Distributed Sensing for Spectrum Agility: Incentives and Security Considerations

S. Arkoulis, P. Frangoudis, G. Marias, G. Polyzos
Athens University of Economics and Business
{arkoulistam,pfrag,marias,polyzos}@aueb.gr

M. Fiedler
Blekinge Institute of Technology
markus.fiedler@bth.se

R. Herkenhöner, H. de Meer
University of Passau
rhk@fim.uni-passau.de, demeer@fmi.uni-passau.de

Euro-NF FIA Workshop, November 2008

Motivation (1/2)

- Trend towards open wireless access
  - Continuous Wi-Fi deployment
  - Ease of installation, operation in **unlicensed** bands
  - Unplanned, anarchic
- Full Wi-Fi coverage in metropolitan areas, but…
  - Interference issues due to unplanned deployment
  - IEEE 802.11b/g: 3 non-interfering, overlapping WLAN cells
  - Residential WLANs often operate on default channel settings
- Low **licensed** spectrum utilization
  - Need for **Dynamic/Opportunistic Spectrum Access**
- Basic functions
  - Sensing the environment
  - Adaptation and “smart” decisions for spectrum sharing

Motivation (2/2)

- The *Internet of Things*
  - Myriads of interconnected devices (Smart home, PANs, Wi-Fi, …)
  - Increased need for spectrum agility
- Technological advances
  - Software Defined Radios / Cognitive radios
  - IEEE 802.11k (radio measurements) finalized

An Open Spectrum Access environment

- Basic premises
  - Use of unlicensed spectrum
  - Open access without necessary prior contracts
- Spectrum allocation not an issue
  - Everyone can become an operator
  - Lack of regulation → interference
  - Need for alternative interference mitigation strategies
- Distributed spectrum sensing (DSS)
  - Mobile terminals, access points, sensors/monitors **sense** and **report**
- Dynamic vs Open Spectrum Access
  - DSA: Opportunistic secondary (unlicensed) user access when primary users are absent
  - Spectrum sensing to detect primary users

Distributed sensing in unlicensed spectrum

- Operations
  - Monitor spectrum usage (when requested)
  - Report to central/distributed entities
- Fuse information from multiple sources
  - Mobile users, local AP measurements, dedicated spectrum “sensors”
- Purpose:
  - Detect service offerings and **hidden interference**
- Wireless coverage maps
  - Real-time or longer term information for informed spectrum access decisions
  - Detect “white spots” → Prospective operators can deploy new infrastructure
  - Help power adaptation, but also …
  - …plan handovers
- Off-the-shelf technology capable of simple SS (e.g. IEEE 802.11 scan)

Incentives and security considerations

- Validating interference reports is non-trivial
  - Fake reports
  - Outdated reports due to spectrum usage dynamics
  - Measurement errors
- Do clients have incentives to submit truthful reports?
  - Performance cost of spectrum sensing
  - Competition among providers
- Information filtering
- Reputations and the role of identities
- Privacy concerns

