Coupling QoS Provision with Interference Reporting in WLAN Sharing Communities

Pantelis A. Frangoudis and George C. Polyzos

Mobile Multimedia Laboratory
Department of Informatics/Computer Science
Athens University of Economics and Business
11362 Athens, Greece

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

SocialNets 2008, Cannes, France, September 2008
Motivation

- Continuous Wi-Fi deployment
  - Ease of installation
  - Operation in unlicensed bands
  - Unplanned, anarchic

- Full Wi-Fi coverage in metropolitan areas, but...
  - ...most are secured using WEP, WPA, etc.
  - Need incentives to share one’s WLAN with strangers

- Interference issues...
  - ...due to unplanned deployment
  - IEEE 802.11b/g: only 3 non-interfering, non-overlapping channels
    - WLAN cells
  - Residential WLANs often operate on default channel settings

- Need solutions to the above problems
  - How about tackling them jointly?
### WCNs

<table>
<thead>
<tr>
<th>Network</th>
<th>City, Country</th>
<th>Nodes/Range</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seattle Wireless</td>
<td>Seattle, US</td>
<td>75 nodes</td>
<td>Mesh</td>
</tr>
<tr>
<td>AWMN</td>
<td>Athens, GR</td>
<td>2331 nodes</td>
<td>Mesh</td>
</tr>
<tr>
<td>CUWiN</td>
<td>Urbana, US</td>
<td>48 nodes</td>
<td>Mesh</td>
</tr>
<tr>
<td>Berlin’s Freifunk</td>
<td>Berlin, DE</td>
<td>316 nodes</td>
<td>Mesh</td>
</tr>
<tr>
<td>NYCWireless</td>
<td>NYC, US</td>
<td>149 nodes</td>
<td>Hotspot-based</td>
</tr>
<tr>
<td>FON</td>
<td>Worldwide</td>
<td>~210 000 registered APs</td>
<td>Hotspot-based</td>
</tr>
</tbody>
</table>
Athens Wireless Metropolitan Network

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

- Sharing Wi-Fi P2P-style
  - Reciprocal Wi-Fi sharing: Open one’s WLAN to roaming users to have the same benefit when mobile

- Client-assisted interference mitigation
  - Use client feedback to decide on optimal WLAN configuration
  - Can reveal hidden interference due to hidden terminals
Peer-to-Peer Wi-Fi Sharing

- P2P Wireless Network Confederation (P2PWNC)*
  - A WLAN 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

P2PWNC Receipts & Gossiping

P2PWNC receipts
- Proof of prior contribution

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

Connection request
OK
Receipt request 1
Receipt request 2
Receipt request 3
Receipt 1
Receipt 2 (increased weight)
Receipt 3
Yes
No

Team A receipts
New A→B receipt

Team B receipts
New B→C receipt

Team C
Team P
Connection request
Cooperate?
Receipt request
Receipt
Store receipt

Team A
Team B
Team C
New B→C receipt
New A→B receipt
P2PWNC Reciprocity Algorithm

- Receipts form a weighted directed graph
  - Nodes: peers/peer IDs
  - Edges: receipts, “dept” between two peers
  - Represents the system’s history of transactions

- Reciprocity algorithm
  - Input: receipt graph, provider ID, consumer ID
  - Output: Subjective Reputation Metric (SRM)
    - Uses maximum flow techniques.

- Subjective Reputation Metric
  - How good a contributor the visitor is in the eyes of the provider
  - Probability that the visitor will be granted access
Dealing with Interference (1/2)

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

- Interference detection
  - AP-centric vs. client-based

- Interference mitigation
  - Channel selection, power control, directional antennas, ...
  - Outside the scope of this work
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

Dealing with Interference (2/2)

- **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)

- **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?
Our Position

- 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
System Operation

- AP owners partition their Internet bandwidth
  - $B_{\text{owner}}$: reserved for personal use
  - $B_{\text{P2PWNC}}$: shared among P2PWNC visitors
  - $B_{\text{bonus}}$: bonus for interference reporting

- Visitor i gets access
  - P2PWNC protocol
  - Reciprocity algorithm $\rightarrow$ SRM$_i$

- Periodically, the AP requests for interference reports from each client
  - Client may (or may not!) perform a channel scan & report to the AP
  - Technologies
    - IEEE 802.11b/g active scan (channel, RSS, …)
    - Future: IEEE 802.11k
  - Client gets a QoS bonus for that
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

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

\[
B_i = \frac{SRM_i}{\sum_{j=1}^{n} SRM_j} \cdot B_{P2PWNC} + \frac{r_i}{n} \cdot B_{bonus}
\]

- Portion of the bandwidth dedicated to P2PWNC users
- Portion of the bandwidth for rewarding interference reports
Performance overhead

- Stations cannot receive/transmit app. packets while scanning
- Active scan on 11 channels: >250msec!
- Overhead depends on report request frequency
- Disincentive for clients to contribute reports?
  - No, if requests are not frequent and considering bandwidth bonus
- But how high is this overhead…
  - …especially for delay-sensitive apps?
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)
Results

- 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
Some Open Issues

- Security and reliability
  - How to spot fake reports?
    - Filter reports using a majority rule
    - Efficiency may depend on client distribution
  - Use a client reputation scheme, punish/reward?
  - Use monitors (Where to place them? How many? Who owns them?)

- Model and study incentives/QoS mechanism
  - Intuitively, no strong incentive to cheat…
  - …but, still, needs to be proven

- Smarter monitoring/reporting
  - Ask each client to scan a subset of the 11 channels
  - Will reduce scanning time
Conclusion

- Community-based WLAN access & interference mitigation can be jointly considered

- Client-based interference sensing/reporting has low overhead if performed moderately

- Network access & QoS rewards for interference reports, under two basic assumptions:
  - Wi-Fi operators value this information
  - No significant overhead for clients

- Many issues need further study
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

SocialNets 2008, Cannes, France, September 2008