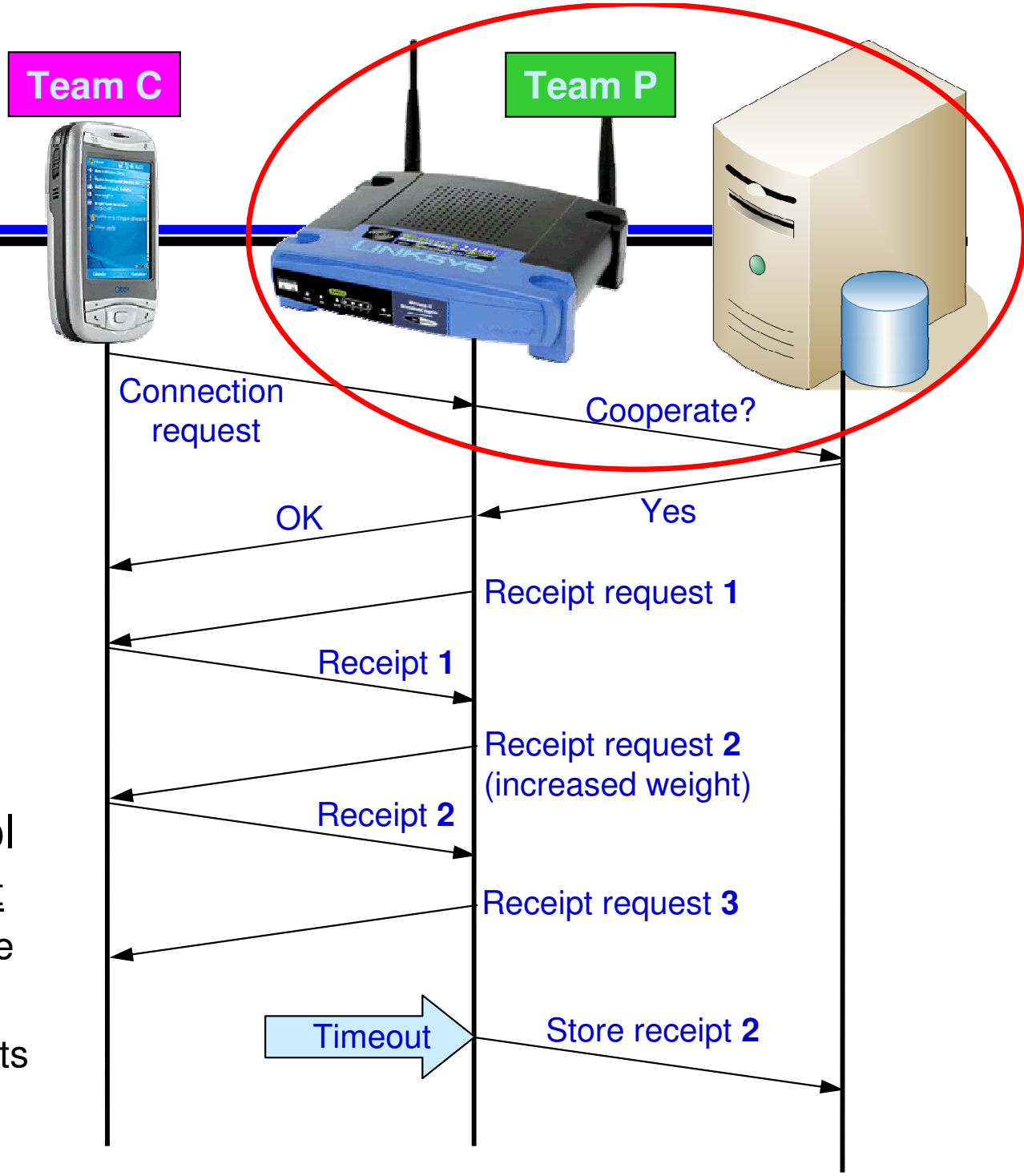
- Proof of prior contribution

Provider public key
Consumer certificate
Timestamp
Weight (bytes)
Consumer signature

Receipt generation protocol

The only time two teams interact

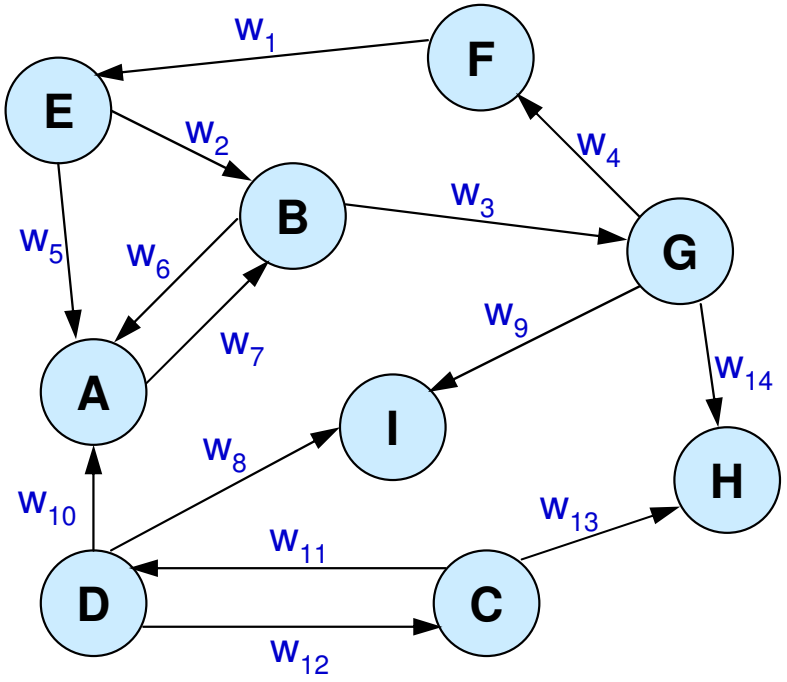
1. Consumer presents certificate
2. Provider decides
3. Provider **periodically** requests receipt
4. Consumer departs



The Receipt Graph

A logical graph

- Vertices represent team/peer IDs
- Edges represent receipts
- Edges point **from** consumer **to** contributor (they **represent 'debt'**)
- Edge weight = sum of weights of corresponding receipts



Possible manipulations

- A peer **can** create many vertices
- A peer **can** create many edges starting from these vertices
- A peer **cannot** create edges starting from vertices he did not create
- A peer **cannot** change the weights on edges

Temporarily, for convenience, assume that a central server exists, which stores the entire receipt graph (global, full view)

Cooperation Strategies

Each one:

- Uses a different **decision algorithm**
  - Input: the receipt graph
  - Output: a decision of whether to provide service or not
- May use a different **gossiping algorithm** (in the decentralized case)
  - Different ways to choose the receipts that roaming members carry
- May use a different **bootstrap algorithm**
  - New teams need to provide before starting to consume
  - For how long, and to whom?

Specific decision algorithms include:

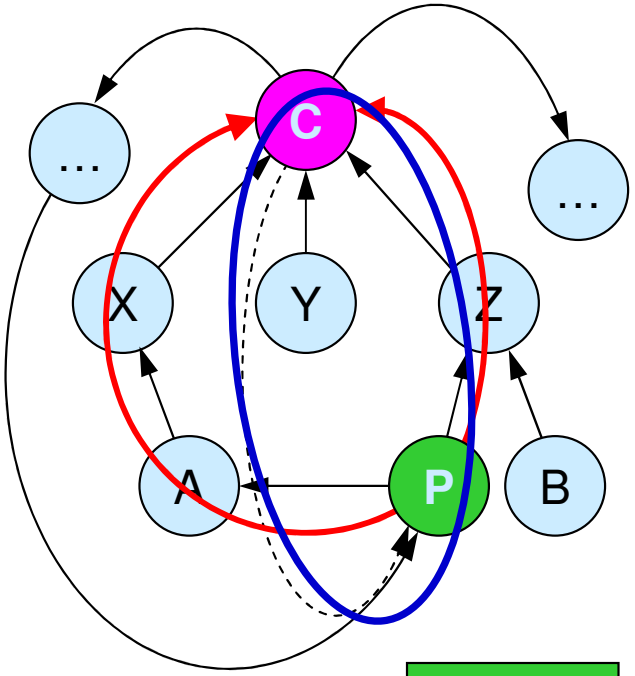
- **NWAY** (assumes unit weights on receipts)
- **Maxflow** (originally suggested by Feldman, Lai, Stoica, Chuang, "Robust Incentive Techniques for P2P Networks," ACM EC'04)
- **GMF: Generalized Maxflow**

