

# Secure Interference Discovery in Future Open Spectrum Access Wireless Networks

---



P. Frangoudis, D. Zografos and G. Polyzos

**Athens University of Economics and Business**

{pfrag, zwgrafos, polyzos}@aueb.gr



Euro-NF WP 3 Workshop on Social Economic Aspects

Leipzig, June 14-16, 2009

# Motivation

---

- Trend towards open wireless access
  - ◆ Continuous Wi-Fi deployment
  - ◆ Ease of installation, operation in **unlicensed** bands
  - ◆ Unplanned, anarchic, sharing common spectrum → Interference
- The *Internet of Things*
  - ◆ Myriads of interconnected devices
  - ◆ Challenges at all network layers
    - Vastly increased communication needs
- Network of the Future
  - ◆ Increased demand for spectrum
  - ◆ Need for spectrum efficiency
  - ◆ Spectrum usage **monitoring**

# 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
- Monitoring spectrum usage
  - ◆ Mobile terminals **sense** and **report**
- Purpose
  - ◆ Detect interference
  - ◆ Assist in wiser spectrum access decisions and more efficient **sharing**

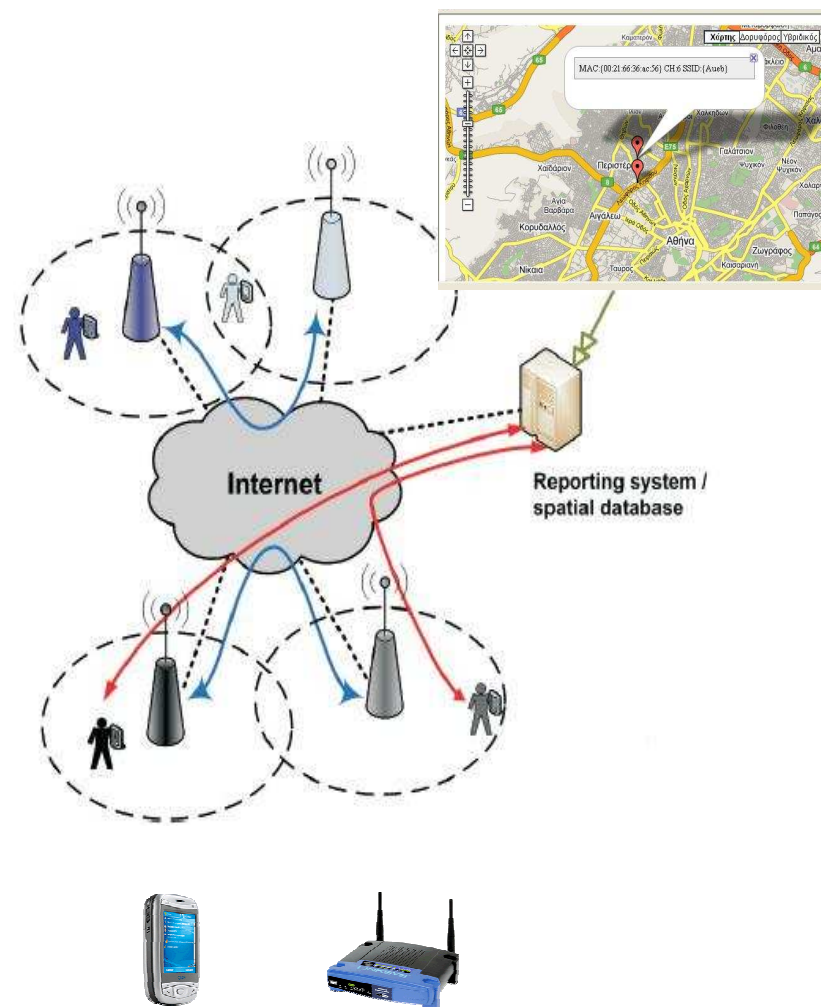
# Spectrum usage monitoring

---

- Operations
  - ◆ Terminals monitor spectrum usage (when requested)
  - ◆ Report to central/distributed entities
- Purpose
  - ◆ Detect service offerings and **hidden interference**
  - ◆ Detect spectrum **inefficiencies**
  - ◆ Detect **violation** of spectrum access rules (if any)
- 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 spectrum sensing
  - ◆ Wi-Fi cards scan for AP beacons
  - ◆ IEEE 802.11k is standardized