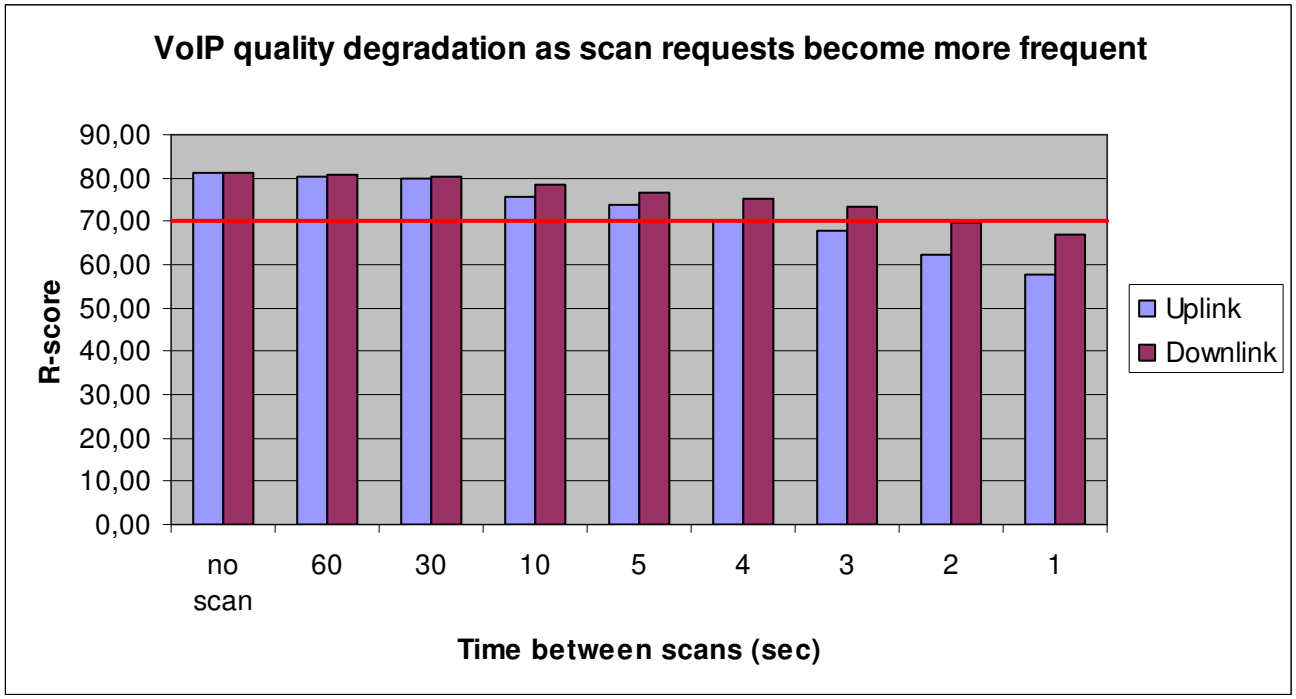
Incentives for truthful reporting

- Reward reporting
  - Access/QoS benefits
  - Cheaper prices – discounts (in commercial deployments)
- Punish cheaters
  - Deny / interrupt service for small intervals
  - No QoS benefits
- How about user reputations?

The cost of spectrum sensing (1/2)

- Test case
  - IEEE 802.11b/g
  - Stations scan for nearby APs when requested (periodically)
- Performance overhead
  - IEEE 802.11 active scan on 11 channels: >250msec
  - Stations cannot receive/transmit app packets while scanning
  - QoE degradation of delay-sensitive apps?
- QoE degradation due to sensing must be sufficiently low…
  - …so that offered “benefits” in exchange outweight it

The cost of spectrum sensing (2/2)



- Testbed experiments: single client, bidirectional VoIP traffic (G.729)
- E-model for VoIP quality assessment
- Acceptable quality: R-score > 70
- Moderate scanning frequency (e.g. 2 scans/min) ➔ Minimal QoE degradation

Competition and misbehavior

- Multiple (micro-)operators compete to offer service
- User affiliated with operator A may send fake reports to operator B
  - Pollute B's view of spectrum conditions and trick him to wrong network configuration decisions …
  - … trying to reduce congestion in A's occupied frequencies
  - … trying to cause dissatisfaction to B's clients

Information filtering (1/2)

- Need mechanisms to filter fake/invalid reports
- Simple approach: voting
  - Easier if reports carry spatial (GPS) and temporal info
  - Filter out “odd” spectrum usage reports
    - for a specific spot/area at a specific period of time

Information filtering (2/2)

- Dedicated monitors
  - Assume “trusted” & tamperproof “sensors” at fixed locations
  - Provide valid reports (for their spot) when requested
  - Can be used as an extra information source
- Challenges
  - Placement, cost, ownership

Applying reputations

- Submitted information weighted against each user's reputation
- Reports considered "fake" reduce reporter's reputation
- Reward for reporting a function of a user's reputation
- But: need a (permanent) user **identification scheme**
- Can we use community identifiers?
  - Example: Users belonging in a wireless community network
  - Interference reporting & coverage maps ➔ community service
  - Good reporters enjoy community benefits
  - Bad reporters suffer punishment/exclusion

Privacy concerns

- Reports may carry sensitive info
  - E.g. actual user location
- Need confidentiality
  - Standard encryption to prevent eavesdropping
- Confidentiality not always enough
  - Users may not wish to disclose their location to the requesting entity

Spectrum sharing challenges

- Unlicensed spectrum **sharing**: a whole new set of challenges
  - Lack of strict regulation
  - Equal spectrum access rights
- May assume a set of predefined sharing policies
  - Sharing dimensions: frequency, space, time
  - Policy conformance should be monitored
- Potential attacks
  - Disrespect to agreed spectrum allocation, rule violation
    - Not always easy to detect, esp. in wireless networks
  - Attacking spectrum sensing/reporting mechanisms
  - Policy distribution attacks
  - …
- How to enforce sharing rules without a regulator?

Conclusion

- Robust distributed spectrum sensing not an easy task
  - Hard to detect invalid information
  - May need to provide incentives for reporting
  - Need to design low-overhead sensing/reporting mechanisms
- Technological advances
  - Cognitive radio
  - IEEE 802.11k
- Many open issues in open spectrum sharing