Progressively more robust against double-spending and collusion

Maxflow-based Decision Rule

- What if a prospective consumer **C** appears at the root of a tree of receipts?
  - All IDs and **receipts could be fake**!
- What if the prospective contributor **P** sees **himself** in the tree?
  - **P** owes direct or indirect debt to **C**
  - Potential for multi-way exchange, like in [10]
- Find all direct and indirect debt paths [11]
  - Maxflow from **P** to **C**
- Find also direct and indirect debt paths from **C** to **P**
  - Feldman et al. [11] propose that **P** cooperates with probability:

$$p = \min\left(\frac{mf(P \to C)}{mf(C \to P)},\ 1\right)$$



[10] K. G. Anagnostakis and M. B. Greenwald, Exchange-based incentive mechanisms for peer-to-peer file sharing, 24th International Conference on Distributed Computing Systems (ICDCS 2004), Tokyo, Japan, 2004.

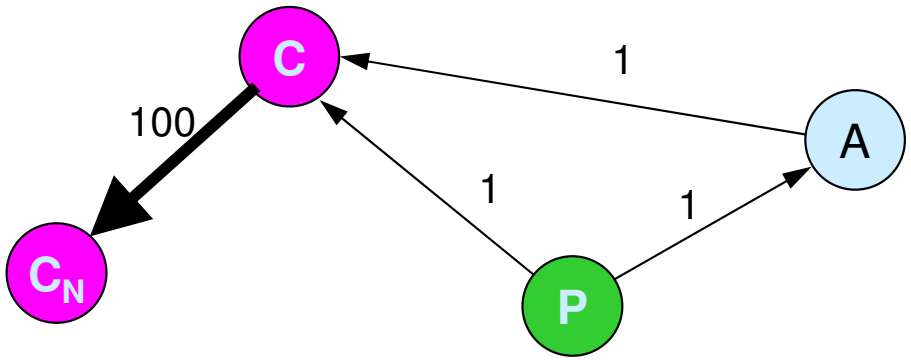
[11] M. Feldman, K. Lai, I. Stoica, and J. Chuang, Robust incentive techniques for peer-to-peer networks, ACM Conference on Electronic Commerce (EC'04), New York, NY, 2004.

Two Problems with Maxflow-based Decision

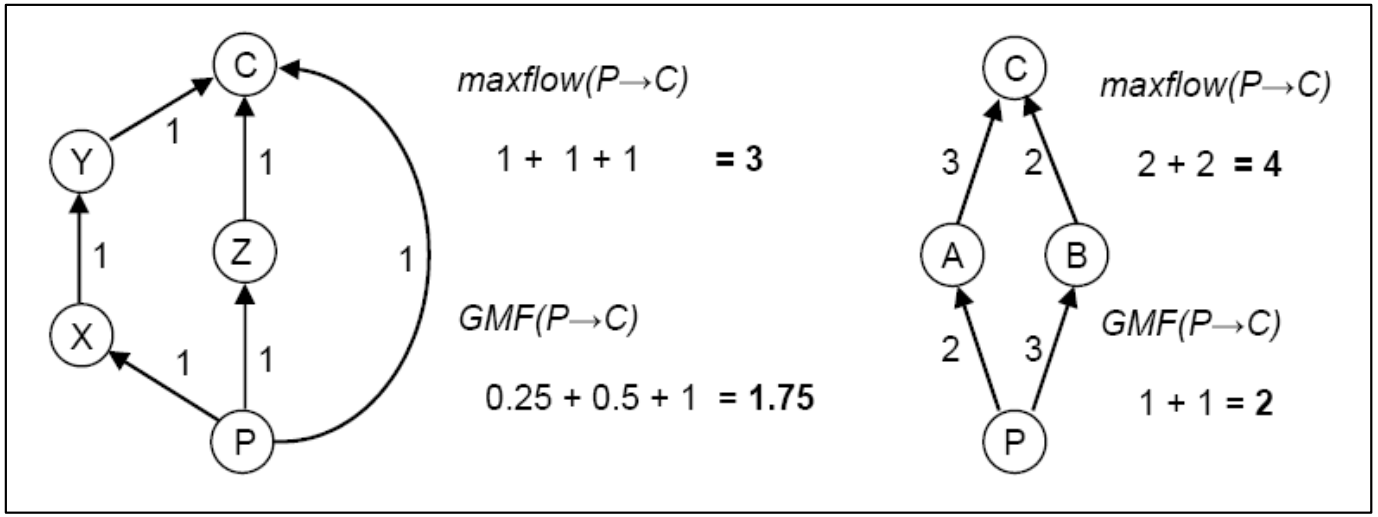
1. Cooperate with a probability?
   - Encourages continuous re-requests
   - Answer: Interpret fraction as service differentiation

$$p = \min\left(\frac{mf(P \to C)}{mf(C \to P)},\ 1\right)$$

2. Problem in denominator
   - Attacker can always get best service with small maxflow in the numerator as long as he 'erases debt' using new ID
   - Answer: GMF heuristic



P2PWNC Reciprocity Algorithm



- First, work around 'erase debt' attack with Generalized Maxflow (GMF)
  - GMF heuristic: examines directness of debt
  - Punishes those who 'push' good reputation away

$$r_1 = \min\left(\frac{mf(P \to C)}{mf(C \to P)},\ 1\right)$$

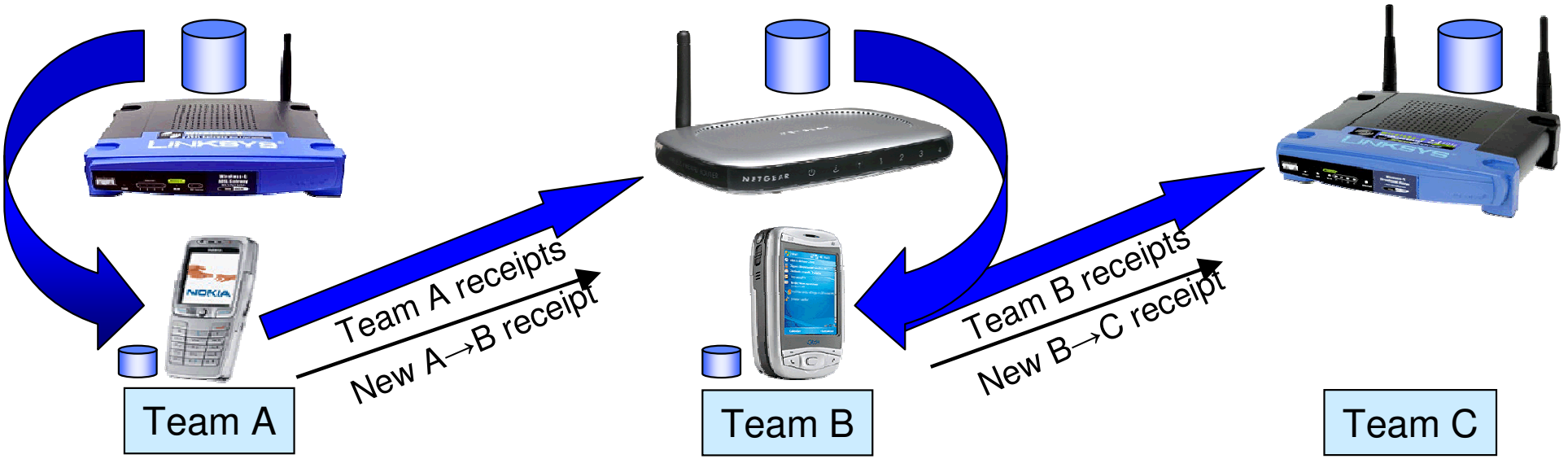
$$r_2 = \frac{GMF(P \to C)}{gmf_{avg}}$$

$$gmf_{avg} \leftarrow gmf_{avg}\ a\ +\ GMF_{new}\ (1-a)$$

- Subjective Reputation Metric (SRM)
  - P2PWNC APs use this to guide cooperation decisions

$$SRM_{P \to C} = \min(1, r_1\, r_2)$$

Gossiping Algorithm



- Realize the receipt graph without overlays or central servers (idea based on [12])
  - Server receipt repositories
  - Client receipt repositories
- Phase 1: Client update
  - Get fresh receipts from team
- Phase 2: Merge
  - Show these receipts to prospective contributors
  - Contributor merges these receipts with 'oldest-out' replacement

[12] S. Čapkun, L. Buttyán, and J.-P. Hubaux, Self-organized public key management for mobile ad hoc networks, *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, 2003.

