ASPECTS: Agile Spectrum Security

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

M. Fiedler, A. Popescu
Blekinge Institute of Technology
{markus.fiedler,app}@bth.se

H. de Meer, R. Herkenhöner, A. Fischer, J. Oberender
University of Passau
{demeer,rhk,andreas.fischer,jens.oberender}@fim.uni-passau.de

7th Euro-NF Conference on Next Generation Internet (NGI 2011)

Facts about ASPECTS

- Euro-NF SJRP, ended Dec. 2009
- Partners
  - Mobile Multimedia Lab, AUEB
  - Blekinge Institute of Technology
  - University of Passau
- Research area
  - Security for Cognitive Radio/Open Spectrum Access Networks

Research Goals

- Identify security & privacy vulnerabilities of the underlying CR/Open Spectrum Access network
  - Thorough review of the state-of-the-art & relevant issues

- Design & evaluate a security and trust framework to detect-report-counter misbehavior

- Address specific cases of misuse in the context of the ASPECTS framework
  - Design, implementation, & evaluation of a user-driven monitoring infrastructure for unlicensed spectrum access

Relevance to the Euro-NF vision

- Deals with (potentially) disruptive technologies at the **edge** of the network

- Wireless FI
  - DSA/CR facilitate **spontaneous and opportunistic** networking
  - Enable efficient **resource utilization**

- Relevance to the Internet of Things
  - will change...
    - traffic volumes,
    - spectrum access dynamics

- Privacy and security issues (JRA 3.4)

ASPECTS outcome

- Conference papers on
  - incentives issues in distributed spectrum sensing
  - user-driven topology/interference discovery
  - network virtualization

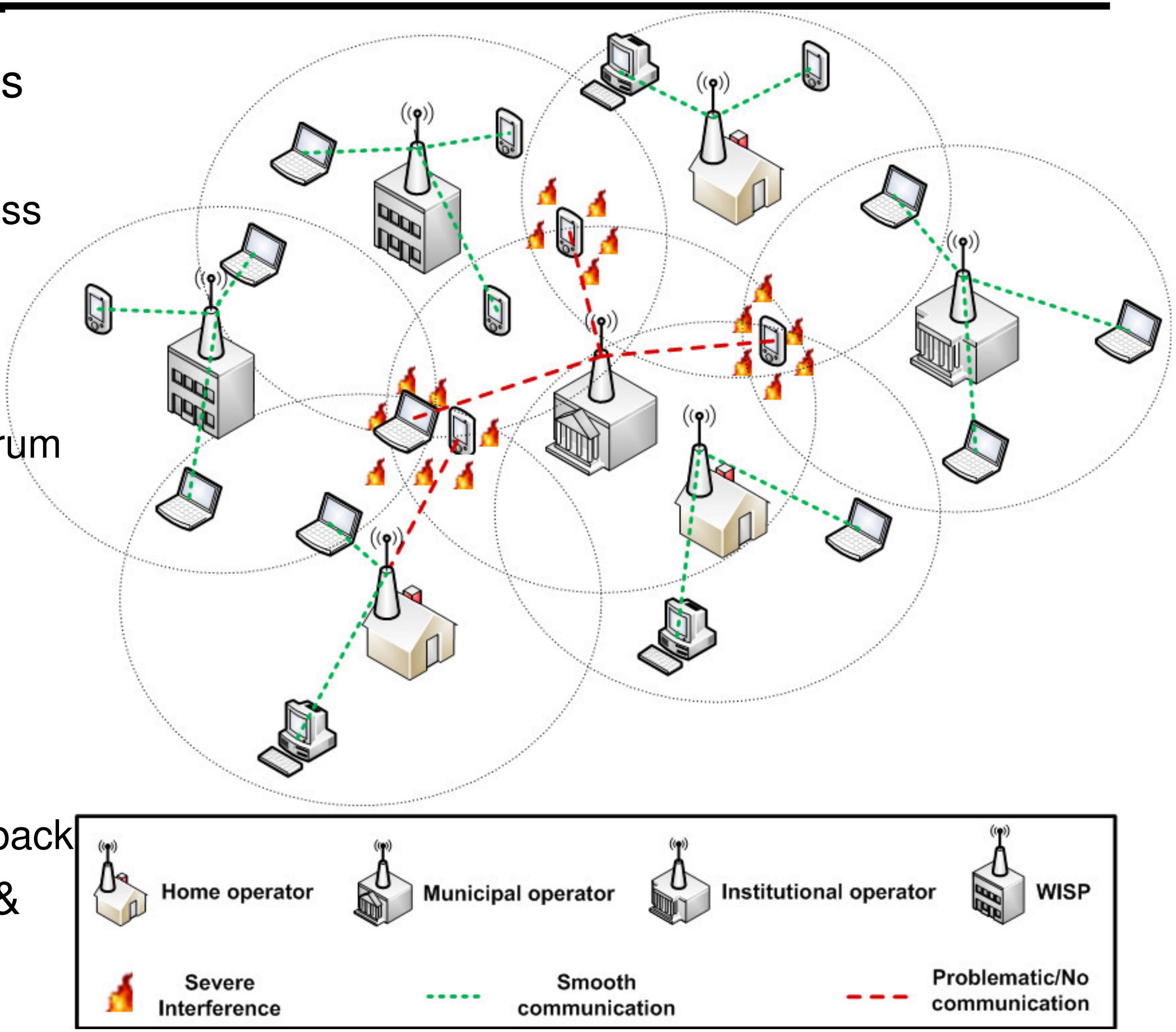
- Joint journal article on misbehavior scenarios in CR networks

