User-centrism in wireless networking

Pantelis Frangoudis

Outline

1. Introduction
2. User-provided wireless network infrastructure
3. User-centric secure multimedia services
4. Crowdsourced Wi-Fi topology discovery
5. Conclusion

Introduction

Background

Traditional view of communications has been disrupted

- Operator-centric view: user as a consumer
- Evident user empowerment

Recent advances

- Increased user-based wireless coverage
- Flexible technologies for wireless home networking
- Versatile technologies at the user end
- The rise of crowdsourcing

Opportunities and challenges for a user-centric networking paradigm

Why user-centric?

- Exploit underutilized resources
- Exploit user capabilities (versatile devices, mobility,...)
- Flexibility, autonomy
- Reduced mgmt complexity and infrastructure cost

Performance challenges

- Low-cost, resource-constrained user equipment
- Lack of technical expertise
- Lack of central planning and control
- Best-effort-style operation

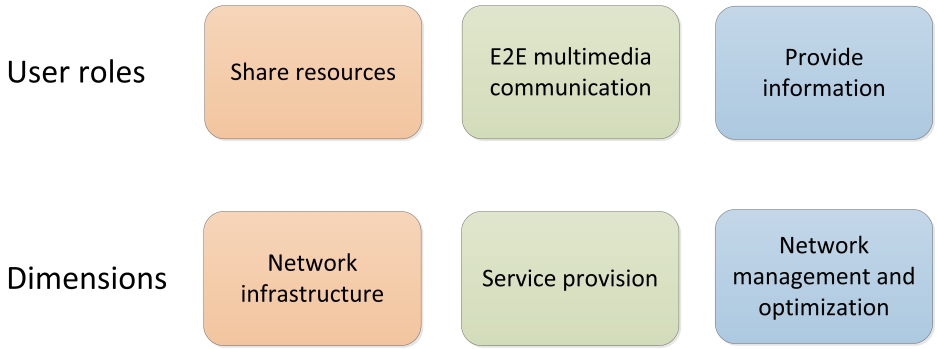
Security challenges

- Untrusted crowds
- Lack of "contracts"
- Loose identification

Thesis

Research axes

- Wireless access
- Multimedia service provision
- Information provision (for network mgmt/optimization)



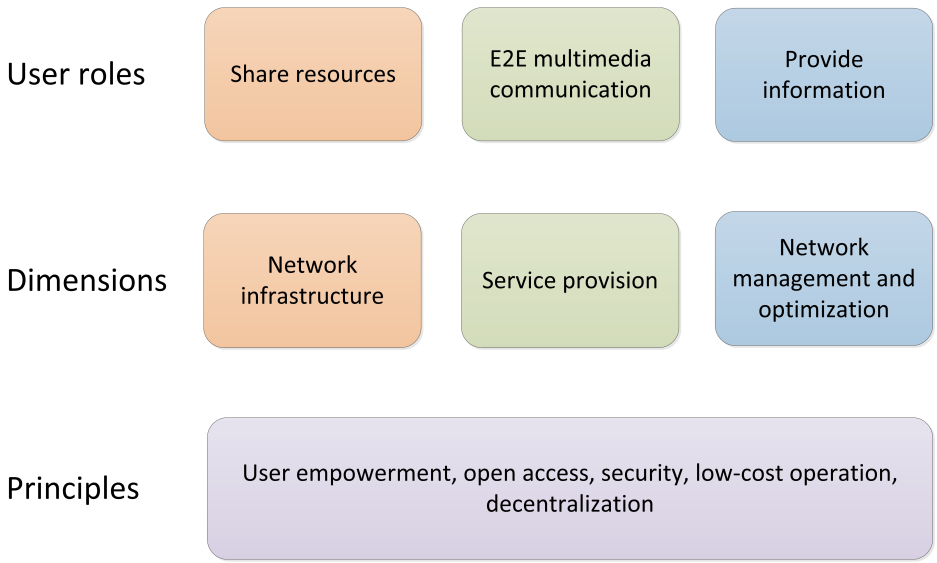
Thesis

Research axes

- Wireless access
- Multimedia service provision
- Information provision (for network mgmt/optimization)

Principles

- User empowerment
- Open access
- Decentralization
- Security
- Low-cost operation



User-centric wireless access

Community wireless mesh networks

- Studied and classified existing wireless communities around the world
- Discovered power law behavior in their structure

Building a Wi-Fi sharing scheme

- Protocol design with existing, low-cost equipment in mind
- First to implement a decentralized Wi-Fi sharing scheme on home Wi-Fi routers

User-centric multimedia services

Highlights

- Built on existing user equipment
- Minimal need for additional rendezvous infrastructure
- Secure and tackling legal implications

First to:

- Propose a tunneling-based secure communication scheme for wireless communities
- Do it purely on home user equipment
- Do it in a purely user-centric way
- Measure its impact on VoIP QoE

User-centric Wi-Fi topology discovery

A robust crowdsourcing approach

- Tailored to managed Wi-Fi deployments
- Distributed information collection for centralized network management
- IEEE 802.11k-based reporting architecture
- Reputation-based report filtering to combat **fake reporting**

First to:

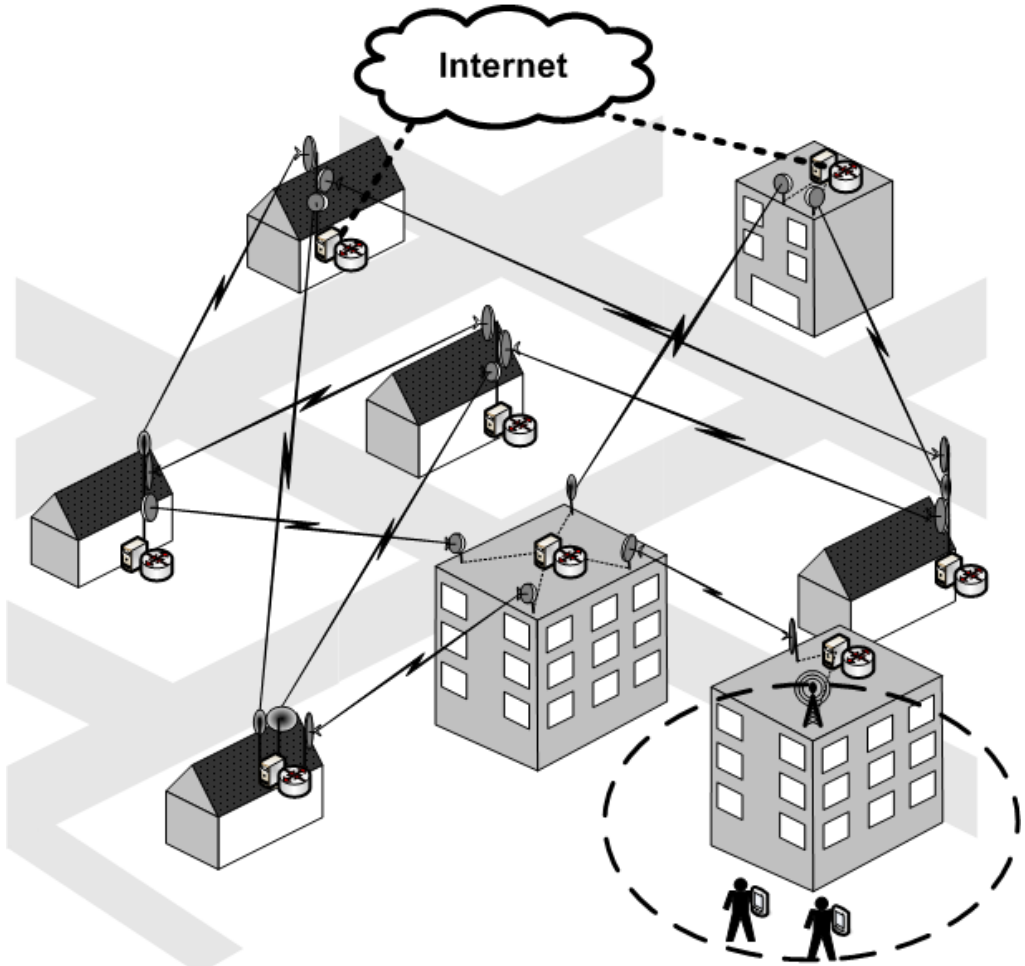
- Address specific IEEE 802.11k attacks & propose/implement countermeasures
- Derive analytic expressions on topology discovery accuracy
- Quantify the performance of a user-centric scheme vs an AP-centric one...
- ...even for large numbers of attackers

User-provided wireless network infrastructure

Wireless Community Mesh Networks

Wireless mesh

- Community owned all-wireless backhaul
- Intra-community services (VoIP, file sharing, ...)
- Focus on autonomy



Large WNCs and their structure

Notable communities

- Athens Wireless Metropolitan Network (2400 nodes)
- guifi.net (14000 nodes)

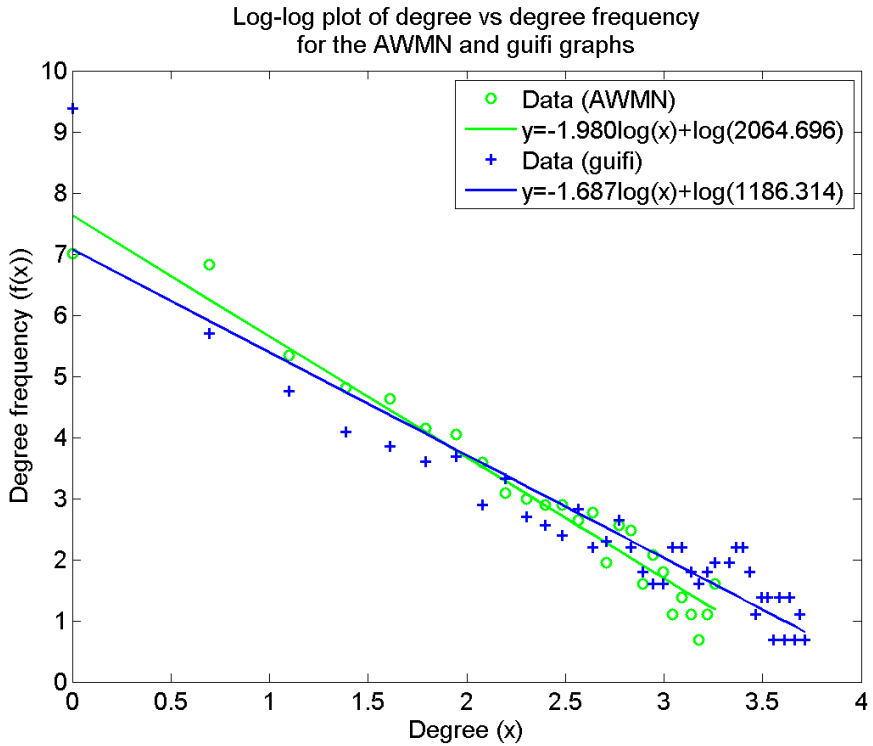
Large WNCs and their structure

Notable communities

- Athens Wireless Metropolitan Network (2400 nodes)
- guifi.net (14000 nodes)

Network structure

- Wireless mesh
- Link distribution not homogeneous
- Most users with few links
- Power-law like properties



- Degree: # links
- Degree frequency: # nodes with degree x

Large WNCs and their structure

Notable communities

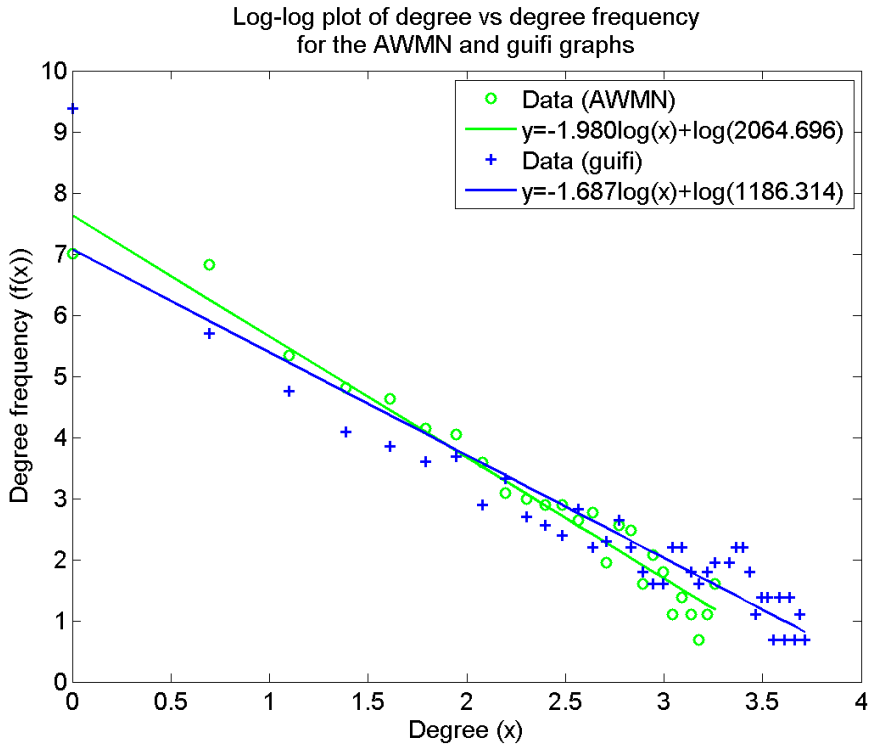
- Athens Wireless Metropolitan Network (2400 nodes)
- guifi.net (14000 nodes)

Network structure

- Wireless mesh
- Link distribution not homogeneous
- Most users with few links
- Power-law like properties

Why?