# Architecture

- Design with dense Wi-Fi deployments in mind
- Roaming clients scan for AP presence when requested
- Report their decisions to AP (with location info, if available)
- APs forward reports to DB
- Wireless coverage maps built
  - ◆ Spatial queries
- Implemented on off-the-shelf Wi-Fi equipment



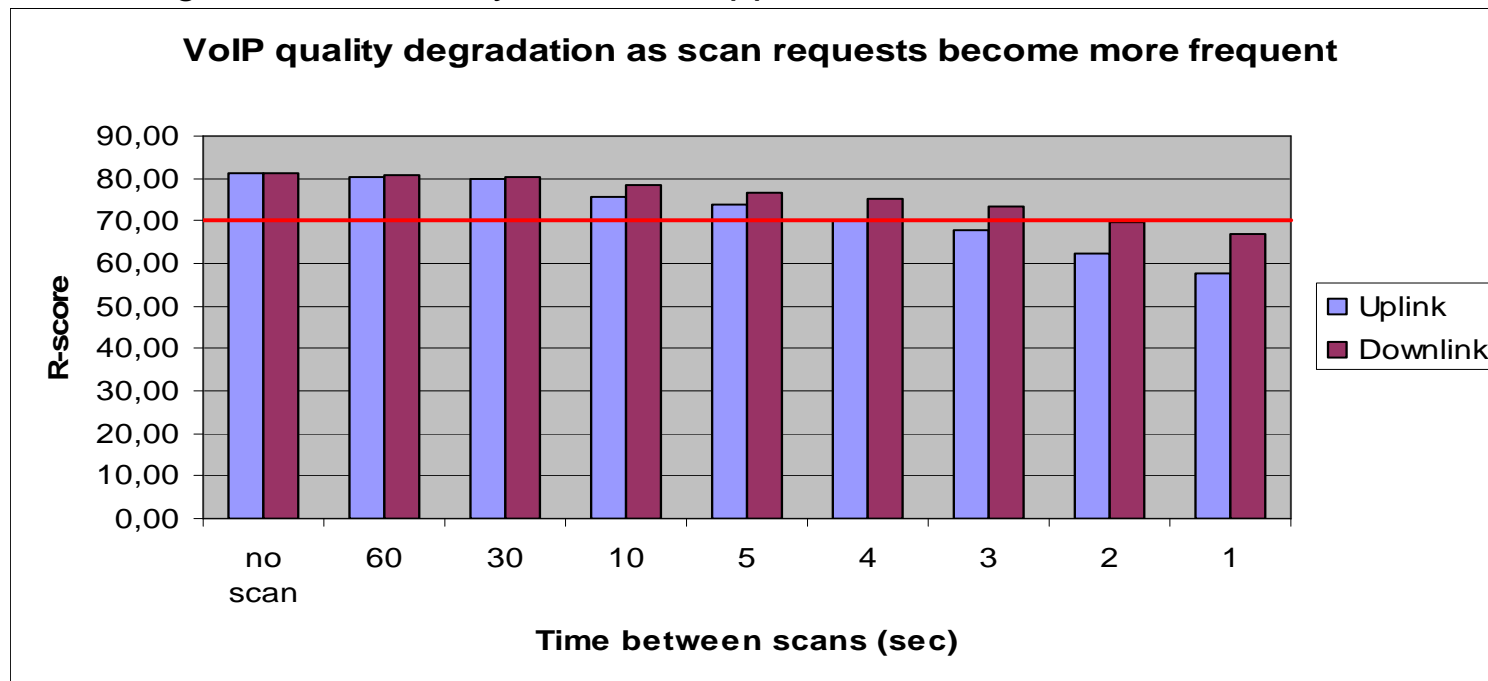
# Incentives and security considerations

---

- Is this secure and robust?
- 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

# The cost of spectrum sensing

- 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
  - ◆ QoE degradation of delay-sensitive apps?