  @Future Internet, SI on "Security for Next Generation Wireless and Decentralized Systems," Aug. 2010

- ASPECTS related presentations @ events outside Euro-NF
  - IEEE ICCCN 2009
  - 23rd WWRF meeting

Networking environment

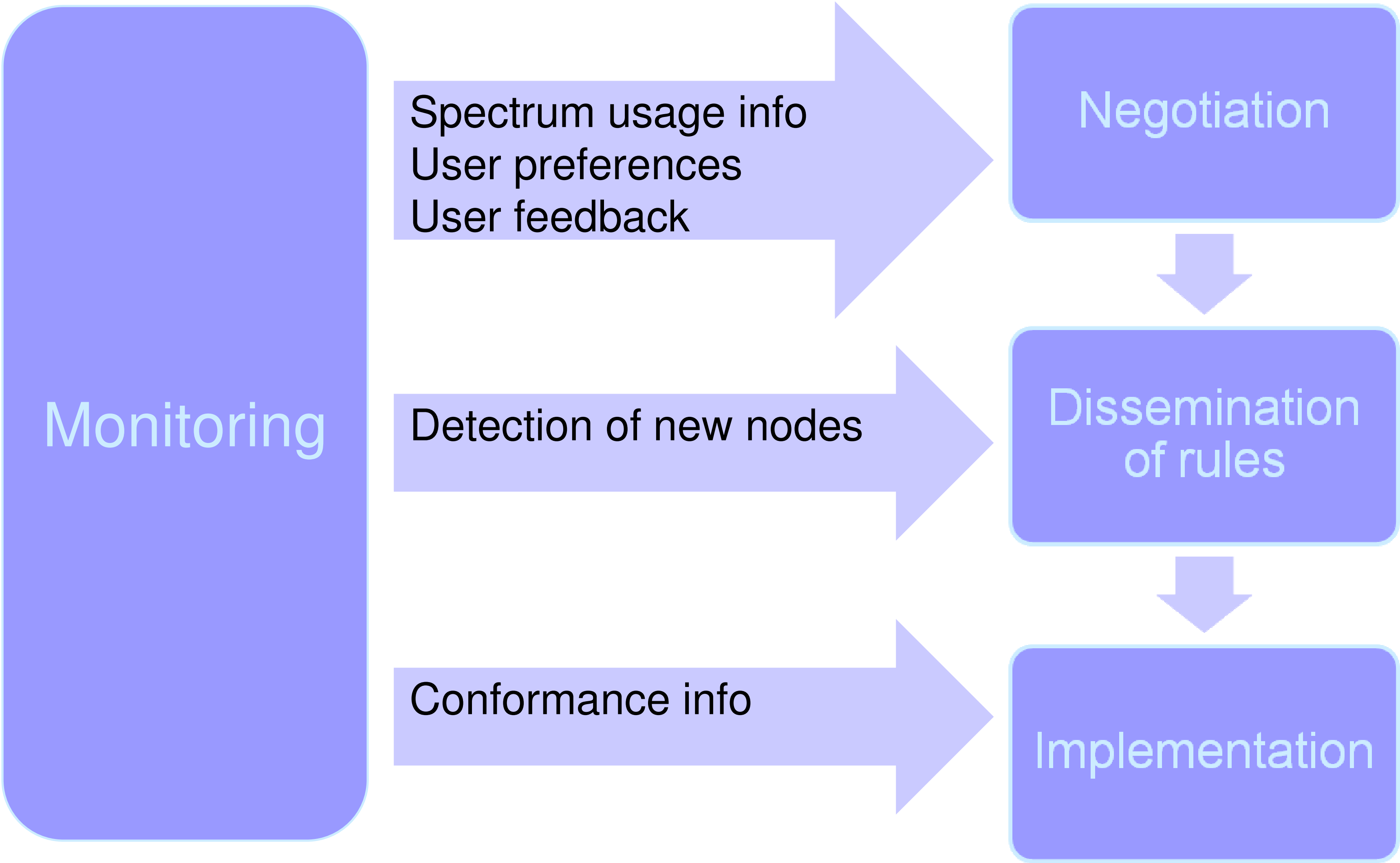
- CR & Open Spectrum Access
- Cognitive Radio Networks
  - Primary vs. secondary access
  - Opportunistic access by “secondary” users
- Open Spectrum Access
  - Access to unlicensed spectrum
  - Lack of spectrum allocation/min. regulation → interference
- Common denominator:
  - Need for sophisticated spectrum sharing schemes
  - Need for monitoring & feedback
- Incentives for non-reporting & mis-reporting