- Few very active members
- Favorable node locations
- It's a social network, after all...



- Degree: # links
- Degree frequency: # nodes with degree x

Peer-to-Peer Wi-Fi sharing

Efstathiou (2006) on Wi-Fi sharing *

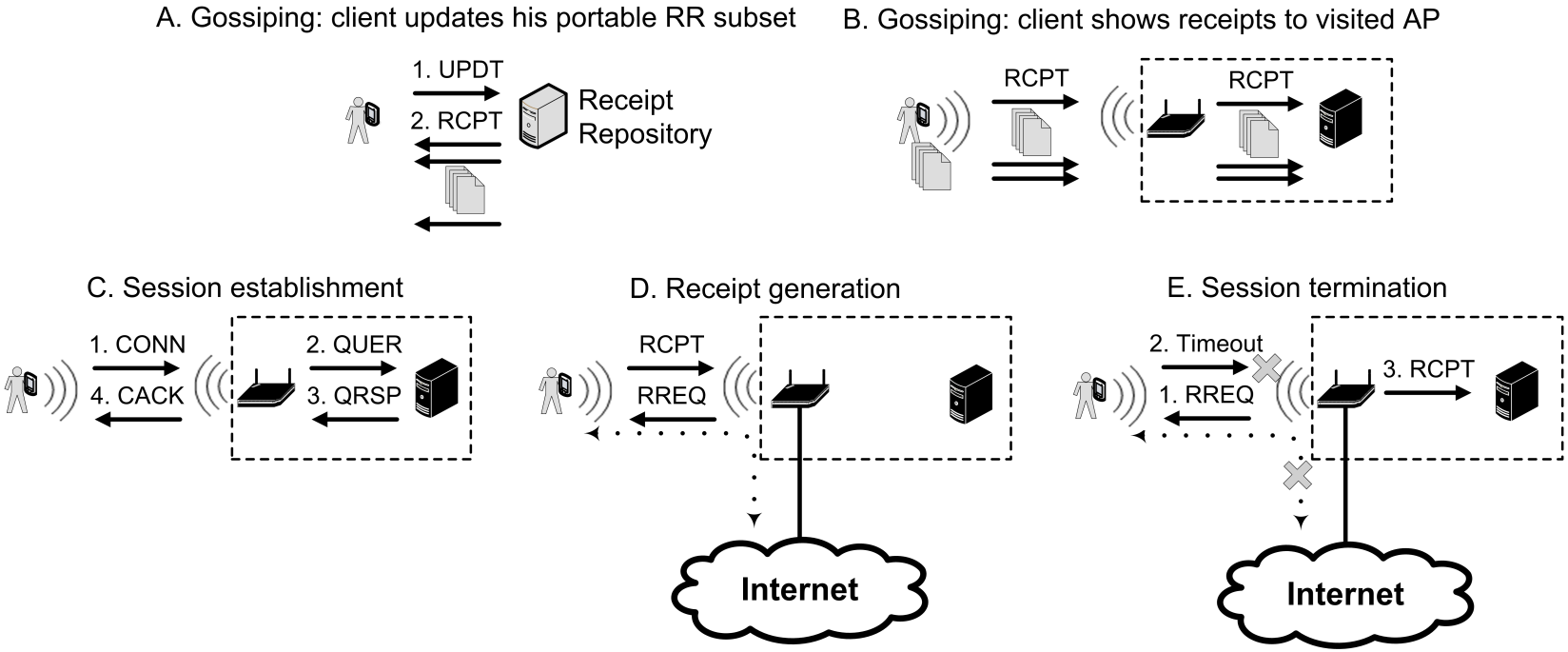
- A fully-distributed, reciprocity-based approach
- Accounting: digital "receipts" signed by consumer
- Distributed algorithms to stimulate cooperation, exclude free riders

Requirements and assumptions

- Users do not trust their provider
- Decentralized operation
- Operation on low-cost equipment

* E.C. Efstathiou, "A peer-to-peer approach to sharing wireless local area networks," Ph.D. dissertation, AUEB, 2006.

P2PWNC operations



P2PWNC Protocol

- Access control, receipt generation
- Design with off-the-shelf equipment in mind
- All functionality in home router firmware
- Elliptic Curve Crypto to reduce receipt storage requirements...
- ...and CPU/battery requirements at the client side

User-centric secure multimedia services

User-centric secure multimedia services

Requirements

- Compatible with P2P Wi-Fi sharing architecture
- Minimize dependence on centralized infrastructure
- Low-cost equipment

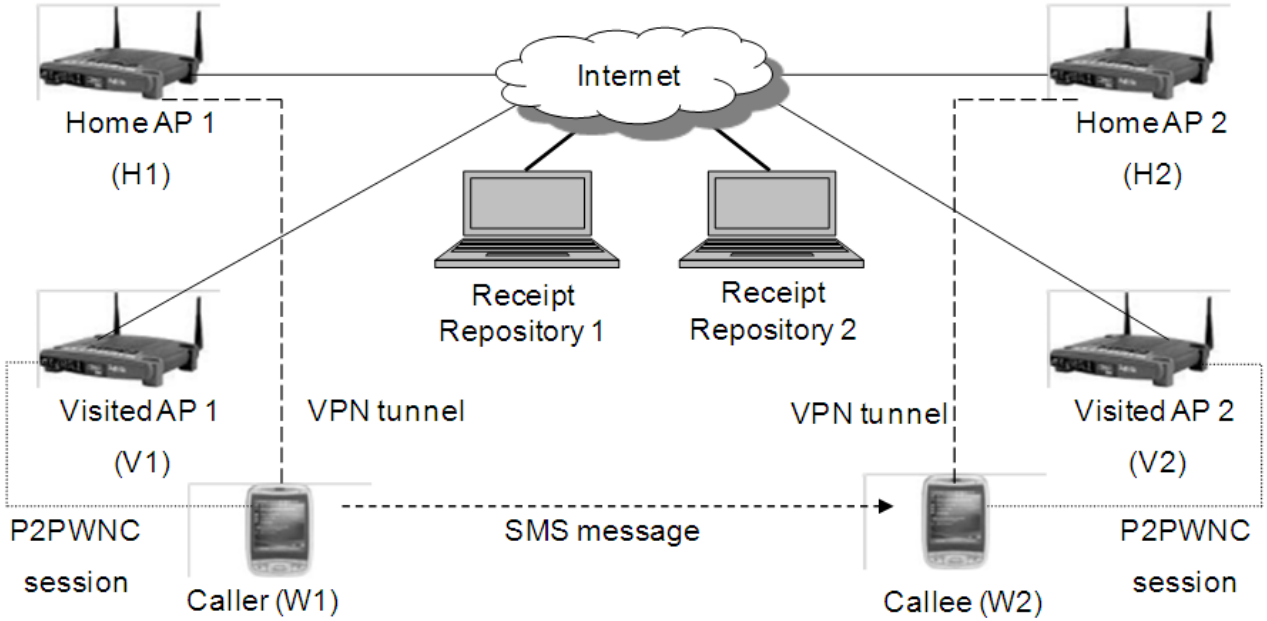
Challenges

- Secure comm. from untrusted networks/peers
- Legal implications
- Acceptable performance/QoE

Design highlights

- Tunneling through visited networks
- P2P VoIP/Multimedia service
- Off-band call setup

Architecture



Assumptions

- Peers operate home VPN GWs
- Know each other's GSM phone no

Discovery/call setup via external channel

- Caller sends SMS with home IP addr, call params

Steps

1. P2PWNC session establishment
2. VPN tunnel setup
3. VoIP call setup (caller sends SMS)
4. Callee responds with VoIP stream (W2-H2-H1-W1)

Experimental methodology

Measure voice capacity of typical P2PWNC-enabled WLAN

- P2PWNC protocol, VPN gateway
- Major quality degradation factors?
- Security overhead?

Call quality estimation

- Reduction of ITU's E-model to delay, packet loss, jitter buffer loss
- Output: R-score (estimate of Mean Opinion Score)
- R-score $< 70 \Rightarrow$ unacceptable quality

Parameters

- G.729a codec (50 pps, 20 bytes audio payload), 60 msec jitter buffer
- OpenVPN for tunnels

Testbed and results

HW and configuration

- Linksys WRT54GL AP (200MHz CPU, 16Mb RAM)
- NTP sync over Ethernet

Degradation factors

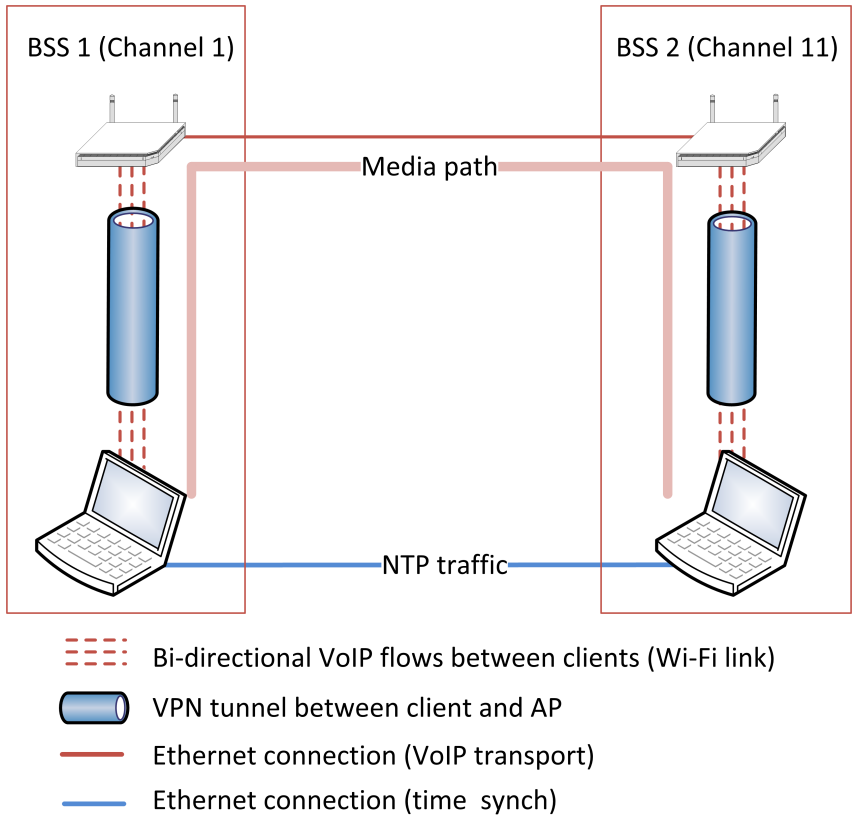
- Wi-Fi PHY/MAC overhead for small packets
- 2.4× packet expansion due to VPN
- Crypto overhead

Supported simultaneous VoIP calls

Scenario	# calls
Plain (11g)	30
Plain (11b)	7
VPN space overhead	21
VPN space+crypto overhead	**8**

P2PWNC RREQ frequency

- ECDSA RCPT verification time = 0.1 sec
- VPN+ECDSA: Support 8 calls w. 1 RREQ/10sec



Summary

User-centric approach

- First to propose (2006) a tunneling-based communications solution for WCNs
- Runs purely on user equipment
- Solves important security and legal issues
- Only relies on central infrastructure for discovery
- Inherently low-cost: off-the-shelf hw

Results

- All-in-one home router capable of a few secure calls
- Important *processing* overhead due to VPN
- 2 wireless hops $\Rightarrow$ increased per packet overhead due to IEEE 802.11 MAC/PHY

Related work

Efstathiou (2006, Ph.D. Dissertation) on P2P Wi-Fi sharing

- Underlying access scheme, requirements, assumptions

Tunneling-based approaches

- Sastry et al. (2007, ACM HotNets)
- Heer et al. (2008, IEEE P2P)

Signaling protocols

- SIP/H.323
- Need for (centralized) servers, proxies, registrars

P2PSIP (IETF WG, WiP)

- DHTs to distribute SIP core functionality
- Incompatible with P2PWNC

Crowdsourced Wi-Fi topology discovery

Motivation

The problem

- Very high Wi-Fi density in cities
- Uncontrolled and anarchic deployment
- Need a mechanism to discover Wi-Fi topology

Motivation

The problem

- Very high Wi-Fi density in cities
- Uncontrolled and anarchic deployment
- Need a mechanism to discover Wi-Fi topology

Use cases

- Detect cell overlaps and reconfigure...
  - ... via channel assignment or power control
- The case for Skyhook
  - Wi-Fi based positioning
  - Beacon DB built by war-driving

Motivation

The problem

- Very high Wi-Fi density in cities
- Uncontrolled and anarchic deployment
- Need a mechanism to discover Wi-Fi topology

Use cases

- Detect cell overlaps and reconfigure...
  - ... via channel assignment or power control
- The case for Skyhook
  - Wi-Fi based positioning
  - Beacon DB built by war-driving

A user-centric scheme

- *Crowdsource* the task to users
- Users with Wi-Fi capable devices (and maybe GPS...)
- *Robustness* issues emerge
  - Are users trustworthy?
  - How about faulty equipment?