# 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

# Countermeasures

---

- Information filtering
- Reward reporting
  - ◆ Access/QoS benefits
  - ◆ Cheaper prices – discounts (in commercial deployments)
- Punish cheaters
  - ◆ Deny / interrupt service for small intervals
  - ◆ No QoS benefits

# Attacker strategies

---

- Attackers acting independently
  - ◆ Each attacker reports a random set of interfering base stations
- Attackers acting collectively
  - ◆ Groups of attackers (**colluders**) attached to AP report the same (random) group of interfering base stations
  - ◆ Different scenario wrt user-provider associations
  - ◆ We assume an AP **trusts** its own users and does not trust roamers
  - ◆ Weighted (discounted) roamer reports

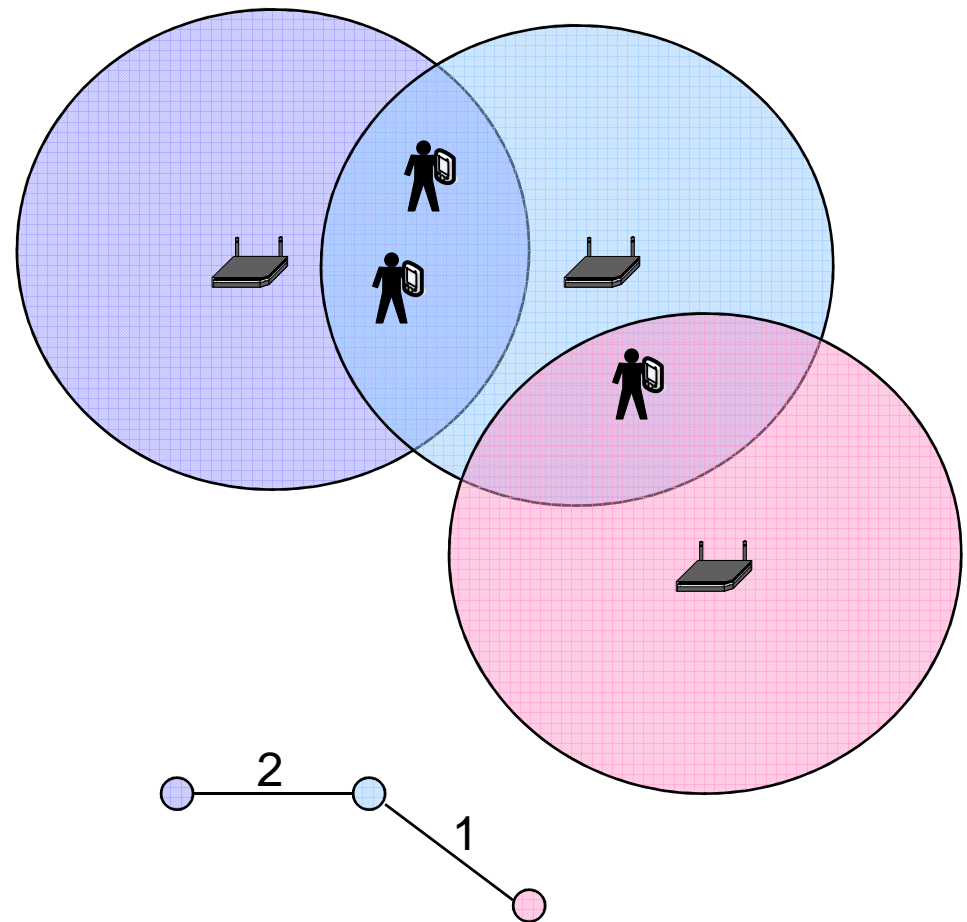
# Information filtering

---

- 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

# The Interference Graph

- System-wide interference conditions
- Nodes: base stations
- Edges: cases of interference between base stations (overlapping cells)
- Edge weight: number of clients reporting an edge
- User-perceived interference
  - ◆ We only care about overlapping cells if reported