Attacker Profiles

- *Malicious*
- *Rational (selfish),* strategic
  - *Cheating*
  - *Polite Cheating*

Spectrum sharing phases



Notable attacks

- Monitoring
  - Primary user emulation
  - Fraudulent spectrum sensing data reporting
- Negotiation
  - Tampering with the (common) control channel
- Dissemination of rules
  - Injecting fake spectrum access rules
- Implementation
  - Over-consuming resources (e.g., timeslots, frequency bands)

Incentives for misbehavior

- Assume self-interested entities

- Competition among providers
  - Why abide to spectrum sharing protocols?
  - Increase power to increase coverage/data-rate
  - Use more bandwidth
  - Use more timeslots

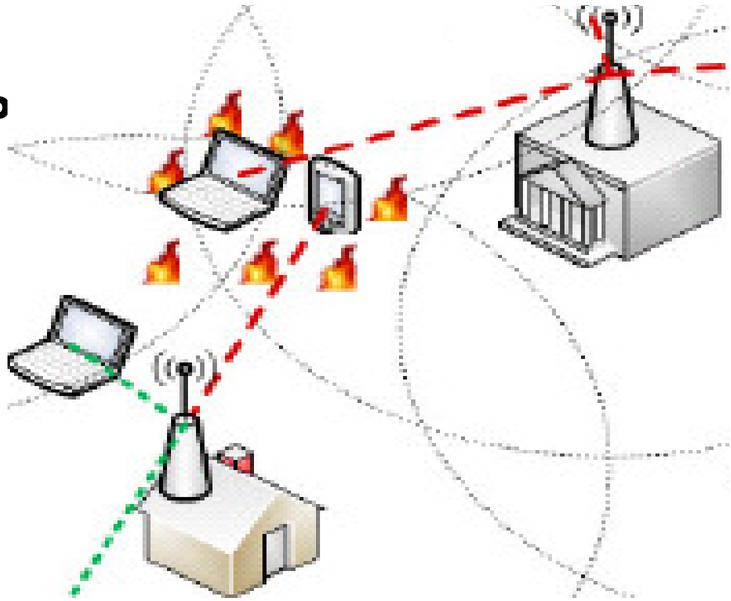
- Attacks on spectrum monitoring mechanisms
  - Spectrum sensing can be costly ➔ why cooperate?
  - Strategic behavior ➔ forge spectrum sensing results to trick spectrum sharing mechanisms

Robust user-driven monitoring in an OSA environment

- WISP deploying a Wi-Fi network in a city or campus
  - Centralized configuration and user AAA
- Needs to know the topology of the network for optimized operation
  - Topology ➔ input for channel assignment /power control
- Two options
  - A pure infrastructure-centric topology discovery scheme, or…
  - Crowdsource this task to clients

Infrastructure-centric vs. user-centric approaches

- Infrastructure-centric
  - Sense spectrum usage at the AP site
  - **Trustworthy** measurements
  - Fail to capture **interference beyond the AP**