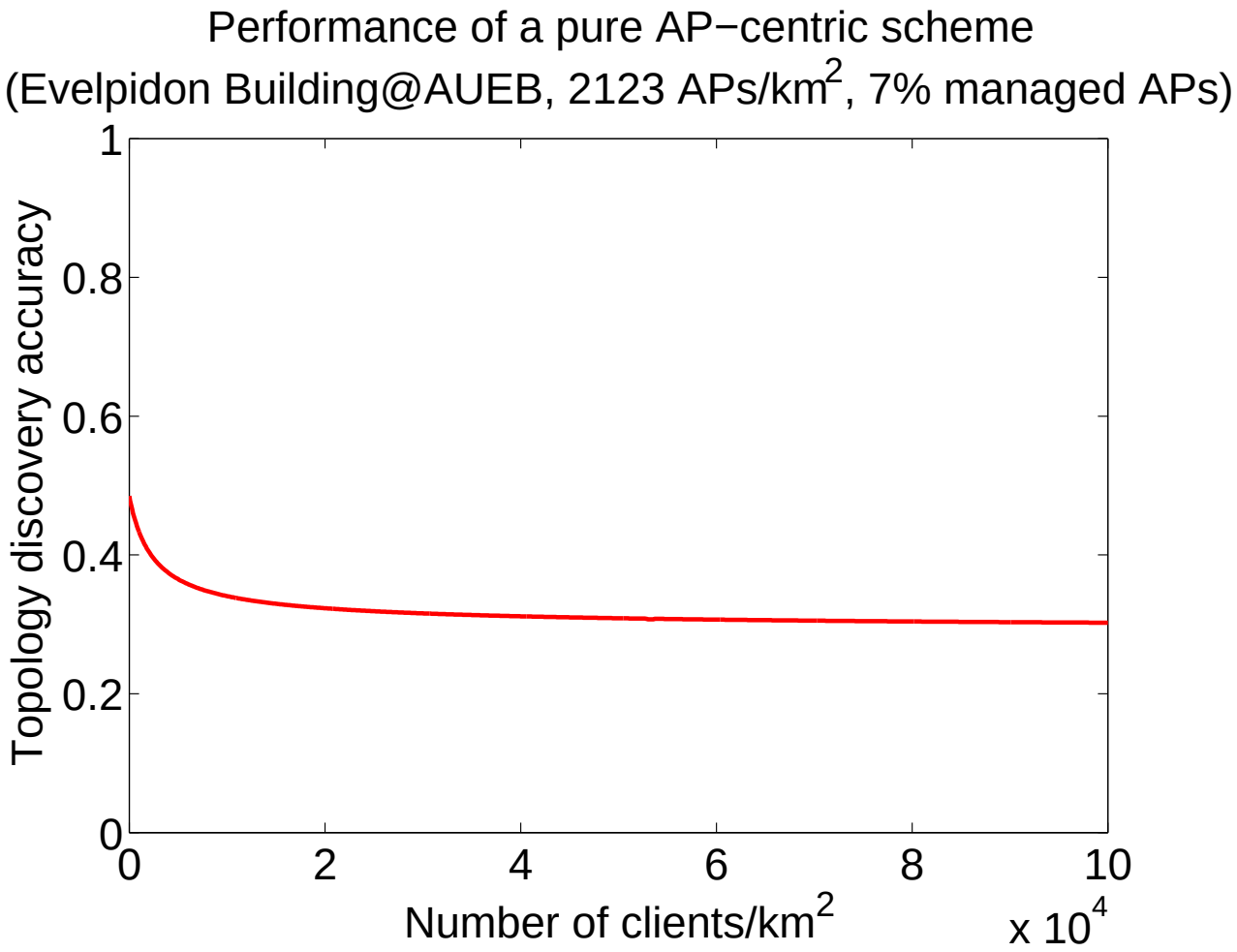
The need for a user-centric scheme

AP-centric scheme limitations

- Limited view of coverage
- Why not exploit user presence?

An example

- Evelpidon Building @ AUEB
- ∼7% of total APs in range managed
- Much information lost!



How about security and robustness?

Fake reporting

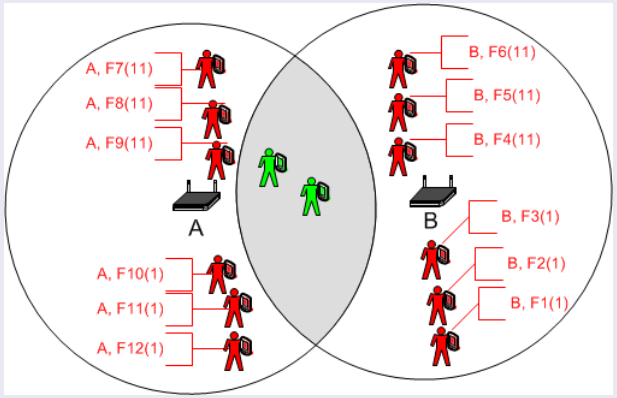
- The infrastructure is trusted
- Users are not
- User-provided information may not be valid!

Significance

- Affect spectrum sharing mechanisms
  - Lead to suboptimal channel selection or tx power assignment
- Wi-Fi-based positioning systems based on crowdsourcing

Attack impact on channel assignment: an example

Example topology



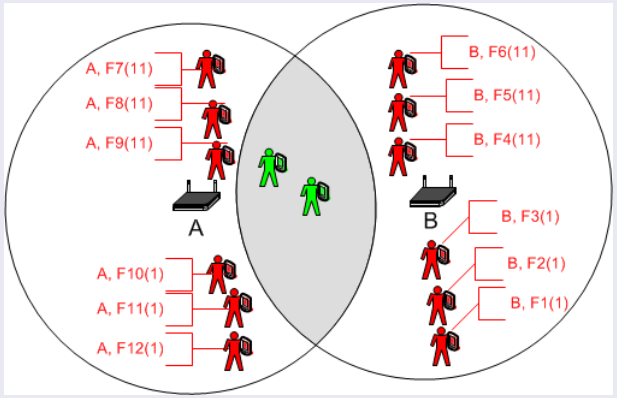
- Attackers report fake $< ID, Channel >$ pairs

CA based on graph coloring

- Channel $\Leftrightarrow$ color (3 for 11b/g)
- **Conflict edges** between vertices of the same color
- Select colors to minimize interference (sum of weights of conflict edges)

Attack impact on channel assignment: an example

Example topology

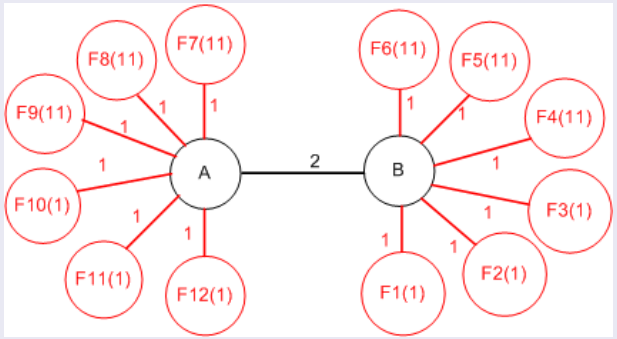


- Attackers report fake $< ID, Channel >$ pairs

CA based on graph coloring

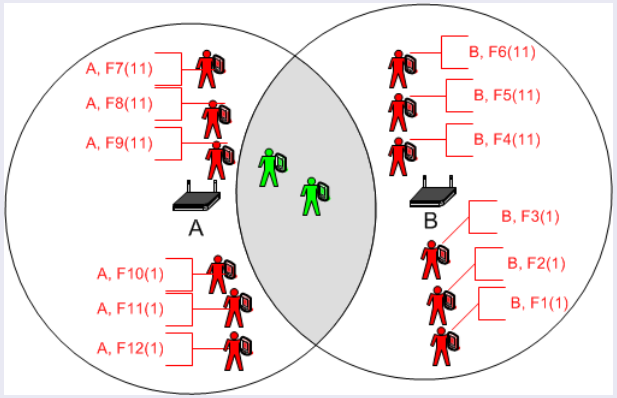
- Channel $\Leftrightarrow$ color (3 for 11b/g)
- **Conflict edges** between vertices of the same color
- Select colors to minimize interference (sum of weights of conflict edges)

Reported Coverage Graph



Attack impact on channel assignment: an example

Example topology

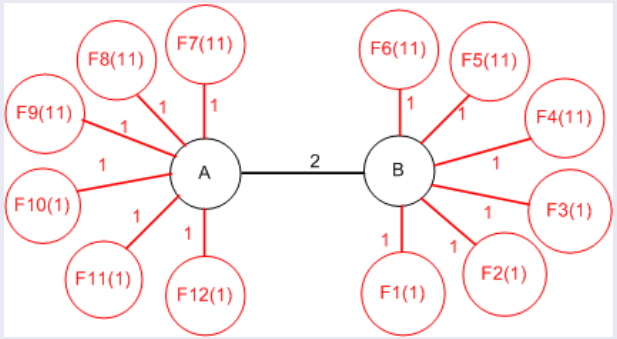


- Attackers report fake $< ID, Channel >$ pairs

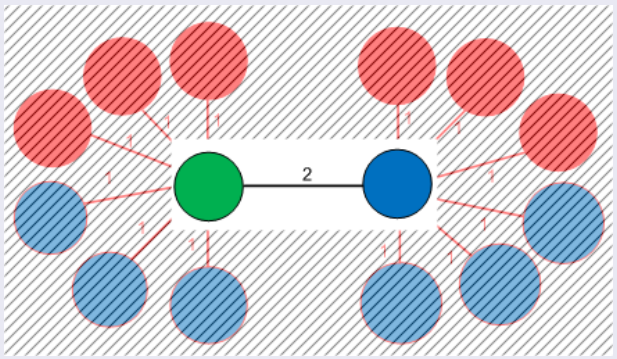
CA based on graph coloring

- Channel $\Leftrightarrow$ color (3 for 11b/g)
- **Conflict edges** between vertices of the same color
- Select colors to minimize interference (sum of weights of conflict edges)

Reported Coverage Graph

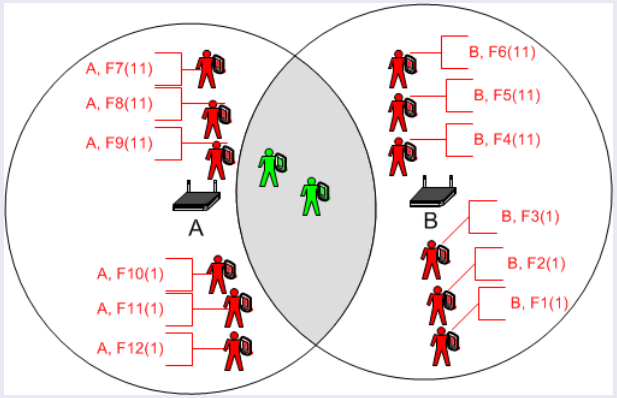


Optimal channel assignment



Attack impact on channel assignment: an example

Example topology

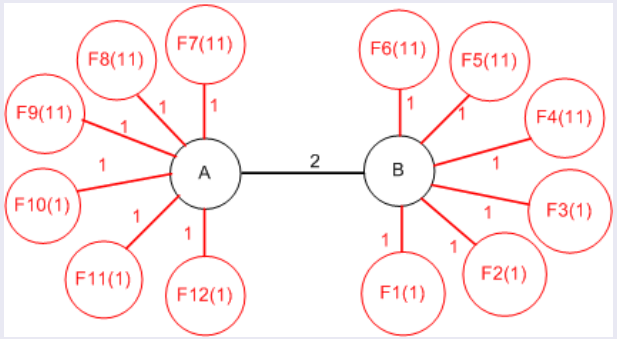


- Attackers report fake $< ID, Channel >$ pairs

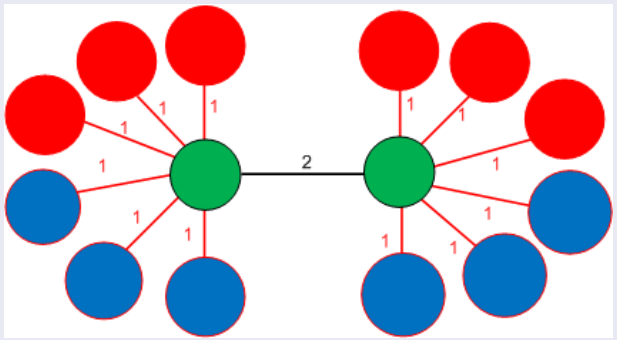
CA based on graph coloring

- Channel $\Leftrightarrow$ color (3 for 11b/g)
- **Conflict edges** between vertices of the same color
- Select colors to minimize interference (sum of weights of conflict edges)

Reported Coverage Graph

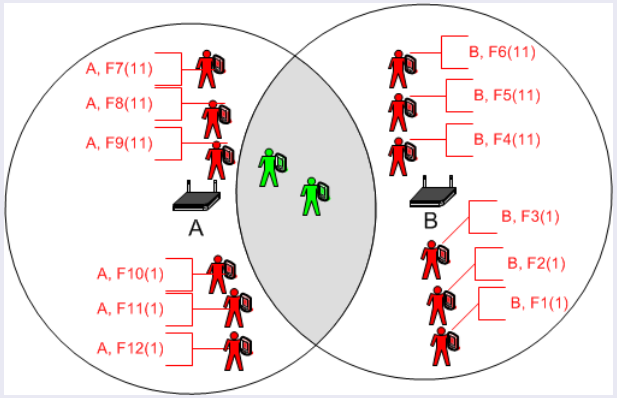


Resulting channel assignment!