Bootstrap Algorithm

- New teams/peers must contribute to the system first
  - Maxflows **from** and **to** a new ID are zero
    - New peer appears as free-rider to others
    - Others appear as free-riders to new peer
  - Cooperate with everyone at first
    - Including free-riders…
- For how long?
  - The 'patience' heuristic
    1. Start to contribute
    2. At the same time, try your luck as consumer
    3. After a number of successful consumptions, start to use the reciprocity algorithm
  - Other simple heuristics possible

P2PWNC Protocol

- 7 messages total: 4 inter-team, 3 intra-team
- Support for both ECDSA and RSA signatures

```
CONN P2PWNC/3.0
Content-length: 164
Algorithm: ECC160
BNibmxStfJlod/LnZubH6pzWHQqKyZFcSMjnZurmTe4KjCRkllhV93MEegPvCsxz
2oe/hqevoPSrwO1JLO/36J8HTIeyeKQqTCfx+EPxweAvYC/ZFb8URLa2faIbvSgD
3lm6Wa1S4cYlSWeSNmFzS/ebDFfzakqNSEs=
```

Member certificate (Base64 encoded)

```
CACK P2PWNC/3.0
Content-length: 0
Timestamp: Tue, 16 May 2006 17:26:41 +0000
```

Session timestamp (RFC 3339 compliant)

```
RREQ P2PWNC/3.0
Content-length: 56
Algorithm: ECC160
Weight: 6336
BEXn8BHHViQ/YMyF2ny+KaI4YXz+W60uED7R8wZefDznyncfQKggzAc=
```

Relayed traffic thus far (bytes)

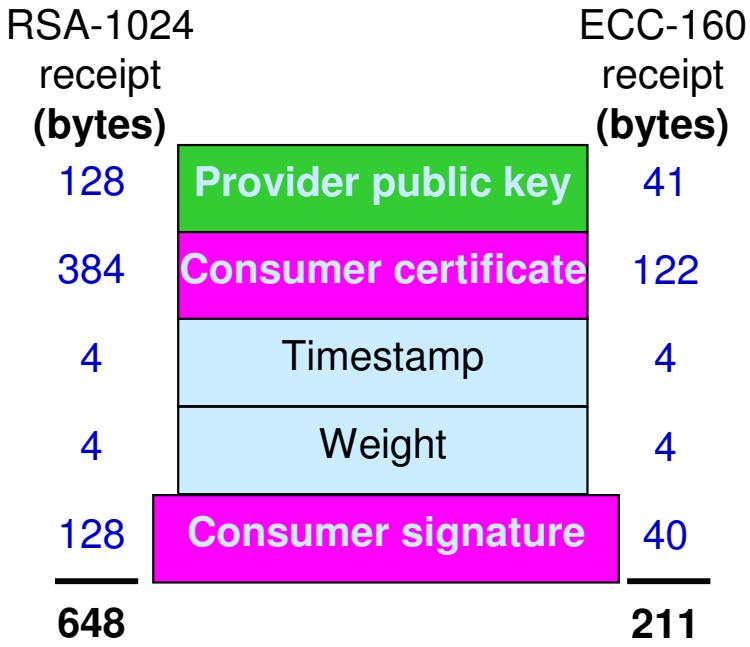
Contributing team public key

```
RCPT P2PWNC/3.0
Content-length: 272
Algorithm: ECC160
Timestamp: Tue, 16 May 2006 17:26:41 +0000
Weight: 6336
BNibmxStfJlod/LnZubH6pzWHQqKyZFcSMjnZurmTe4KjCRkllhV93MEegPvCsxz
2oe/hqevoPSrwO1JLO/36J8HTIeyeKQqTCfx+EPxweAvYC/ZFb8URLa2faIbvSgD
3lm6Wa1S4cYlSWeSNmFzS/ebDFfzakqNSEsERefwEcdWJD9gzIXafL4pojhhfP5b
rS4QPtHzBl58POfKdx9AqCDMBxRoGALKJSJYYXlsrwtiyZJKvPlU5B3lWrFuL25P
d+kv2iMVRElXk/4=
```

Signed receipt

Public Key Cryptography: Time, Space, Trade-offs

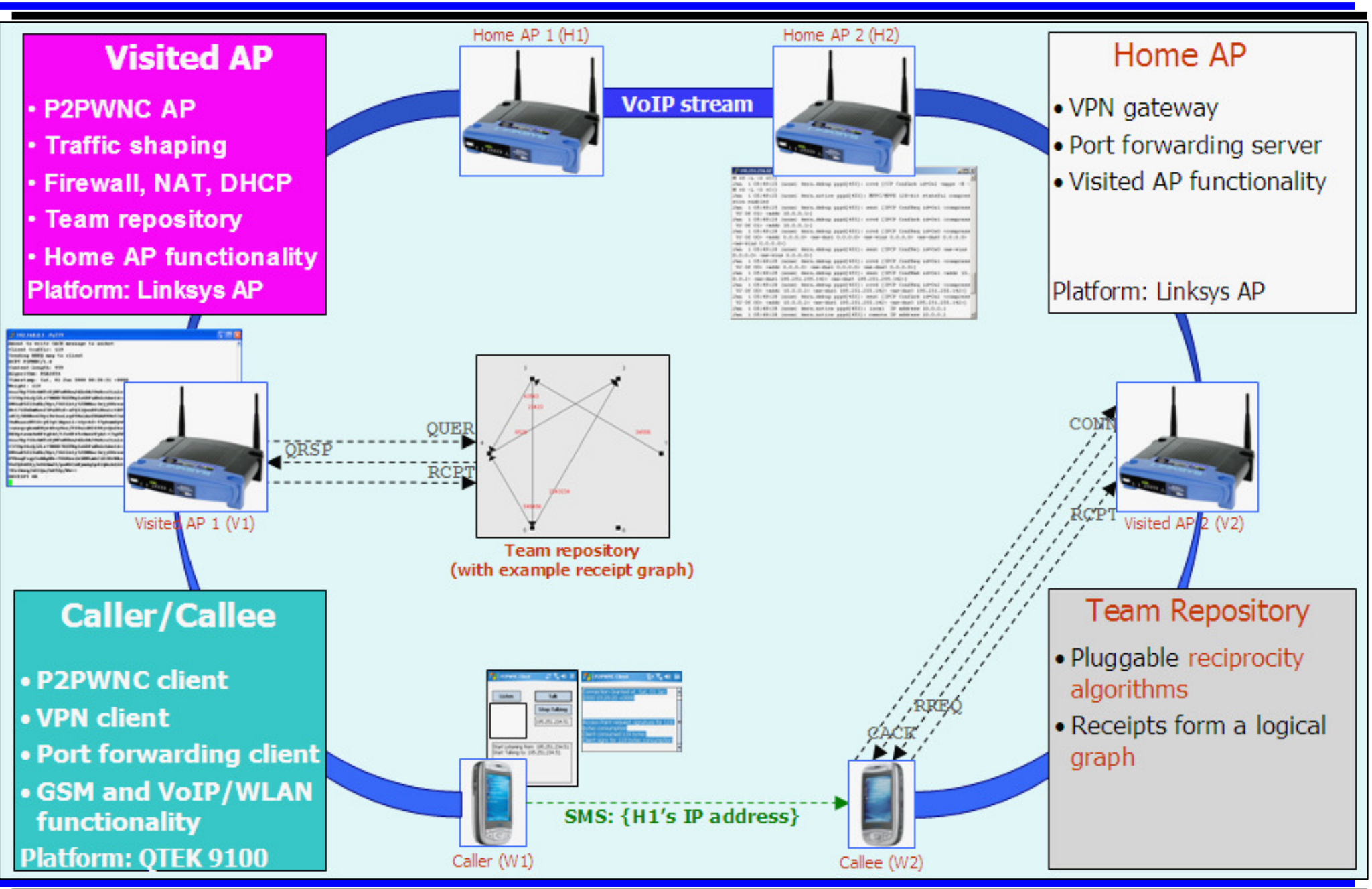
	Athlon XP 2800	Linksys WRT54GS
CPU speed	2.08 GHz	200 MHz
CPU type	AMD Athlon XP 2800	Broadcom MIPS32
RAM	512 MB	32 MB
Storage	60 GB HD	8 MB Flash, 32 KB NVRAM
Operating system	Linux kernel 2.4.18 (Red Hat Linux 8.0)	Linux kernel 2.4.18 (Broadcom specific)