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

- **How to deal with fake reports?**

Our (crowdsourcing) approach

- Topology discovery for centrally-managed Wi-Fi deployments
  - Detect overlapping coverage
- Authenticated users report wireless coverage at their spot
  - IEEE 802.11i for security/authentication
  - Reports using IEEE 802.11k
  - When requested, **each user reports about the APs in range**
  - Managed APs also provide **trusted** reports
- A **coverage graph** is built
  - Vertices: APs, edges: potential interference
  - Channel assignment algorithms can be executed on it
- A reputation scheme to weigh user reports
  - Truthful reporters have higher reputation in the long run

Dealing with fake reporting

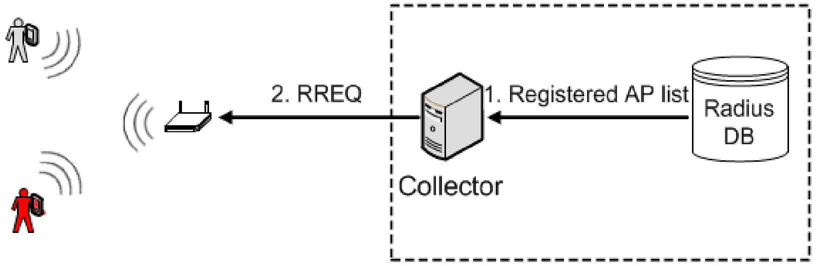
- Attack scenario
  - A user submits a (**random) fake list** of AP identifiers

- **Consensus**-based scheme
  - Weighted reports
  - Sum of reports about a coverage instance (i.e., overlapping coverage between 2 APs) should exceed a **threshold**
  - Cases of overlap below the threshold are **filtered**

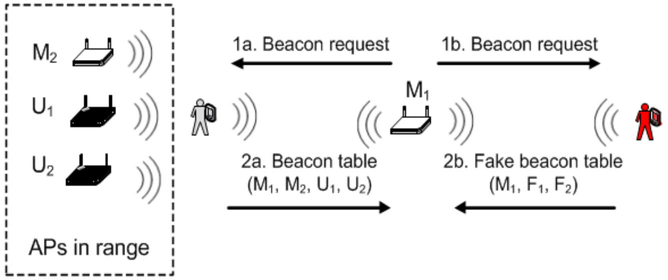
- Filtering
  - If we assume no collusion, all fake information is filtered
  - True info may also be filtered (not meeting the threshold)
  - AP-based measurements help **audit** user reports
  - User score: % reported info exceeding the threshold at a reporting round
  - Reputation updated based on score

System operation

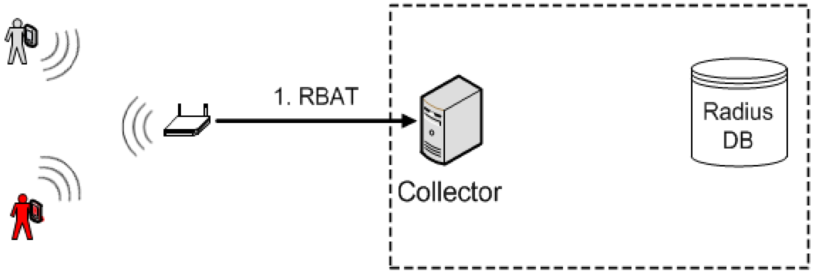
A. Collector requests for reports from **managed** APs



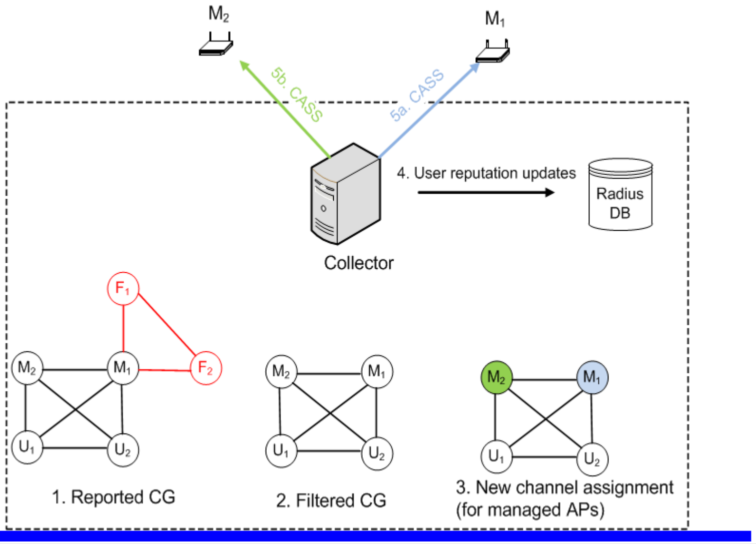
B. AP collects reports from clients using **IEEE 802.11k**