Attack impact on channel assignment: an example

Example topology

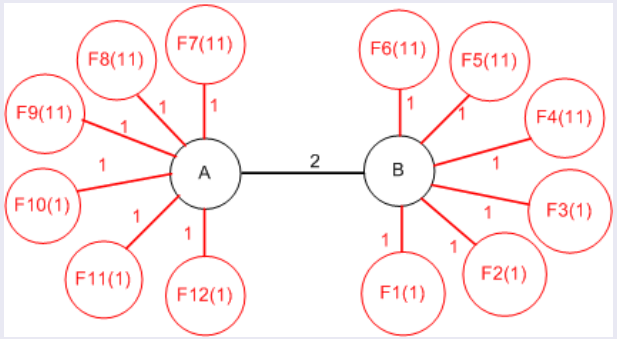


- Attackers report fake $< ID, Channel >$ pairs

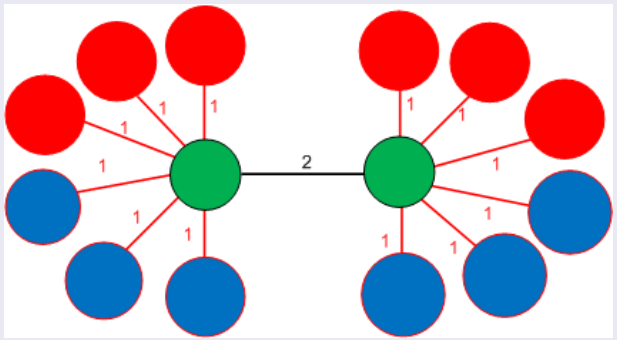
CA based on graph coloring

- Channel $\Leftrightarrow$ color (3 for 11b/g)
- **Conflict edges** between vertices of the same color
- Select colors to minimize interference (sum of weights of conflict edges)

Reported Coverage Graph



Resulting channel assignment!



Performance effects

Simulations show dramatic throughput reduction

Our approach

Networking environment

- Managed Wi-Fi deployments
- Centralized AAA
- Examples: Corporate/Campus Wi-Fi, WISP aggregator

Authenticated users report wireless coverage at their spot

- **IEEE 802.11i** for security/authentication, **IEEE 802.11k** for reports
- When requested, each user reports about the APs is range (ESSID, channel, ...)
- Managed APs provide **trusted** info
- Coverage Graph is built

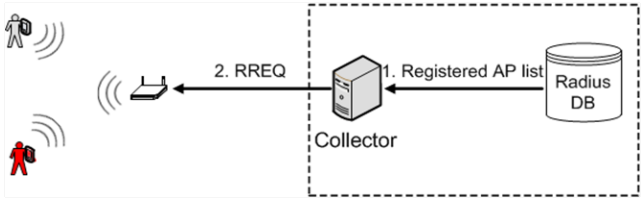
User reputations and consensus-based report evaluation

- Sum of reports about overlapping coverage between 2 APs should exceed a threshold
- Report weighted based on user reputation
- User score $= \frac{\text{validated info}}{\text{reported info}}$
- Reputation updates: $r_i = \beta r_{i-1} + (1 - \beta) score_i$

Architecture

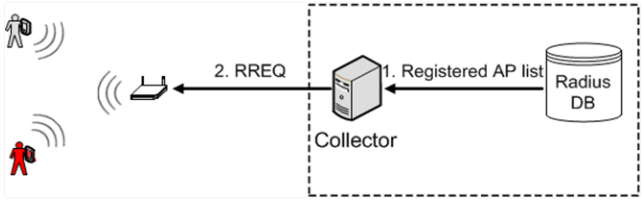
Architecture

A. Collector requests for reports from managed APs

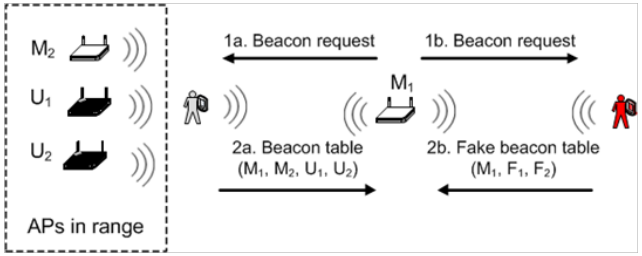


Architecture

A. Collector requests for reports from managed APs

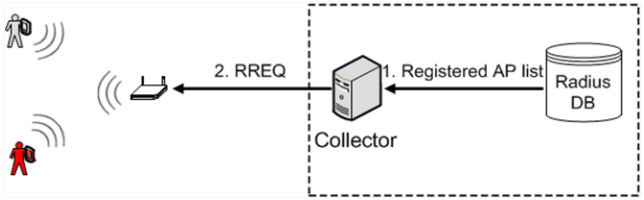


B. AP collects reports from clients using IEEE 802.11k

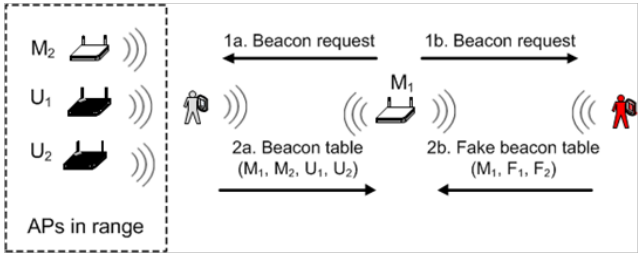


Architecture

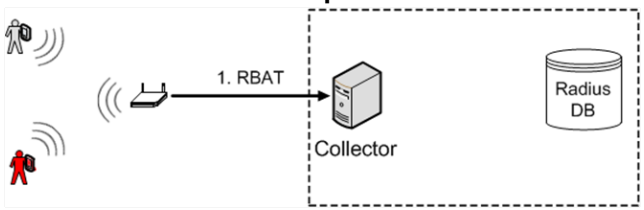
A. Collector requests for reports from managed APs



B. AP collects reports from clients using IEEE 802.11k

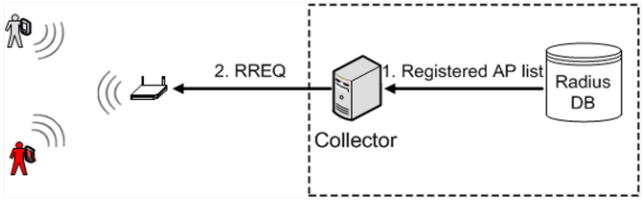


C. AP sends report batch to collector

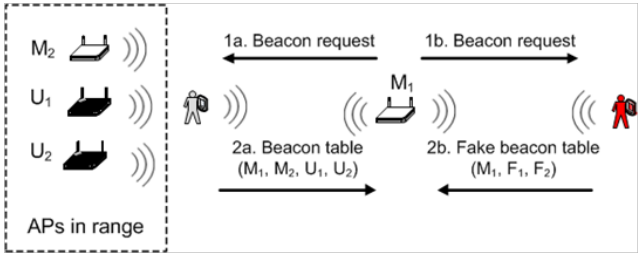


Architecture

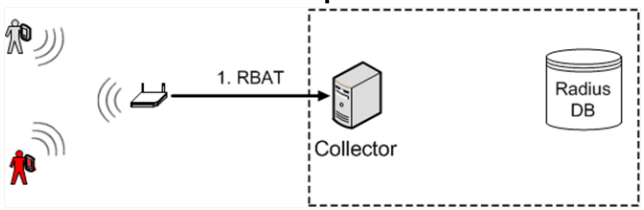
A. Collector requests for reports from managed APs



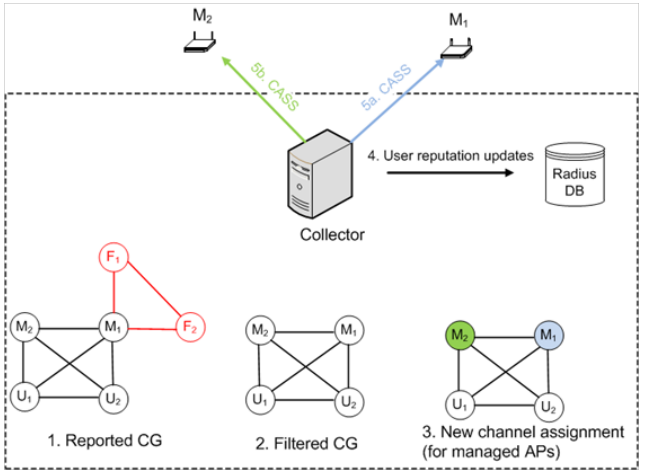
B. AP collects reports from clients using IEEE 802.11k



C. AP sends report batch to collector

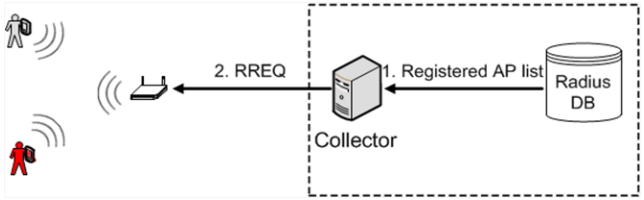


D. End of reporting round: filtering, reputation updates, new channel assignment

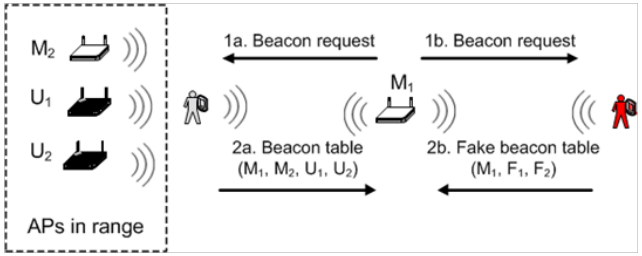


Architecture

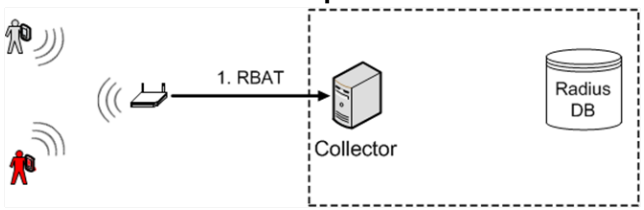
A. Collector requests for reports from managed APs



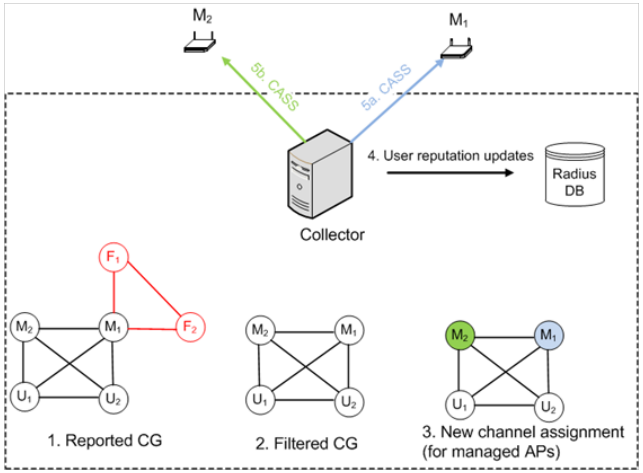
B. AP collects reports from clients using IEEE 802.11k



C. AP sends report batch to collector



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



Implementation

- Subset of IEEE 802.11k (mac80211, Linux Kernel 2.6.38) and reporting attacks
- Radius auth, EAP-PEAP, WPA2-AES
- Atheros AR5213 Wi-Fi cards (MadWifi)

Attacks and countermeasures

Attacker model

- Independent attackers
- Each submits a random fake set of AP IDs
- Fake CG edge weight = user reputation (< 1.0)
- Some users always truthful, some potential attackers (with prob. p_a)

Countermeasures

- Users begin with zero reputation (untrusted by default)
- AP-based measurements help audit user reports
- Edges with weight $< T = 1.0$ are filtered $\Rightarrow$ all fake edges removed

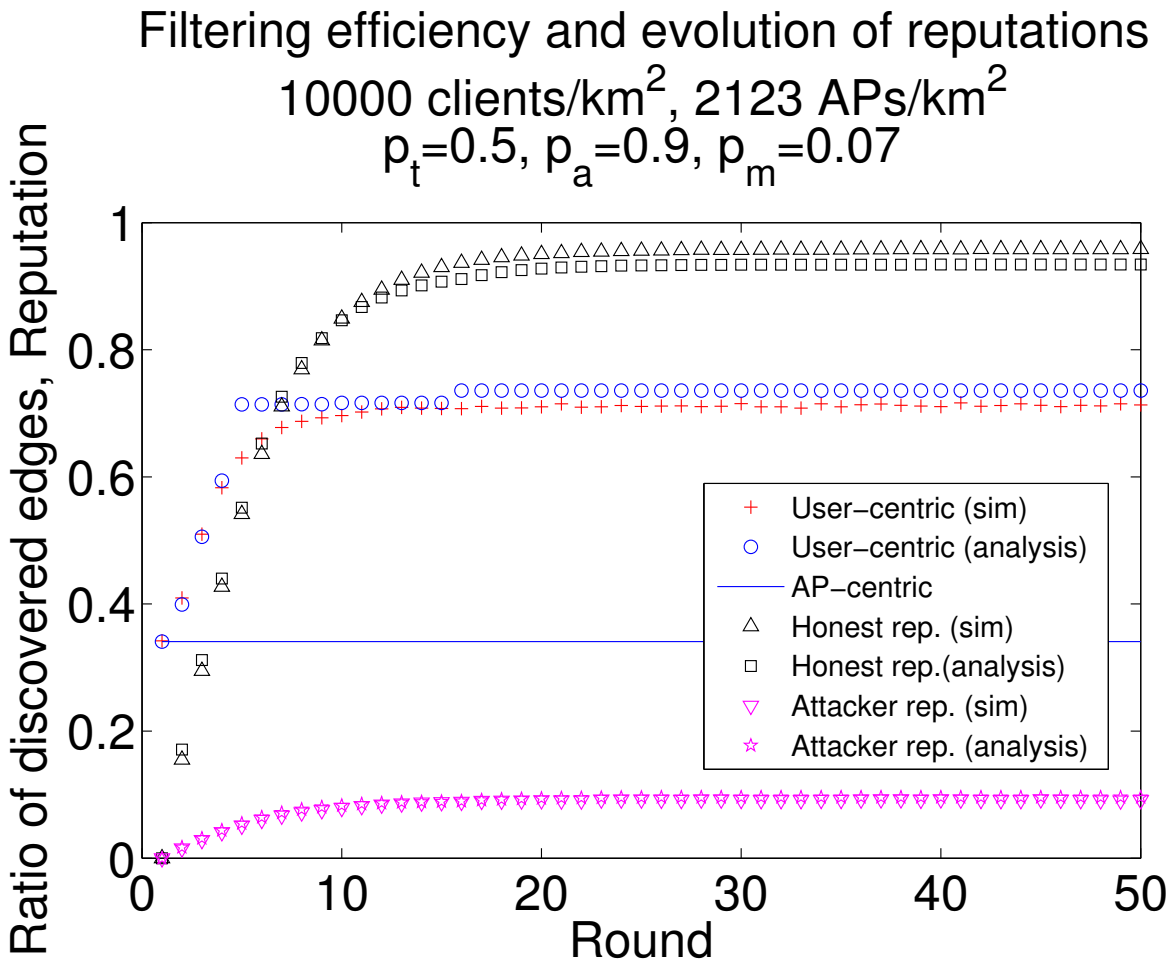
Evaluation metric

- % discovered CG edges
- We only face false negatives (missed real edges)