Signing	Athlon XP 2800		Linksys	
Bit length (RSA/ECC)	RSA (ms)	ECC (ms)	RSA (ms)	ECC (ms)
1024/160	**9.0**	**1.3**	**300.6**	**20.3**
1536/192	**25.9**	**1.2**	**655.6**	**18.5**
2048/224	**47.3**	**1.4**	**1529.0**	**23.4**
3072/256	**149.1**	**1.7**	**3939.0**	**73.1**

Verification	Athlon XP 2800		Linksys	
Bit length (RSA/ECC)	RSA (ms)	ECC (ms)	RSA (ms)	ECC (ms)
1024/160	**0.4**	**6.5**	**12.3**	**114.7**
1536/192	**0.8**	**6.0**	**21.4**	**99.9**
2048/224	**1.3**	**7.1**	**37.9**	**135.7**
3072/256	**2.8**	**8.6**	**75.3**	**453.0**

Demos @ IEEE INFOCOM'06, ACM MobiSys'06



Services and Applications on top of P2PWNC

- VoIP over P2PWNC
- Multimedia conferencing
- Secure… private…
  - Using standard network security techniques (VPN tunnels…)
  - Fully distributed implementation

- (Broadband) Internet Access! – the ***Killer*** Application?

- ... “Micro-operators”
  - Trust
  - Reliability, availability
  - Security
  - Privacy (location tracking…)
    - Fully distributed implementation – no authorities
    - Cheap / renewable IDs

Open Issues

- P2PWNC and Wireless Community Networks
- ISP Acceptable Use Policies / Business Models
- Peripheral peers
  - Can expanded teams include them?
  - Or, factor location in receipt weight?
- Extend cost-benefit model
- Collusion among teams, other adversarial strategies
- Mobility
  - Handovers

P2PWNC Summary

- Proposed a P2P system for the sharing of WLANs
  - Fully decentralized
    - Open to all, free IDs
    - No super peers, no tamperproof modules
  - Rational participants
    - No overlay networks, no account holders
  - Minimal protocol
- Proof of concept
  - Promising evaluation results
  - Implementation on common WLAN equipment
- Lessons learned
  - Generalized exchange economies are a good match for electronically mediated P2P communities
  - Each P2P community different: understand the users and the shareable good first (as well as the centralized alternatives)
  - Security and incentive techniques are intertwined

μ-Operators

User Provided Networks

μ-Operators

- Anybody can easily become a (wireless μ-)Operator
  - First time in history...
  - Legal issues...
- But... more interestingly...
  - Reliability, Availability
  - Trust
  - Security
  - Privacy (location tracking…)
    - Fully distributed implementation – no authorities
    - Cheap / renewable IDs
- Business issues
  - ISP Acceptable Use Policies (towards link sharing)
    - Business Models
    - BT alliance with FON
  - entry of ISPs to advanced Cellular market (4G?) with no (further) investment!(?)

Alternative Spectrum Utilization Model …

- Unlicensed spectrum
  - Anyone can become an operator
    - Low entry cost
      - Residential WLAN owners, (W)ISPs, 3G operators, municipalities, etc.
    - Increased coverage (@ broader BW, lower cost)
    - Significantly increased number of operators
      - lawyer driven roaming agreements imparcatical
  - Increased competition
    - Fewer market hijacking phenomena...
    - Wider service offerings
      - Subject to operator interactions and not user priorities
    - Increased interference ⇒ sensing, mitigating
  - Privacy, Security, Trust…
- Open access
  - Without any form of prior contract (subscription)
  - Getting (buying? in kind?) network access in small quanta

Wireless Trends & Challenges (the dream?)

- Broadband Wireless Access
  - over unlicensed & minimally regulated spectrum
  - where competition **and** cooperation are the norm at all scales
- to a true i/Internet [a really distributed system]
  - which needs serious reconsideration/redesign
  - to address non-fully cooperative agents/networks
    - including aspects of exploiting asymmetric information
    - in an automated way (fast decisions, select from set of “contracts”)
- to access or provide a wide array of services
  - including multimedia content generated (and stored) at the edges
  - & all types of secure / anonymous communications
  - & also including a wide variety of devices and attached networks of sensors & actuators
- where the following are important at many layers:
  - Privacy, Security, Trust (reputation), Availability (PaSTA)
- Automated Trust Management
  - becoming a key issue for interconnection and successful interoperation

Cognitive Radio Networks

Interference Sensing & Reporting

The Problem

- Proliferation of wireless networks & devices
- Increased demand for radio spectrum
  - Need for regulation …
- Traditional approach rather inefficient
  - Difficult to find a vacant frequency
  - Competition leads to need for high investments
    - High entry barrier for new operators
    - Long payback time
    - Customers tied to a specific network
      - Often impossible to choose the best price-quality
  - Frequency bands tied to specific technologies
  - Licensed bands
    - temporal & spatial underutilization of the spectrum
  - Unlicensed bands
    - interference