M_2
U_1
U_2
APs in range
1a. Beacon request
1b. Beacon request
M_1
2a. Beacon table (M_1, M_2, U_1, U_2)
2b. Fake beacon table (M_1, F_1, F_2)

C. AP sends report batch to collector



D. End of reporting round: filtering, reputation updates, new channel assignment



- Implemented a subset of IEEE 802.11k (Linux Kernel 2.6.38) and reporting attacks;)
- Radius auth, EAP-PEAP, WPA2-AES
- Atheros AR5213 Wi-Fi cards (MadWifi)
- Collector – AP communication over UDP

Evaluation

Metric

- % (real) graph edges discovered
- The rest are filtered
- Only edges between managed APs matter

Scenario

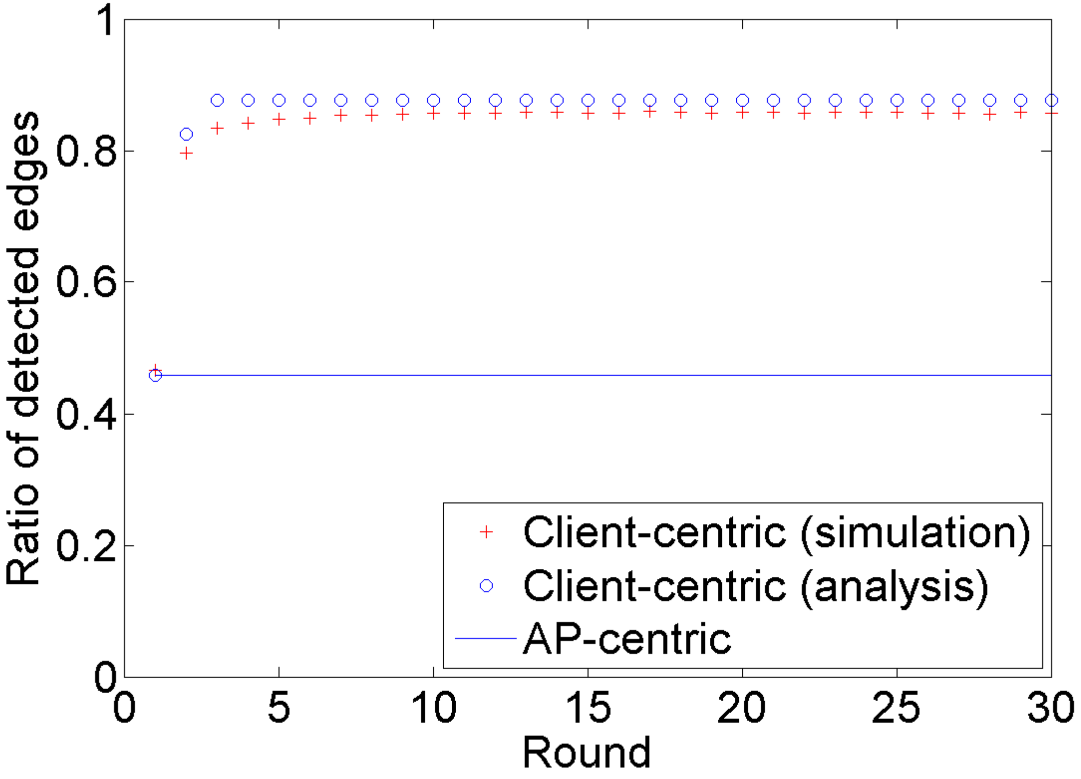
- potential attackers
  - each attacks with p
- x% APs participate
  - Same administrative domain
  - Only users attached to managed APs can report (authenticated)
- Clients start with 0 reputation

Results

- Hostile environment but high performance as rounds progress
- Reason: honest reporters increase their reputation and thus their report weights
- **AP-centric scheme: lower bound**

Filtering efficiency

(Boston: 4947 clients/km^2, 729 APs/km^2)



Conclusion: ASPECTS main results

- Detailed classification of security threats & countermeasures in Cognitive Radio networks
- Identified incentives for misbehavior
- Design/implementation/evaluation of a user-centric architecture for coverage & interference detection for a specific case of the ASPECTS environment