Performance

User- vs AP-centric schemes

- AP-centric scheme: lower bound
- Improved accuracy even in the presence of many attackers



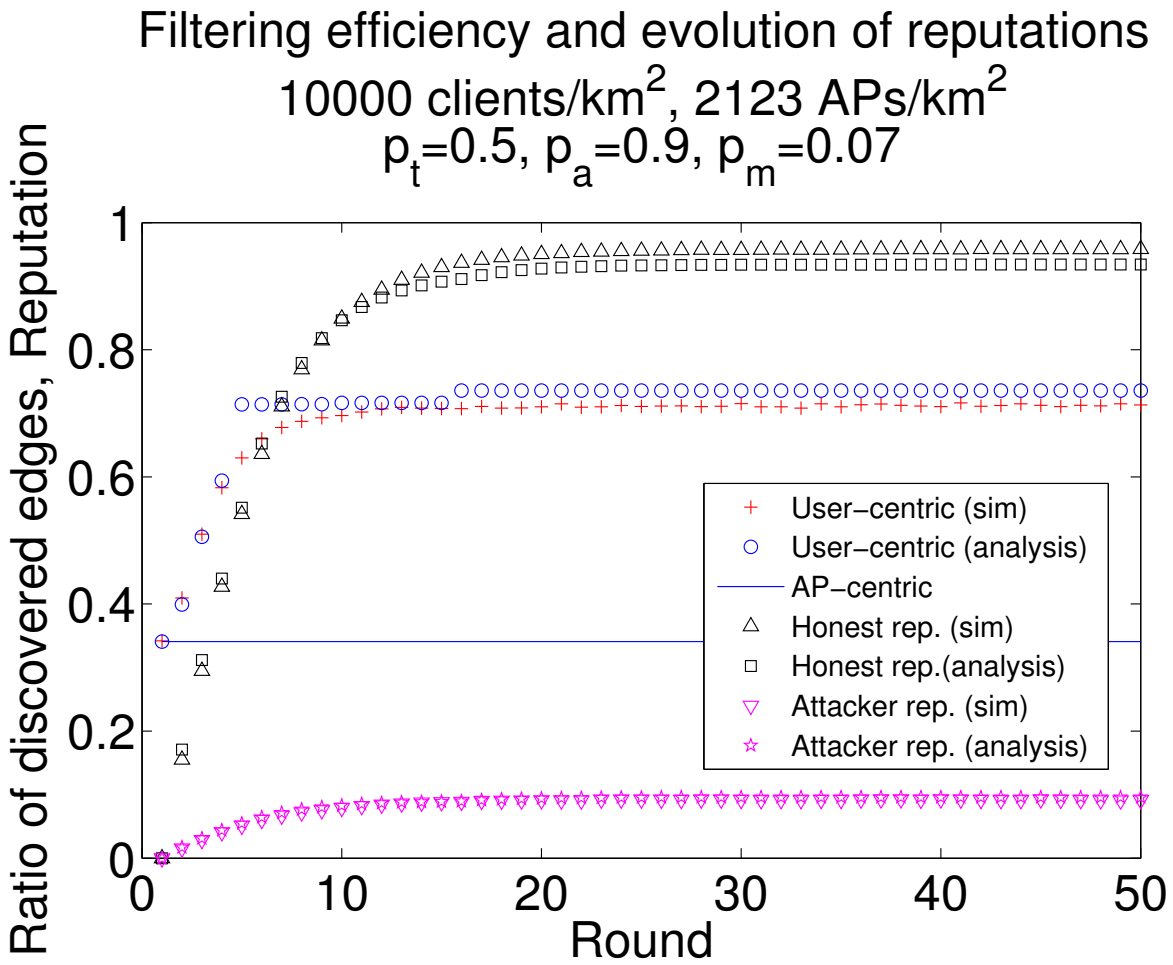
Performance

User- vs AP-centric schemes

- AP-centric scheme: lower bound
- Improved accuracy even in the presence of many attackers

Evolution of reputations

- Honest users are "promoted"
- Attacker reputation is bounded



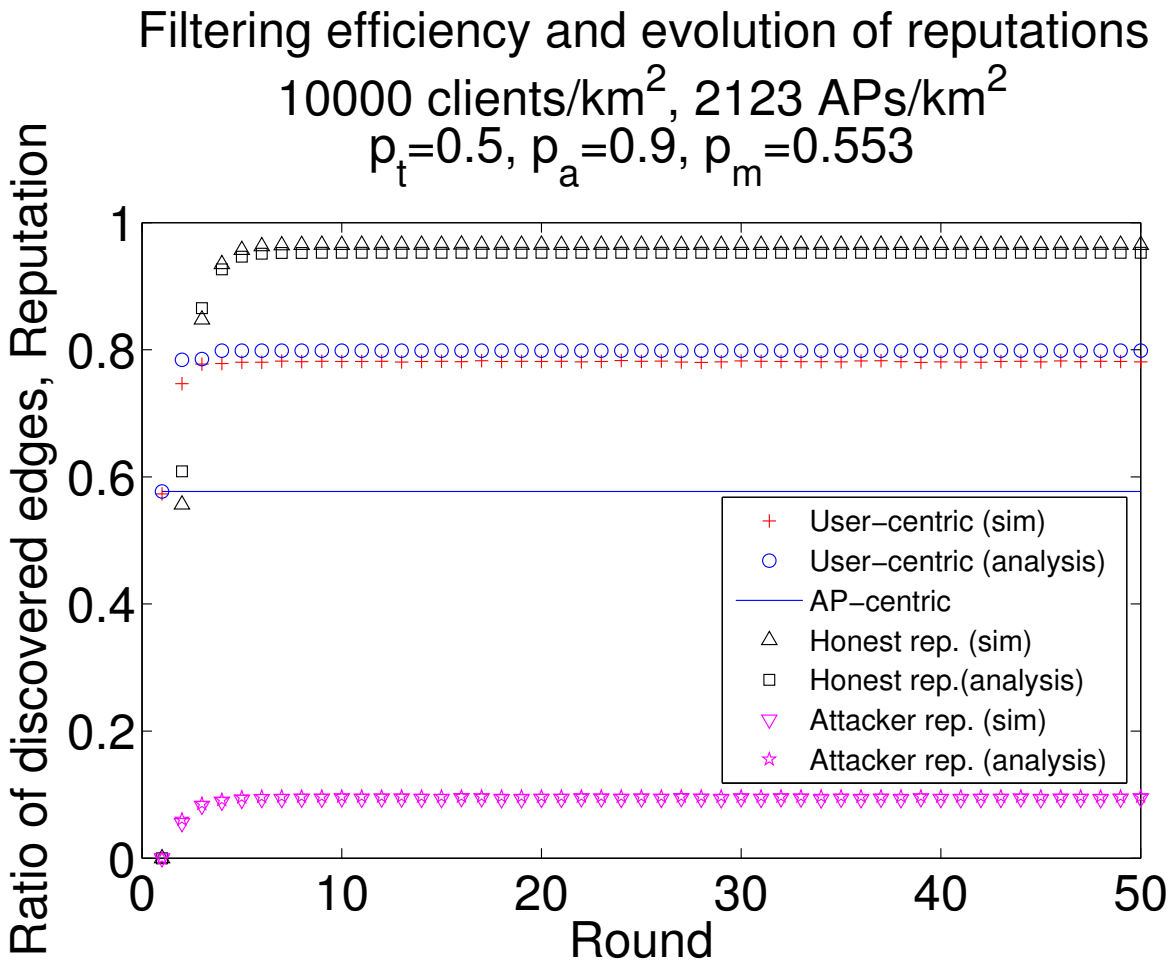
Performance

User- vs AP-centric schemes

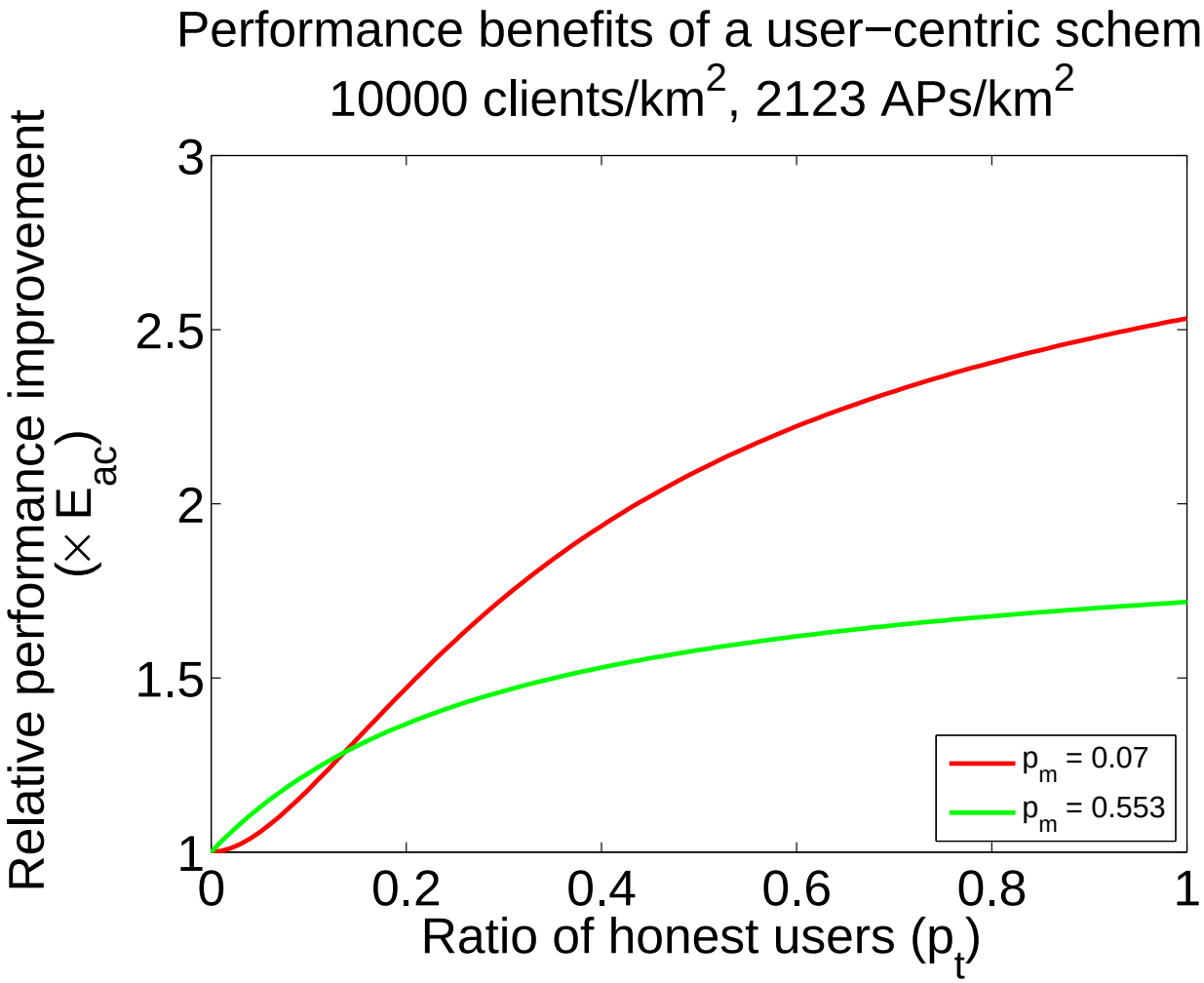
- AP-centric scheme: lower bound
- Improved accuracy even in the presence of many attackers

Evolution of reputations

- Honest users are "promoted"
- Attacker reputation is bounded



Relative efficiency



Summary

User-centric approach

- Reduce monitoring infrastructure cost by crowdsourcing
- Tackle attacks by untrusted users
- Decentralization by default
- Open participation: Users may or may not contribute
  - Enforcing participation could be tackled at another layer

Summary of results

- User-centrism offers increased topology discovery accuracy
  - $> 2\times$ improvement in realistic settings...
  - ...even with $> 50\%$ attackers
- Simple but **realistic** attacks are countered
  - Consistent attackers achieve low reputation
  - Without collusion, all fake reports are filtered

Related work

Wireless topology models

- Graph representation of cell overlap for channel assignment (Mishra et al., ACM MC2R 2005)

Wi-Fi-based positioning

- Crowdsourcing helps (Skyhook, Google, Apple, MS already do it!)
- Tippenhauer et al. identify the effects of fake reporting (2009, ACM Mobisys)

Distributed spectrum sensing for Cognitive Radio Networks

- Purpose: Detect primary user presence
- Chen et al. on PU emulation and fake reporting (2008, IEEE Communications Magazine)
- Similar motivation, different context

IEEE 802.11k

- IEEE std for radio resource measurements
- Does not address security issues

Conclusion

Conclusion

User-centric approach to wireless networking

- Reconsidered the role of users as consumers
- User empowerment
- Exploited centralized schemes to offer decentralized solutions
- Tackled security, reliability and performance challenges

Future work

Wireless Community Networks

- Structure characterization using empirical data
- Realistic topology generators

P2P multimedia services

- Performance optimizations
- Dealing with user mobility

Crowdsourced topology discovery

- More sophisticated attacks and countermeasures
- Effects on Wi-Fi-based postitioning
- Alternative uses of topology info (handover planning, and more...)