The Role of Cognitive Radio

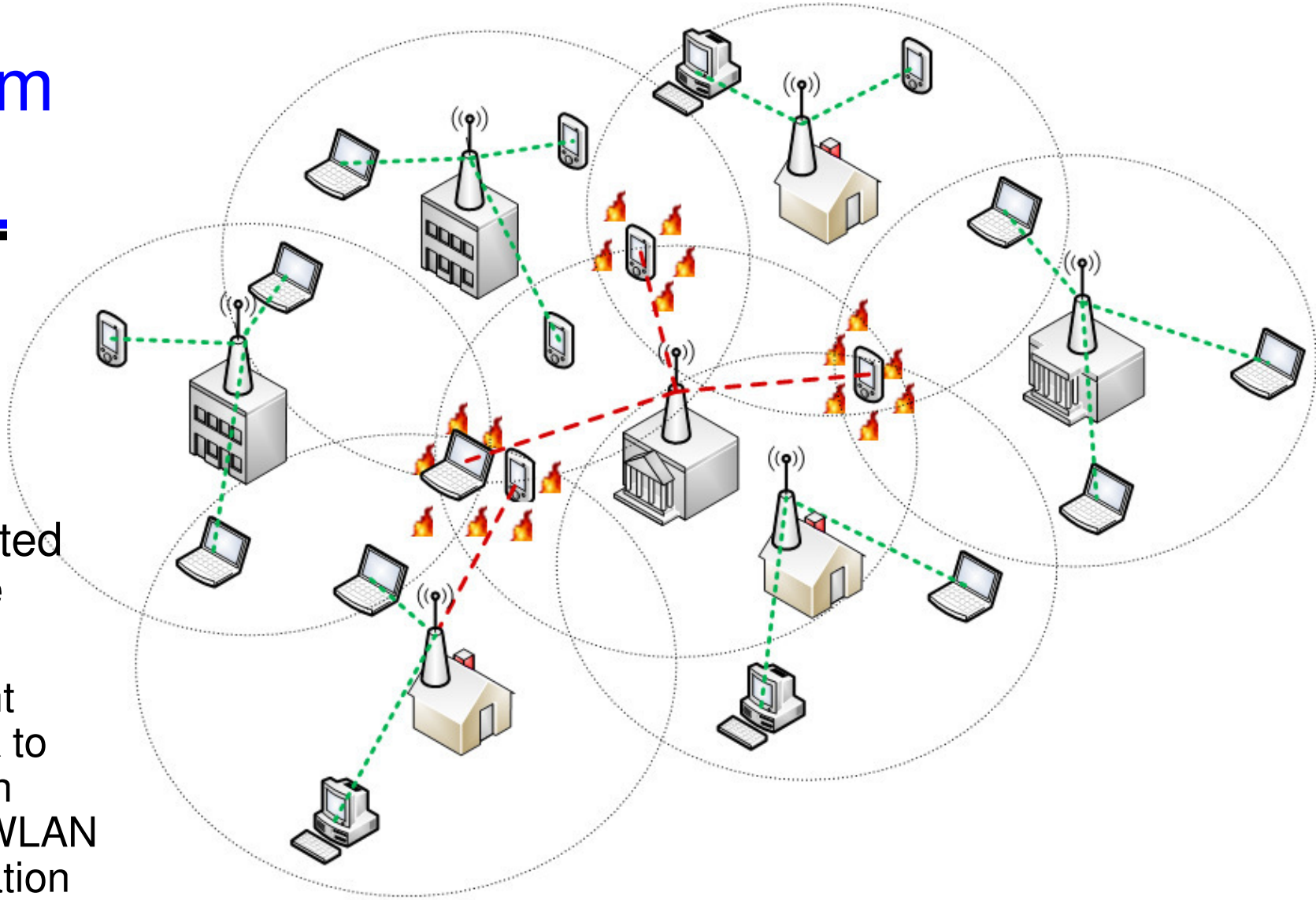
- Interact with the wireless environment
  - Sense, learn and adapt/react
- Historically mostly focused on the Primary/Secondary user model
  - Focus on spectrum underutilization
    - Filling spectrum *holes*
  - Spectrum access priorities
- However…
  - still hard/risky for secondary users/operators
    - primary user priority hinders even the minimum service guarantees
  - primary operator investments still key for growth of wireless networks & services

Dynamic Spectrum Access: Challenges and Goals

- *Spectrum sharing dimensions:* frequency (code), space and time
  - A unified framework considering all dimensions will provide the necessary flexibility (unlicensed spectrum)
- *Primary/Secondary model vs. Open Spectrum Access (OSA)*
  - enable new (μ-)operators to enter the market
- *Centralized vs. distributed (information repositories)*
  - Outer/inner feedback loop
  - Goal: a low overhead reporting system
- *Cooperative vs. non-cooperative spectrum sharing*
  - Design incentives that will lead to a high degree of cooperation between competing spectrum users
- *Game theoretic modeling of spectrum sharing*
  - Various degrees of cooperation
    - Expressed by the amount and quality of the available information
  - Translation of a game-theoretic model to a practical system

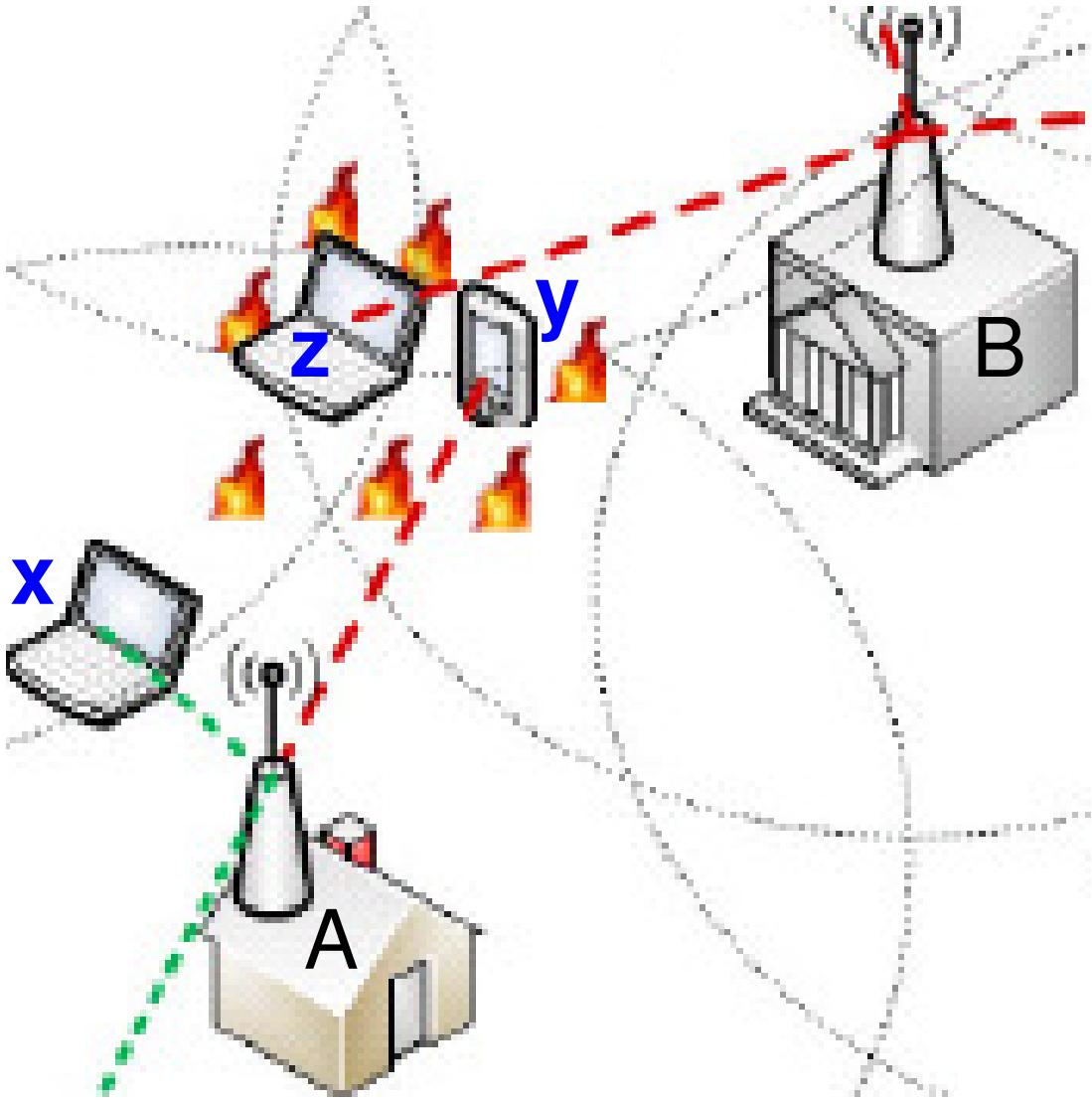
Spectrum Sharing

- Open Spectrum Access
- Client-assisted interference mitigation
  - Use client feedback to decide on optimal WLAN configuration
  - Can reveal *hidden interference* due to hidden terminals