# Filtering mechanisms

---

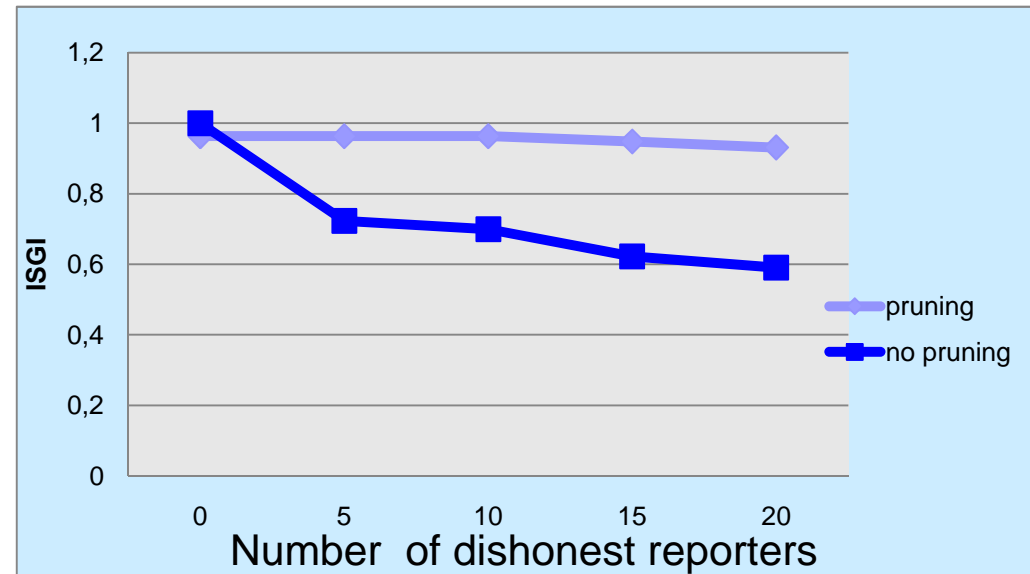
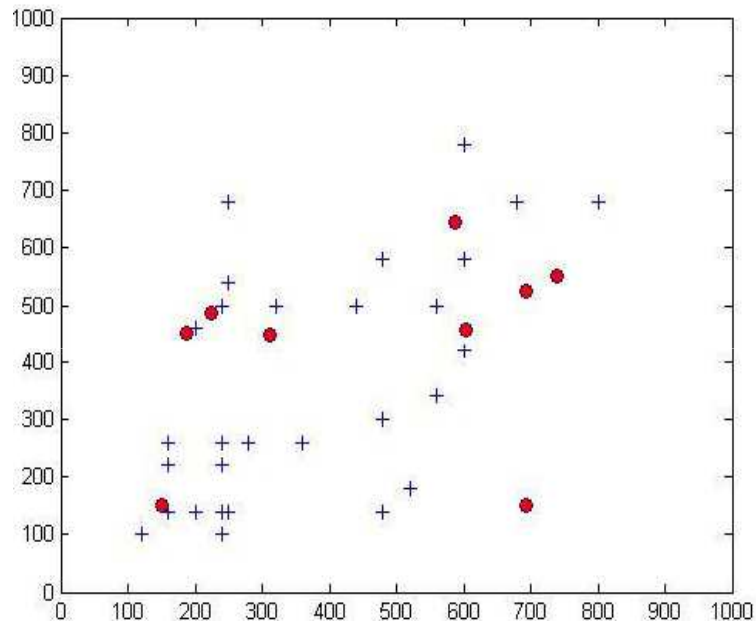
- Ignore (prune) edges with small weight
  - ◆ e.g. instances of interference reported only by a single user
- Tackles attack #1
  - ◆ Random fake reports: unit-weight edges
- Tackles attack #2...
  - ◆ ...only if colluder reports are discounted
- Introduces false negatives...
  - ◆ ...but works well in dense Wi-Fi deployments