Coupling access, service and feedback provision

- High reputations $\Rightarrow$ QoS, better access opportunities
- Incentives for participation and honest behavior

Thank you!

Publications (I)

Wi-Fi sharing & service architectures

- E. Dimopoulos, P.A. Frangoudis, and G.C. Polyzos, "Exploiting super peers for large-scale peer-to-peer Wi-Fi roaming," Proc. IEEE Globecom 2010 Workshop on Advances in Communications and Networks (User-Provided Networking session), 2010.
- E.C. Efstahiou, P.A. Frangoudis, and G.C. Polyzos, "Controlled Wi-Fi Sharing in Cities: a Decentralized Approach Relying on Indirect Reciprocity," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1147-1160, August 2010.
- P.A. Frangoudis and G.C. Polyzos, "Coupling QoS Provision with Interference Reporting in WLAN sharing Communities," Proc. IEEE PIMRC 2008 Workshops, Cannes, France, September 2008.
- P.A. Frangoudis, V.P. Kemerlis, D.C. Paraskevaidis, E.C. Efstathiou, and G.C. Polyzos, "Experimental Evaluation of Community-based WLAN Voice and Data Services," Proc. ACM/ICST MobiMedia 2007, Nafpaktos, Greece, August 2007.
- P.A. Frangoudis and G.C. Polyzos, "Peer-to-Peer Secure and Private Community Based Multimedia Communications," Proc. 2nd IEEE International Workshop on Security and Pervasive Multimedia Environments (MultiSec 2006), San Diego, CA, December 2006.
- E.C. Efstathiou, F.A. Elianos, P.A. Frangoudis, V.P. Kemerlis, D.C. Paraskevaidis, E.C. Stefanis, and G.C. Polyzos, "Public Infrastructures for Internet Access in Metropolitan Areas," Proc. 1st International Conference on Access Networks (AccessNets 2006), Athens, Greece, September 2006.
- E. C. Efstathiou, F. A. Elianos, P. A. Frangoudis, V. P. Kemerlis, D. C. Paraskevaidis, G. C. Polyzos, and E. C. Stefanis, "Practical Incentive Techniques for Wireless Community Networks," Proc. ACM MobiSys 2006 Demo Session, Uppsala, Sweden, June 2006.
- E.C. Efstathiou, F.A. Elianos, P.A. Frangoudis, V.P. Kemerlis, D.C. Paraskevaidis, G.C. Polyzos, and E.C. Stefanis, "Building Secure Media Applications over Wireless Community Networks," Proc. 13th Annual Workshop of the HP Openview University Association (HP-OVUA) Poster/Demo Session, May 2006.
- E.C. Efstathiou, P.A. Frangoudis, and G.C. Polyzos, "Stimulating Participation in Wireless Community Networks," Proc. IEEE INFOCOM 2006, Barcelona, Spain, April 2006.
- E.C. Efstathiou, F.A. Elianos, P.A. Frangoudis, V.P. Kemerlis, D.C. Paraskevaidis, G.C. Polyzos, and E.C. Stefanis, "The Peer-to-Peer Wireless Confederation Scheme," IEEE INFOCOM 2006 Demo Session, Barcelona, Spain, April 2006.
- E.C. Efstathiou, F.A. Elianos, P.A. Frangoudis, V.P. Kemerlis, D.C. Paraskevaidis, G.C. Polyzos, and E.C. Stefanis, "The Peer-to-Peer Wireless Confederation Scheme: Protocols, Algorithms, and Services," Proc. IEEE/CreateNet TridentCom 2006 Demo Session, Barcelona, Spain, March 2006.
- P.A. Frangoudis, E.C. Efstathiou, and G.C. Polyzos, "Reducing Management Complexity through Pure Exchange Economies: A Prototype System for Next Generation Wireless/Mobile Network Operators," 12th Annual Workshop of the HP Openview University Association (HP-OVUA), Porto, Portugal, July 2005.

Publications (II)

Wireless Community Networks

- P.A. Frangoudis, G.C. Polyzos, and V.P. Kemerlis, "Wireless Community Networks: An Alternative Approach for Broadband Nomadic Network Access", *IEEE Communications Magazine*, vol. 49, no. 5, pp. 206-213, May 2011.
- F.A. Elianos, G. Plakia, P.A. Frangoudis, and G.C. Polyzos, "Structure and Evolution of a Large-Scale Wireless Community Network," Proc. IEEE WoWMoM 2009, Kos, Greece, June 2009.

Wi-Fi topology discovery

- P.A. Frangoudis and G.C. Polyzos, "Robust crowdsourcing for accurately determining Wi-Fi topology," in preparation, 2012.
- P.A. Frangoudis, D.I. Zografos, and G.C. Polyzos, "Robust client-based Wi-Fi topology discovery," Proc. IEEE CCNC 2011.
- P.A. Frangoudis and G.C. Polyzos, "Report-based topology discovery schemes for centrally-managed Wi-Fi deployments," Proc. NGI 2010, Paris, France, June 2010.
- P.A. Frangoudis, D.I. Zografos, and G.C. Polyzos, "Secure Interference Reporting for Dense Wi-Fi Deployments," Proc. ACM CoNEXT 2009 Student Workshop, Rome, Italy, December 2009.

Cognitive Radio security

- G.C. Polyzos, G.F. Marias, S. Arkoulis, P.A. Frangoudis, M. Fiedler, A. Popescu, H. de Meer, R. Herkenhöner, A. Fischer, and J.O. Oberender, "ASPECTS: Agile spectrum security," Proc. NGI 2011, Kaiserslautern, Germany, June 2011.
- S. Arkoulis, I. Marias, P.A. Frangoudis, J. Oberender, A. Popescu, M. Fiedler, H. de Meer, and G.C. Polyzos, "Misbehaviour Scenarios in Cognitive Radio Networks," *Future Internet*, vol. 2, no. 3, pp. 212-237, 2010.
- S. Arkoulis, M. Fiedler, P.A. Frangoudis, R. Herkenhoner, G.F. Marias, H. de Meer, and G.C. Polyzos, "Distributed Spectrum Sensing for Spectrum Agility: Incentives and Security Considerations," Proc. 1st Euro-NF Workshop on Future Internet Architectures, Paris, France, November 2008.
- P.A. Frangoudis, S. Arkoulis, G.F. Marias, and G.C. Polyzos, "Incentives and Security Considerations in Distributed Spectrum Sensing," Proc. 1st Euro-NF Socioeconomics Workshop, Athens, Greece, October 2008 (extended abstract).

Publications (III)

Misc

- E.A. Panaousis, P.A. Frangoudis, C.N. Ververidis, and G.C. Polyzos, "Optimizing the Channel Load Reporting Process in IEEE 802.11k-enabled WLANs," Proc. IEEE LANMAN 2008, Cluj-Napoca, Transylvania, Romania, September 2008.
- K. Katsaros, P.A. Frangoudis, G.C. Polyzos, and G. Karlsson, "Design Challenges of Open Spectrum Access," Proc. IEEE PIMRC 2008 Workshops, Cannes, France, September 2008.
- V.G. Douros, P.A. Frangoudis, K. Katsaros, and G.C. Polyzos, "Power Control in WLANs for Optimization of Social Fairness," Proc. 12th Pan-Hellenic Conference on Informatics (PCI 2008), Samos, Greece, August 2008.
- N.N. Leontiadis, V.P. Kemerlis, P.A. Frangoudis, and G.C. Polyzos, "Secure Network Management Using a Key Distribution Center," Proc. 2007 Workshop of the HP Software University Association (HP-SUA) Poster Session, Garching/Munich, Germany, July 2007.

Preliminaries (I)

Assumptions

- Homogeneous PPP distribution of APs/users
- Some APs are managed (p_m)
- AP coverage: Disk of fixed radius (R)
- $A(x)$: area of overlap between d-distance APs
- Isolated users: no edges to report
- Two types of users
  - Always honest: p_t
  - Potential attackers: p_a
- Managed APs always honest

Evaluation metric

$$\mathcal{E} = \frac{N_d^{(1)} + N_d^{(2)}}{N_e^{(1)} + N_e^{(2)}}$$

- $N_d^{(*)}$: Discovered Type-* edges
- $N_e^{(*)}$: Existing Type-* edges
- *={1,2}

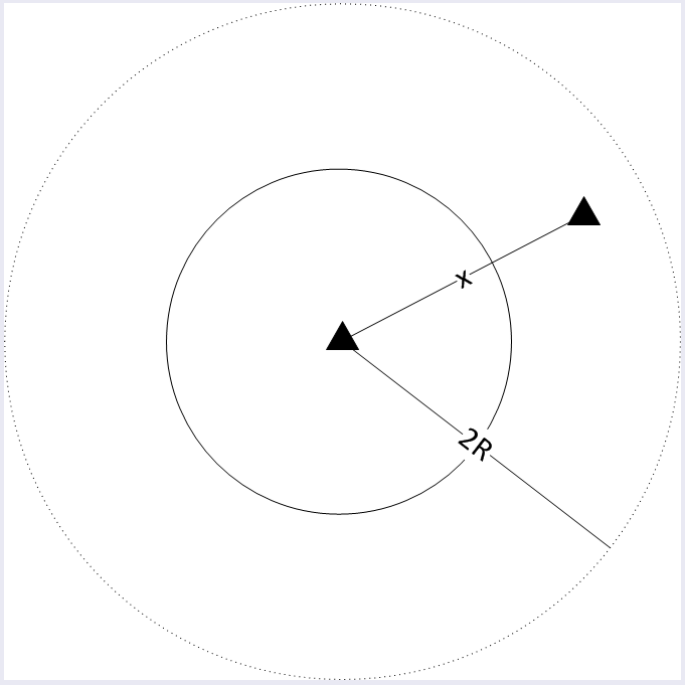
Number of CG edges

- $N_e^{(1)} = N_{pe} F_X(R)$
- $N_e^{(2)} = N_{pe} \int_R^{2R} f(x)(1 - e^{-(\lambda_c + \lambda_{AP})A(x)})dx$
- N_{pe}: # potential edges (cell overlap involving managed AP)

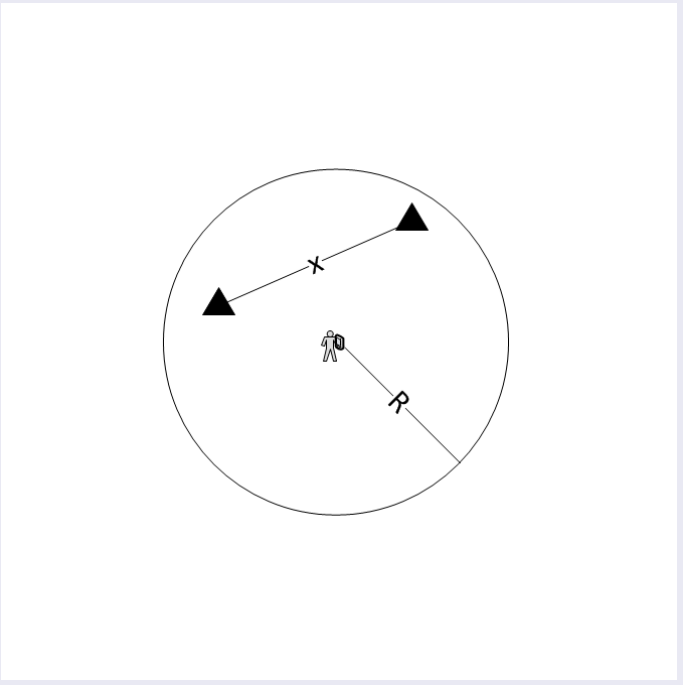
Preliminaries (II)

Distance distributions

- $F_X(x)$: distance between an AP and a random neighbor



- $L_X(x)$: distance between two APs in range of a client



Performance of an AP-centric scheme

Only managed APs report

- Type-1 edges always reported by at least one mAP
- Type-2 edges w/o a mAP located there: **missed**

Discovery probability for a Type-2 x-distance edge

$$P_d^{(2)}(x) = 1 - (1 - e^{-(\lambda_u+\lambda_c)A(x)})e^{-\lambda_m A(x)}$$

Number of discovered Type-2 edges

$$N_d^{(2)} = N_{pe} \int_R^{2R} f(x)P_d(x)dx$$

Performance of a user-centric scheme

Edge discovery conditions

- At least 1 mAP in the overlapping region, or
- Sum of client report weights meets threshold