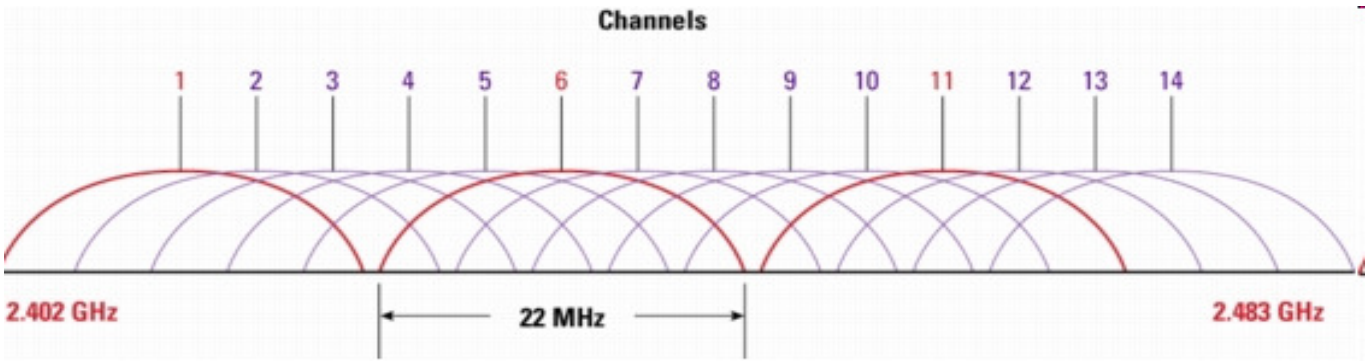
Competition and Cooperation

- Convince **A** to limit power
- Probably to **B**'s advantage to serve **A**'s client (**y**) directly (at no cost to **A**)
  - y far from A
    - low rate => long channel time
  - y closer to B
    - Can be served by B at high(er) rate => small(er) channel time



Interference

- Contributing...
  - IEEE 802.11 channels not truly orthogonal
    - 802.11b/g: 3 interference-free (non-overlapping) channels

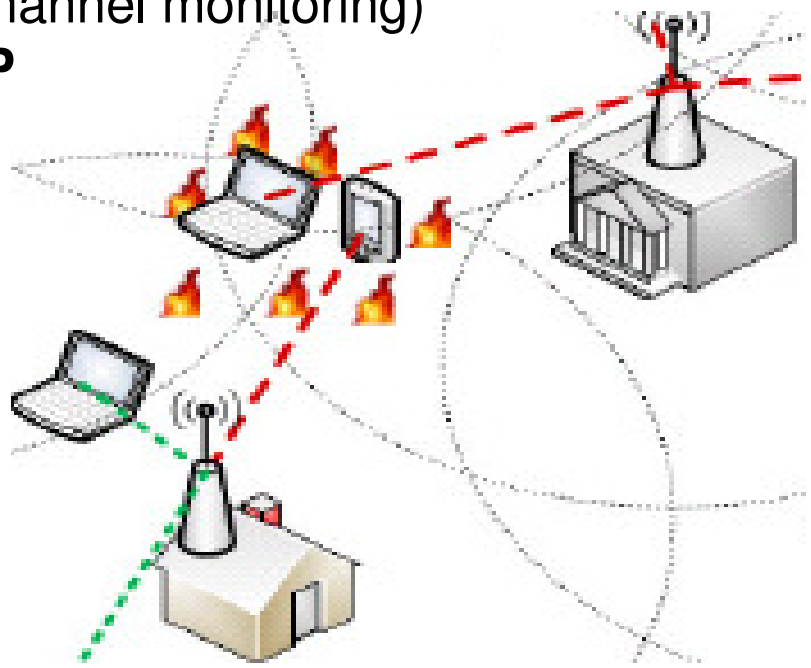


- Interference detection

- Interference mitigation
  - channel selection,
  - **power control**, coverage,
  - directional antennas, ...

Detecting Interference / Spectrum Monitoring

- AP-centric schemes
  - Sense spectrum usage at the AP site
  - Easier to control/manage
  - May require additional Wi-Fi interface (for channel monitoring)
  - Fail to capture **interference beyond the AP**
    - due to “hidden” terminals
    - probably the most important

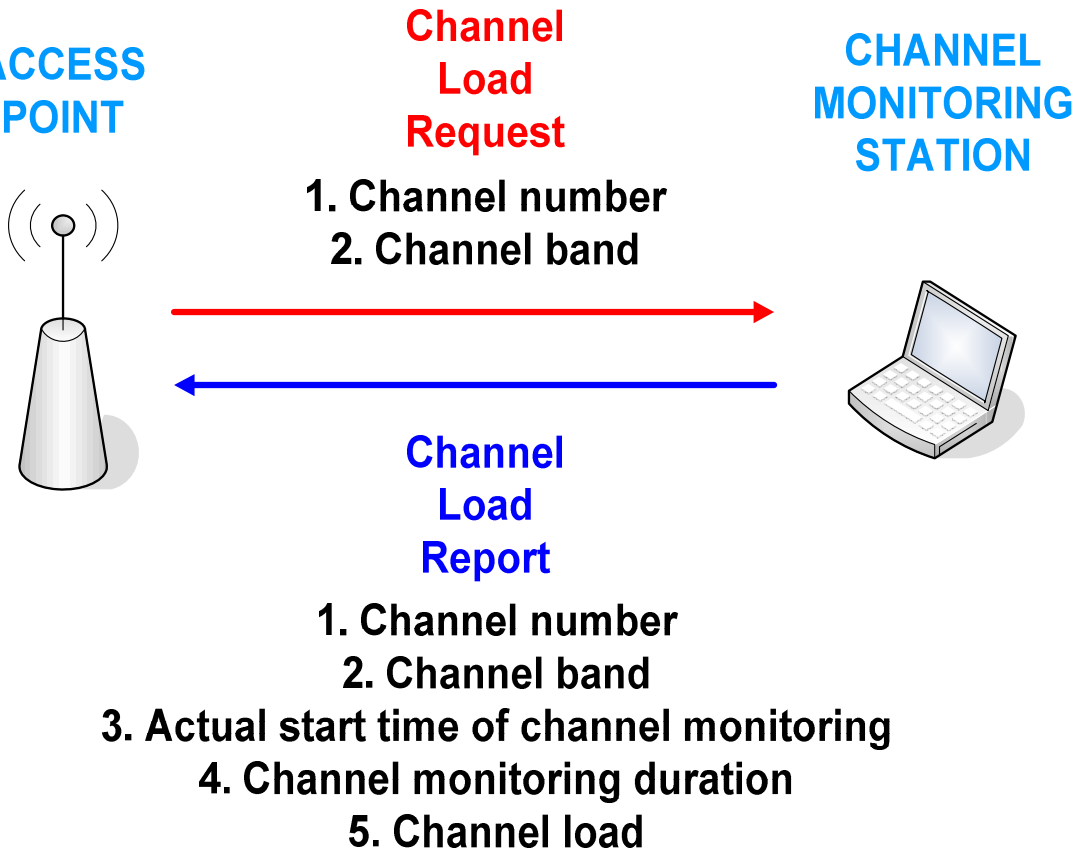


- Client-based schemes
  - Clients periodically monitor channel usage
  - Report to APs (or other control entity)
  - Reveal more information
    - capture user-perceived interference
  - Trustworthy reports?
  - Monitoring overhead?

- Ad hoc sensing devices / special purpose sensors
  - Carefully placed?

IEEE 802.11k: Radio Resource Measurements

- Specifies types of ***radio resource information*** to measure and the associated request and report mechanisms
  - Provides information to discover the best available access point
  - Load Balancing
  - Improve the way traffic is distributed within a network



- **Mangold & Berlemann**: "IEEE 802.11k: Improving Confidence in Radio Resource Measurements," IEEE PIMRC 2005.
- **"Optimizing the Channel Load Reporting Process in IEEE 802.11k-enabled WLANs"**, Panaousis, Ververidis, & Polyzos, IEEE LANMAN 2008.