# Evaluation methodology

---

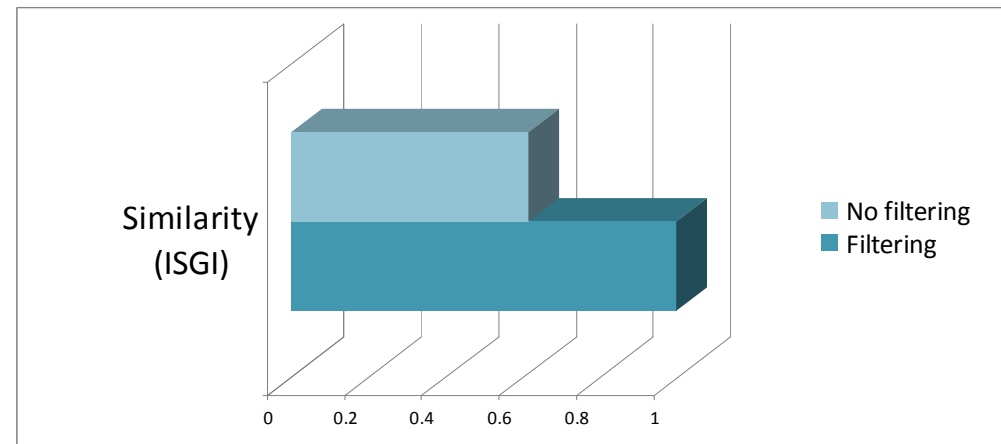
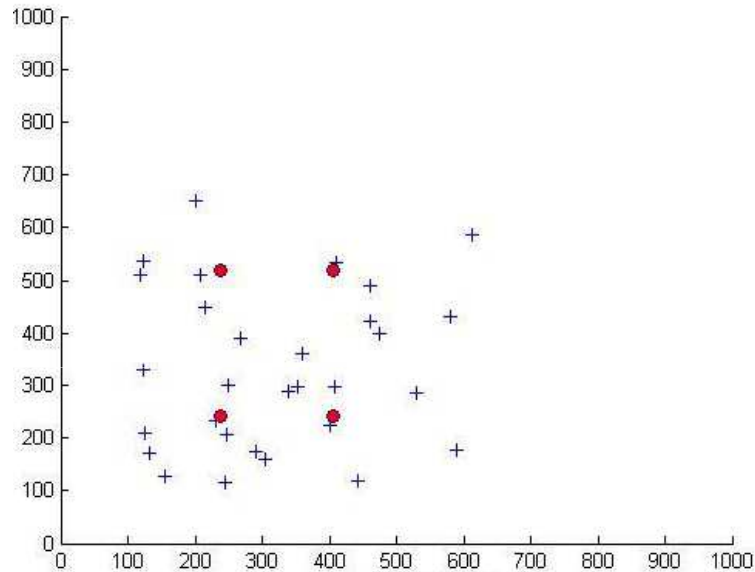
- Simulate attacks
- Apply filtering mechanism
- Compare 2 graphs
  - ◆ Original IG (actual interference conditions)
  - ◆ Reported IG, after applying our filtering mechanism
- Reported IG should
  - ◆ contain “important” edges of the original IG
  - ◆ not contain fake edges that “affect” many nodes
- Original vs reported IG
  - ◆ Interference Graph Similarity Index (ISGI)

# Simulation results – scenario A



- Random topology
  - ◆ 10 APs, 30 clients
- Effectively tackles attack #1 even for large percentage of attackers

# Simulation results – scenario B



- 50% roamers
- Each AP's roamers collude!
- Roamer reports are weighted → very efficient filtering

# Summary

---

- Spectrum usage monitoring is significant for achieving efficient spectrum utilization
- Security issues in spectrum usage/interference reporting
- Simple security mechanisms can prove efficient