Number of discovered Type-2 edges

$$N_d^{(2)} = N_{pe} \int_R^{2R} f(x) P_d^{(i)}(x) dx$$

Contribution to the weight of an edge

- A: # mAP, X: # honest users, Y: # **non-attacking** potential attackers at round i
- Assume $A = 0$, $X = j$, $Y = k$
- If honest users contribute $j\overline{r_t^{(i)}} < T$, then $> T - j\overline{r_t^{(i)}}$ should be contributed by non-attackers
- **Success** when $k \geq \frac{T - j\overline{r_t^{(i)}}}{\overline{r_a^{(i)}}}$

Discovery probability for a Type-2 x-distance edge

$$P_d^{(i)}(x) = 1 - \sum_{j=0}^{\left\lfloor \frac{T}{\overline{r_t^{(i)}}} \right\rfloor} \sum_{k=0}^{\left\lfloor \frac{T - j\overline{r_t^{(i)}}}{\overline{r_a^{(i)}}} \right\rfloor} Pr\{A = 0\} Pr\{X = j\} Pr\{Y = k\}$$

Reputation updates

Honest users

- Reputation updated based on score
- Isolated users (prob. p_i) do not get reputation update

$$\overline{r_t^{(i+1)}} = p_i \overline{r_t^{(i)}} + (1 - p_i)(b\overline{r_t^{(i)}} + (1 - b)\overline{s_t^{(i)}})$$

Potential attackers

- Attackers get zero score, reputation discounted
- Those who cooperate contribute to the avg attacker reputation

$$\overline{r_a^{(i+1)}} = p_i \overline{r_a^{(i)}} + (1 - p_i)\{p_a b\overline{r_a^{(i)}} + (1 - p_a)\left[b\overline{r_a^{(i)}} + (1 - b)\overline{s_a^{(i)}}\right]\}$$

Score calculation

- Focus on average score of honest users, with $\overline{r_a^{(i)}}$ reputation
- Use $L_X(x)$

Define the following events:

- D: $x-$distance edge discovered.
- B: $x-$distance edge reported by ≥ 1 honest user ($X > 0$)
- C: Sum of **client** reports $\geq$ T

Edge discovered given that it is reported by the user

$$P_s(x) = Pr\{D|B\} = \frac{Pr\{D \cap B\}}{Pr\{B\}}$$

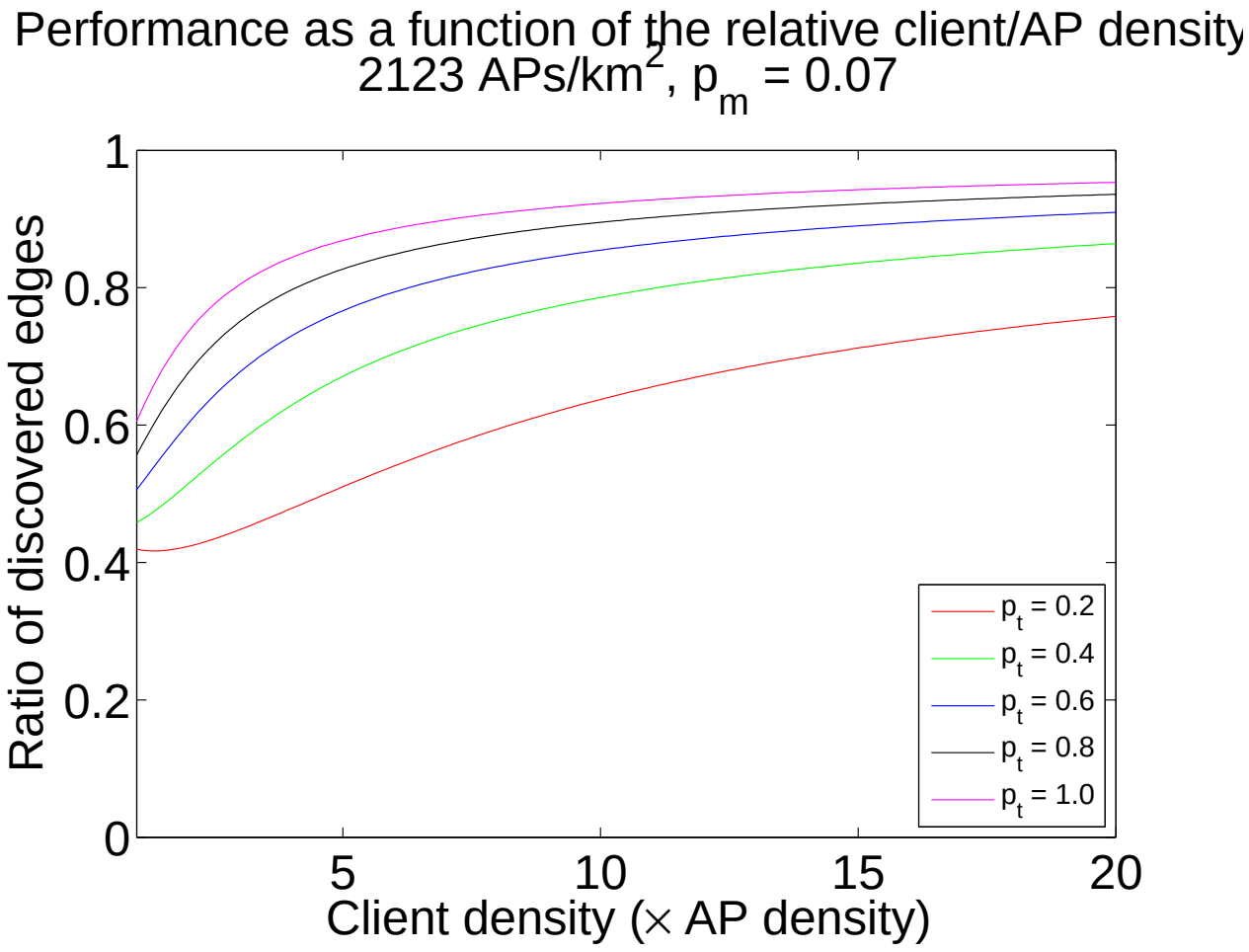
- $Pr\{B\}$ follows from Poisson distribution
- $Pr\{C\}$: Similar approach as with $P_d^{(i)}(x)$

$Pr\{D \cap B\}$ calculation

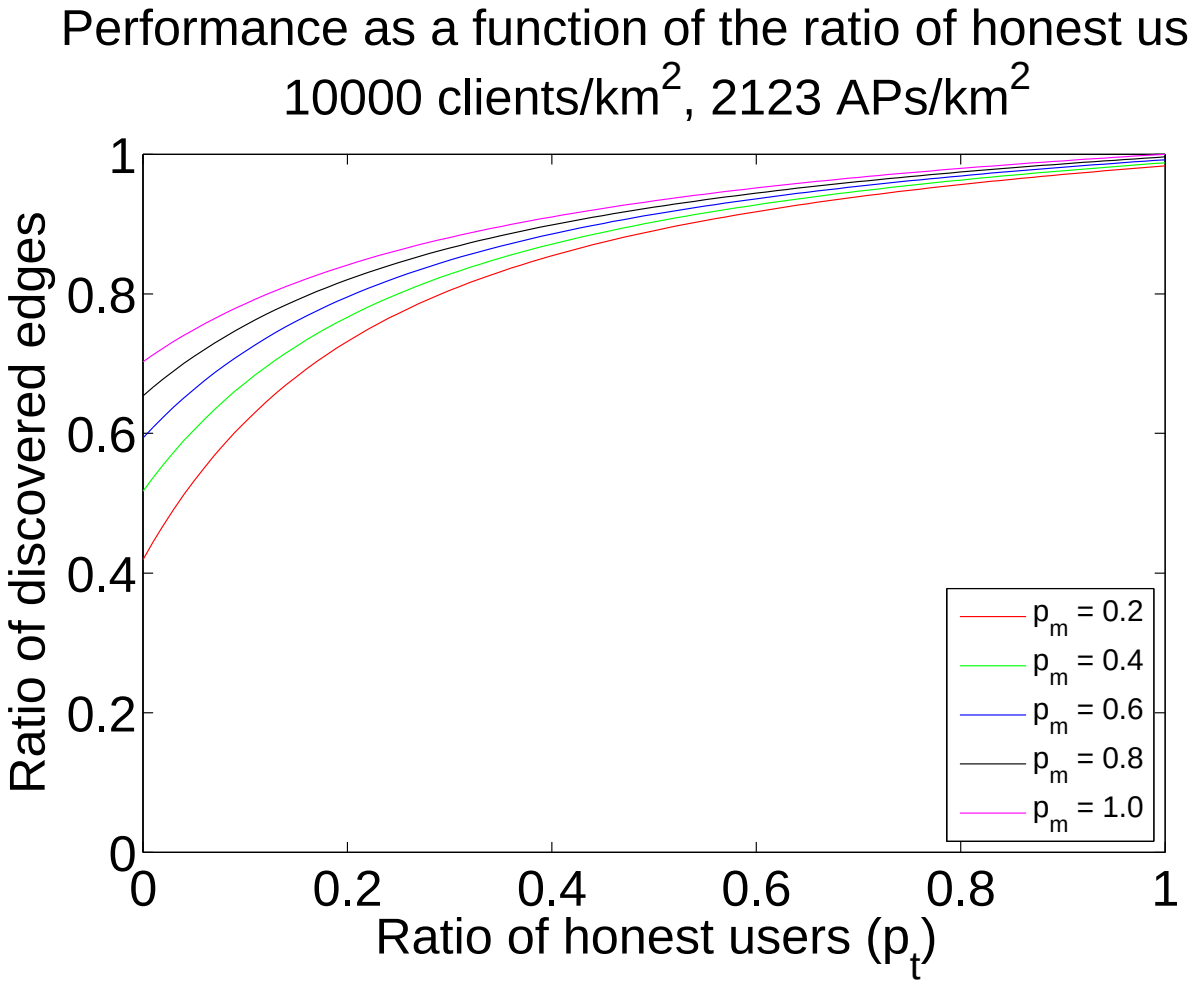
- Reported by **mAP** ($\Rightarrow$ discovered) AND **reported by user**, or
- Reported by **0 mAP** AND by **many clients** ($\Rightarrow$ discovered), at least least 1 of them truthful...
  - ...i.e., $Pr\{A = 0\}Pr\{B \cap C\}$

$$Pr\{D \cap B\} = Pr\{A > 0\}Pr\{B\} + Pr\{A = 0\}Pr\{B \cap C\}$$

Dependence on client density



Dependence on the ratio of honest users



Upper bounds on VoWLAN capacity (I)

Configuration and assumptions

- Both call endpoints over IEEE 802.11g
- Assume no collisions, $T_{DCF} \approx \frac{CW_{min}}{2} \times T_{SLOT} = 8 \times T_{SLOT}$
- G.729a, 20 bytes audio pld, $R_a = 16Kbps$

Throughput model

$$S = \frac{T_P}{T_P + T_{Overhead}} \times R$$

Number of VoIP calls

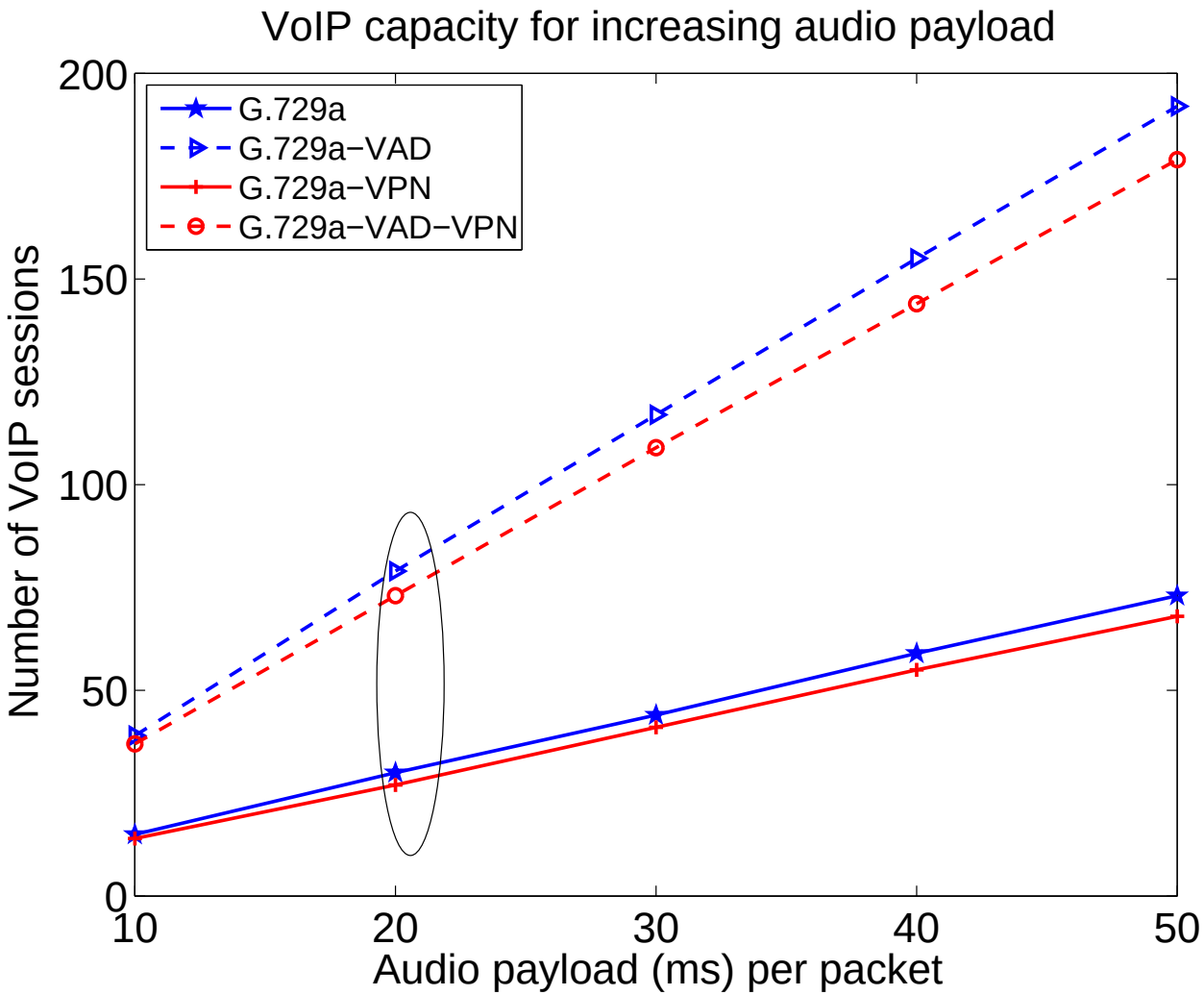
$$n_{max} = \left\lfloor \frac{T_P \times R}{(T_P + T_{Overhead}) \times R_a} \right\rfloor,$$