A Proposed Architecture

- Utilization of client-supplied information
  - Outer feedback loop
  - Spectrum usage, service offerings
  - Hidden interference problem …
  - Planning AP deployment
  - Cheap sensors deployed to supply spectrum utilization information
- Adaptive wireless infrastructure
  - Inner feedback loop
  - Interference mitigation
- Service discovery, negotiation and handovers
  - *Direct:* mobile node – AP interactions
  - *Indirect:* user reports

The Proposed Architecture:
Functional Requirements

Mobile Node

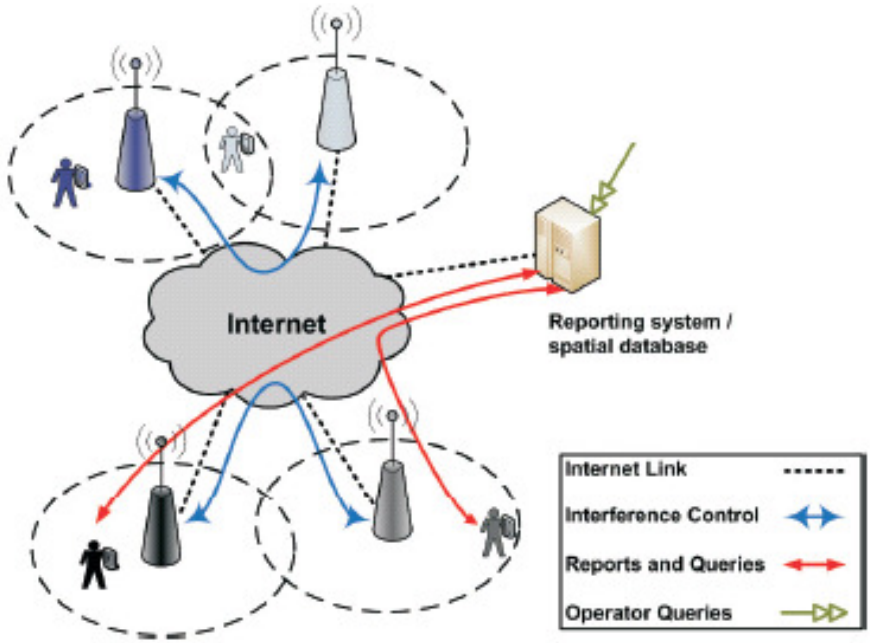
- Spectrum sensing
- Service discovery
- Reporting (especially of *white spots*)
- Spectrum agility
- Secure micro-payments
- Advanced handover capabilities (frequency, air interface, AP, operator)

Reporting System/Spatial Database

- Aggregate reports
- Monitoring
- Provides information on service availability and spectrum usage
  - Operators: *white* spots, interference, etc.
  - Users: coverage, services, etc.

Access Point

- *Announcing*
  - *Spectrum portfolio*
  - *Service capabilities*
- Secure micro-payments
- Interference feedback and reporting
- Interference control
- Handover preparation



A Proposition

- Tackle public wireless access and interference mitigation jointly
  - P2PWNC for mobile Wi-Fi access
  - Client feedback about interference suffered
- Why should a P2PWNC client provide feedback about interference?
  - Offer QoS benefits in exchange
- Will it work?
  - Yes, if it has low overhead for the client
  - Otherwise: clients refuse to report, provide fake feedback

Improved QoS as an incentive for interference reporting

- QoS extensions to the basic P2PWNC scheme
  - Clients get proportional bandwidth to their SRMs…
  - …plus a bonus for the amount of interference reports they provide

Portion of the bandwidth dedicated to P2PWNC users

% of "successful" client reports

- Assume an AP with n visitors. Visitor i gets:

$$B_i = \frac{SRM_i}{\varepsilon + \sum_{j=1}^{n} SRM_j} B_{P2PWNC} + r_i \frac{B_{bonus}}{n}$$

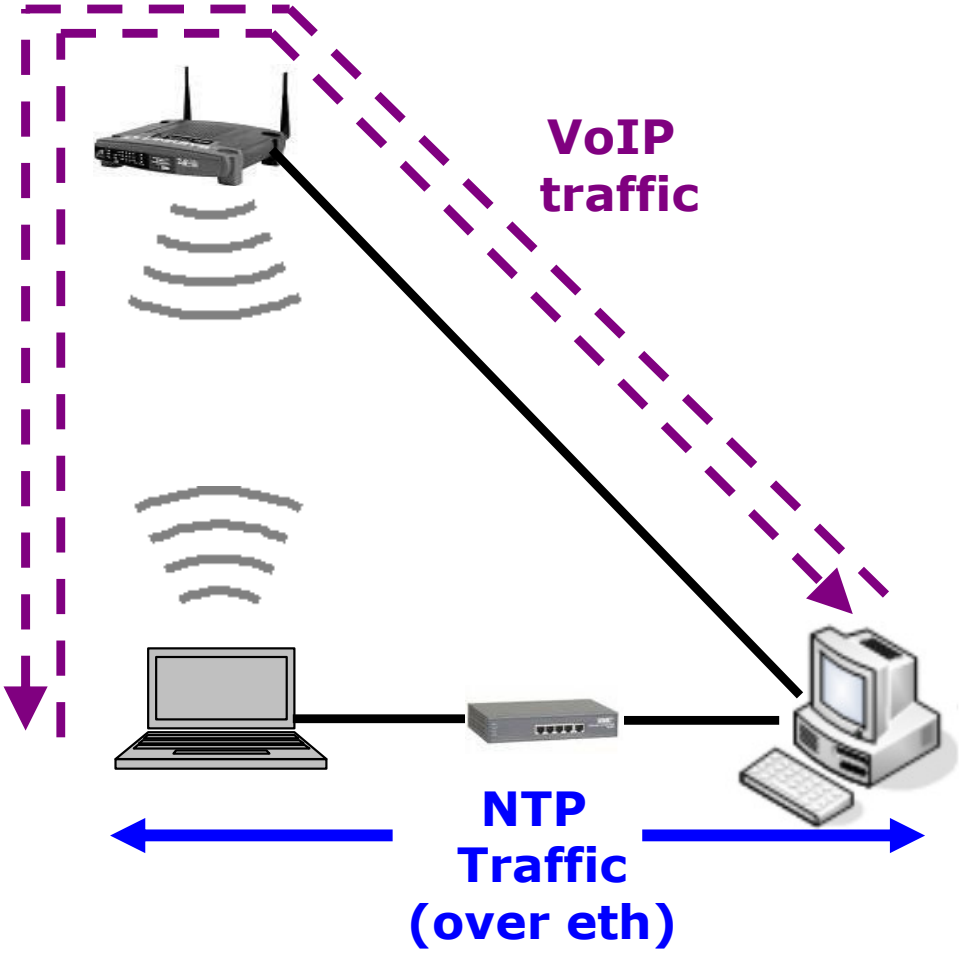
Portion of the bandwidth for rewarding interference reports

Performance Overhead of Spectrum Sensing

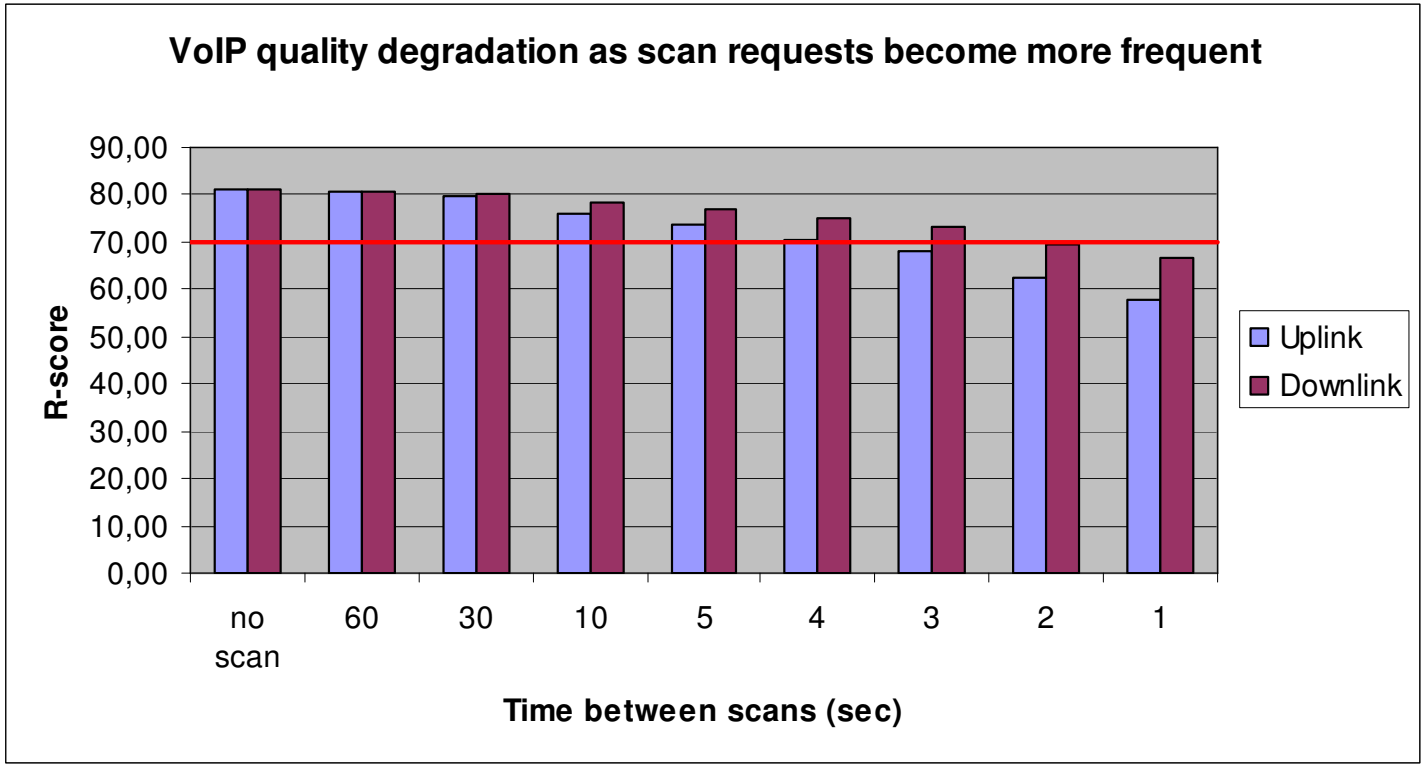
- Stations cannot receive/transmit application packets while scanning
- Active scan on 11 channels: >250msec!
- Overhead depends on report request frequency
- Disincentive for clients to contribute reports
  - Need incentives
    - Bandwidth/QoS bonus?
- But how high is this overhead?
  - …especially for delay-sensitive applications