where

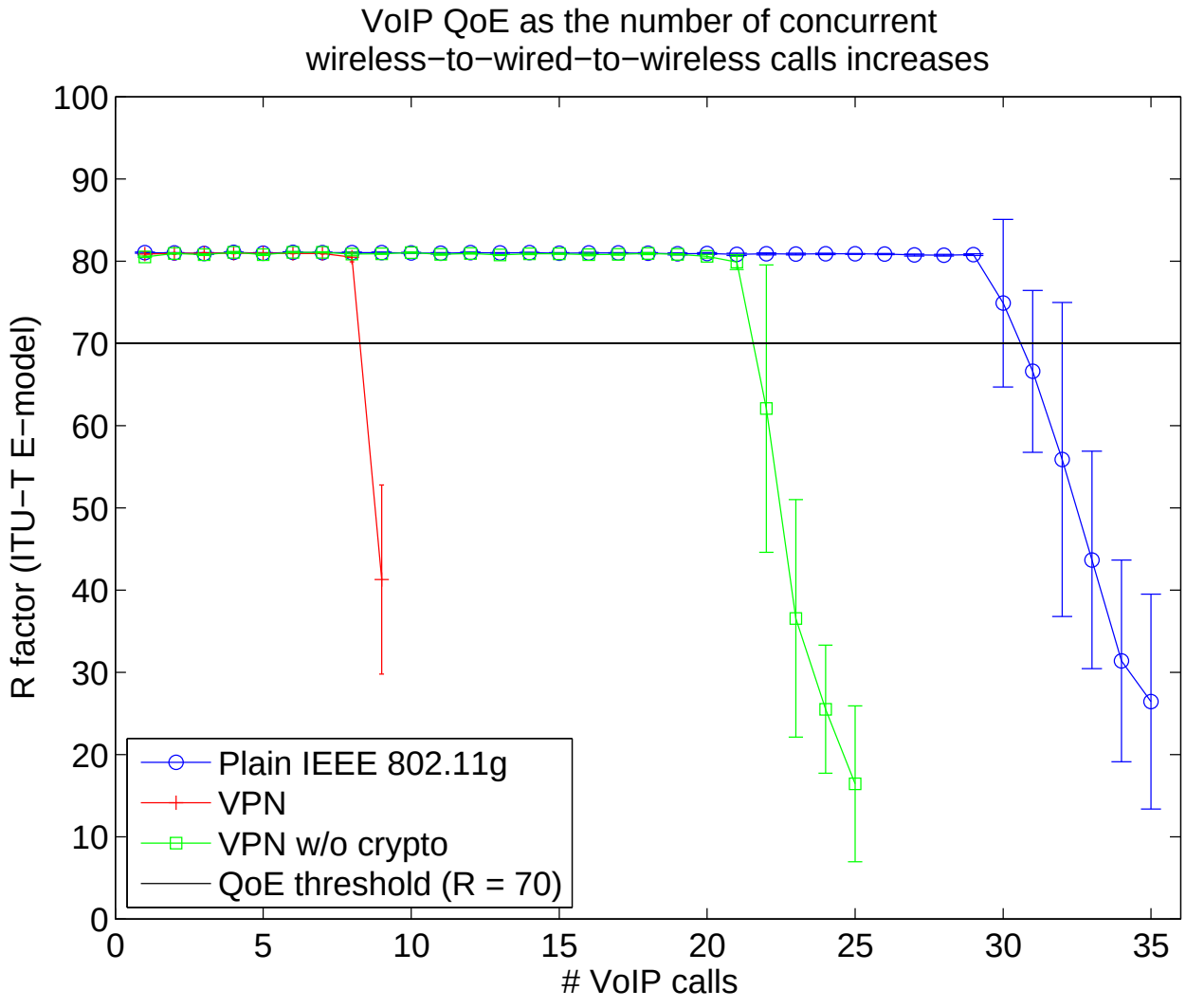
$$T_{Overhead} = 2 \times (T_{DIFS} + T_{DCF} + T_{SIFS} + T_{ACK} + T_{Headers}) + T_P.$$

	Time (IEEE 802.11g @54Mbps)
Slot time (T_{SLOT})	9 μsec
Backoff time (T_{DCF})	72 μsec
Audio payload (T_P)	**3** μsec
Overhead ($T_{Overhead}$)	**329** μsec
Overhead ($T_{Overhead}$) w. OpenVPN	**354** μsec

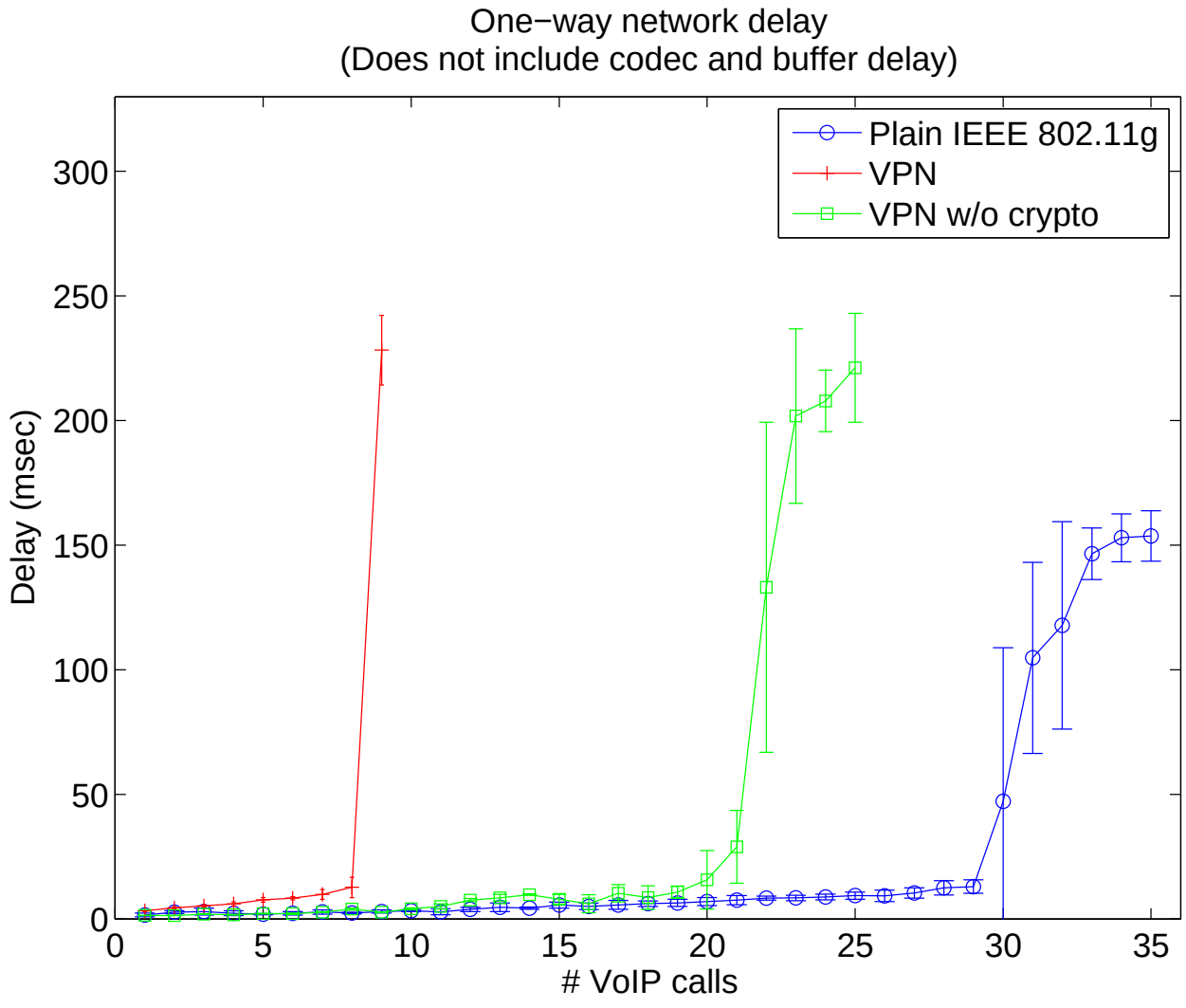
Upper bounds on VoWLAN capacity (II)



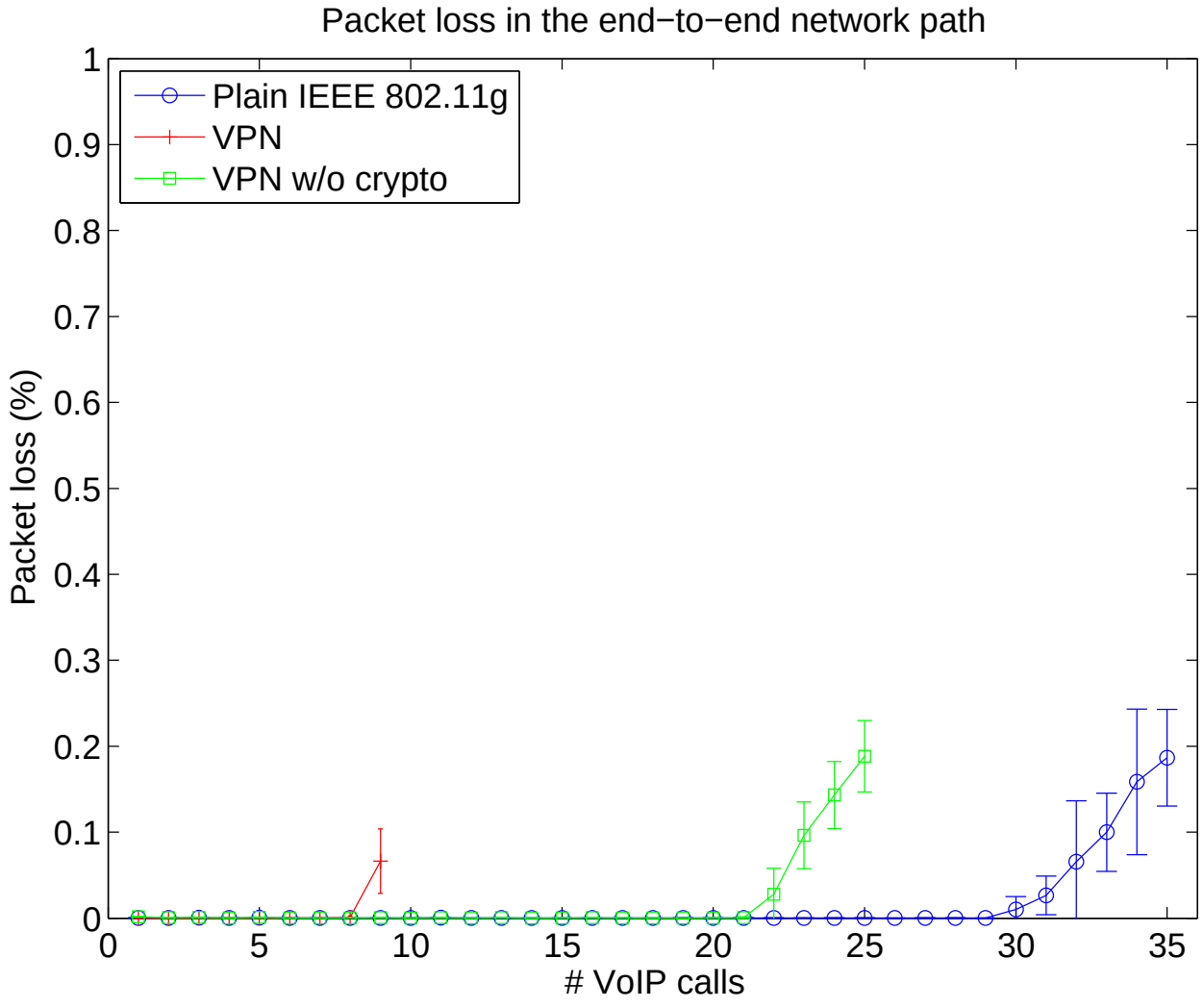
R-score


VoIP QoE as the number of concurrent
wireless−to−wired−to−wireless calls increases
R factor (ITU−T E−model)
VoIP calls
Plain IEEE 802.11g
VPN
VPN w/o crypto
QoE threshold (R = 70)
0
10
20
30
40
50
60
70
80
90
100
0
5
10
15
20
25
30
35

One-way network delay



Network packet loss



Dejitter buffer loss