Measuring the Overhead…

- Purpose: measure VoIP performance degradation due to periodic scanning
  - Experiment with various request frequencies
- Traffic pattern
  - Bidirectional UDP/RTP traffic, 50 packets/sec, 20bytes payload (G.729)
- VoIP quality assessment
  - E-model (R-score/Mean Opinion Score)
  - Based on network-level per-packet measurements (delay, loss, jitter)
- Testbed
  - IEEE 802.11b @ 11Mbps, no RTS/CTS
  - Linksys WRT54GS AP
  - Intel PRO Wireless 2200 card, ipw2200 Linux driver
  - Sync using NTP (over eth interfaces)



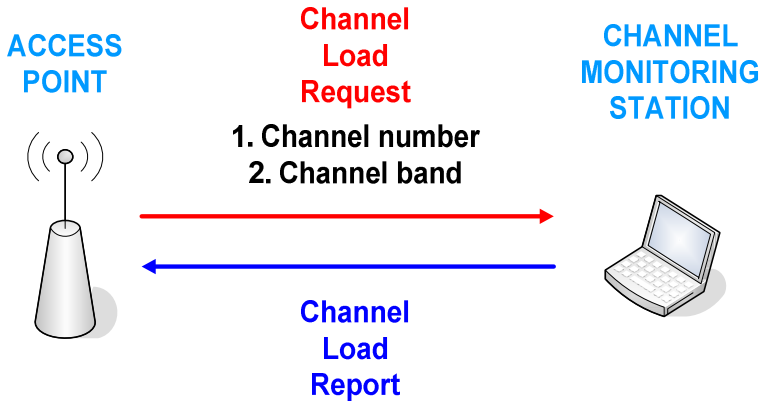
Quantification of Sensing Overhead



- Acceptable quality: R-score > 70
- Moderate scanning frequency (e.g. 2 scans/min) ➔ Minimal QoE degradation
- Negligible mean e2e delay
- Worse quality mainly due to jitter

Open Issues in Interference Detection & Reporting: the ASPECTS project

- Security and reliability
  - How to spot fake reports?
  - Use a client reputation scheme, punish/reward?
  - Use monitors/sensors
    - Where to place them?
    - How many? Who owns/deploys them?
- Model and study incentives mechanism
  - Intuitively, no strong incentive to cheat…
    - …but, still, needs to be proven



- The **ASPECTS** project: Agile SPECTrum Security
  - Euro-NF (NoE) Specific Joint Research Project
    - AUEB, Blekinge Institute of Technology (M. Fiedler), Universität Passau (H. de Meer)

- Smart monitoring/reporting
  - Optimize monitoring time, energy etc.
  - Ask each client to scan a subset of the channels/spectrum
    - Will reduce scanning time
    - Cooperative scheme / build interference maps
      - Who has the picture? Partial?

Random Comments

- Power to the people
  - no central office
  - privacy, security...
- Management? (of User Premises Networks)
  - Managed vs. non-managed
  - professionally managed vs. auto/self-managed
  - Femtocells
    - by definition, professionally (Telco) managed
    - o.w., (multi-technology?) Access Points
- Networking: Matured... Stabilized...
- IP is all we want/need...(?)
  - Publish/Subscribe Internet Routing Paradigm
  - in overlay mode? inertia...

Thanks!

George C. Polyzos

Mobile Multimedia Laboratory

Department of Informatics/Computer Science
Athens University of Economics and Business
47A Evelpidon, 11362 Athens, Greece

polyzos@aueb.gr, http://mm.aueb.gr/
Tel.: +30 210 8203 650, Fax: +30 210 8203 325

Our Related Work

- **"Stimulating Participation in Wireless Community Networks"**
  E.C. Efstathiou, P.A. Frangoudis, and G.C. Polyzos
  Proc. IEEE INFOCOM 2006, Barcelona, Spain, April 2006
- **"Power Control in WLANs for Optimization of Social Fairness"**
  V. Douros, K. Katsaros, P.A. Frangoudis, and G.C. Polyzos,
  Proc. 12th Pan-Hellenic Conference on Informatics (PCI'08), Samos, Greece, August 2008
- **"Optimizing the Channel Load Reporting Process in IEEE 802.11k-enabled WLANs"**
  E. Panaousis, C.N. Ververidis, and G.C. Polyzos
  Proc. IEEE LANMAN 2008, Cluj-Napoca, Romania, September 2008
- **"Coupling QoS Provision with Interference Reporting in WLAN Sharing Communities"**
  P.A. Frangoudis and G.C. Polyzos,
  Proc. Social and Mesh Networking Workshop (IEEE PIMRC 2008), Cannes, France, September 2008

Selected References on the *P2P Wireless Network Confederation*

- "Stimulating Participation in Wireless Community Networks," IEEE INFOCOM 2006, Barcelona, Spain, April 2006 (E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos).
  - [P2PWNC evaluation through simulation & implementation]
- "Self-Organized Peering of Wireless LAN Hotspots," ***European Transactions on Telecommunications***, vol. 16, no. 5, Oct. 2005 (Special Issue on Self-Organization in Mobile Networking, E. C. Efstathiou and G. C. Polyzos).
  - [P2PWNC and the "NWAY" decision function]
- "Peer-to-Peer Wireless LAN Consortia: Economic Modeling and Architecture," 3rd IEEE International Conference on Peer-to-Peer Computing, Linköping, Sweden, Sept. 2003 (P. Antoniadis, C. Courcoubetis, E. C. Efstathiou, G. C. Polyzos, and B. Strulo).
  - [An economic analysis of P2PWNC]
- "A Peer-to-Peer Approach to Wireless LAN Roaming," ACM MobiCom Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH), San Diego, CA, Sept. 2003 (E. C. Efstathiou and G. C. Polyzos).
  - [The first position paper on P2PWNC]

Key Survey Papers on Cognitive Radio

- Qing Zhao and B.M. Sadler, "**A Survey of Dynamic Spectrum Access**," ***IEEE Signal Processing Magazine***, vol. 24, no. 3, pp. 79-89, May 2007.

- I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "**Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey**," ***Computer Networks***, vol. 50, no. 13, pp. 2127-2159, September 2006.

- S. Haykin, "**Cognitive Radio: Brain-Empowered Wireless Communications**," ***IEEE Journal on Selected Areas in Communications***, vol. 23, no. 2, pp. 201-220, Feb. 2005.