Institut für Kommunikations-Technik

Social WiFi: Hotspot Sharing with Online Friends

IRTF GAIA Meeting
Prague, July 2015

Panagiotis Papadimitriou
Leibniz Universität Hannover

In collaboration with:
Zhen Cao, Jürgen Fitschen (Leibniz Universität Hannover)

Leibniz Universität Hannover

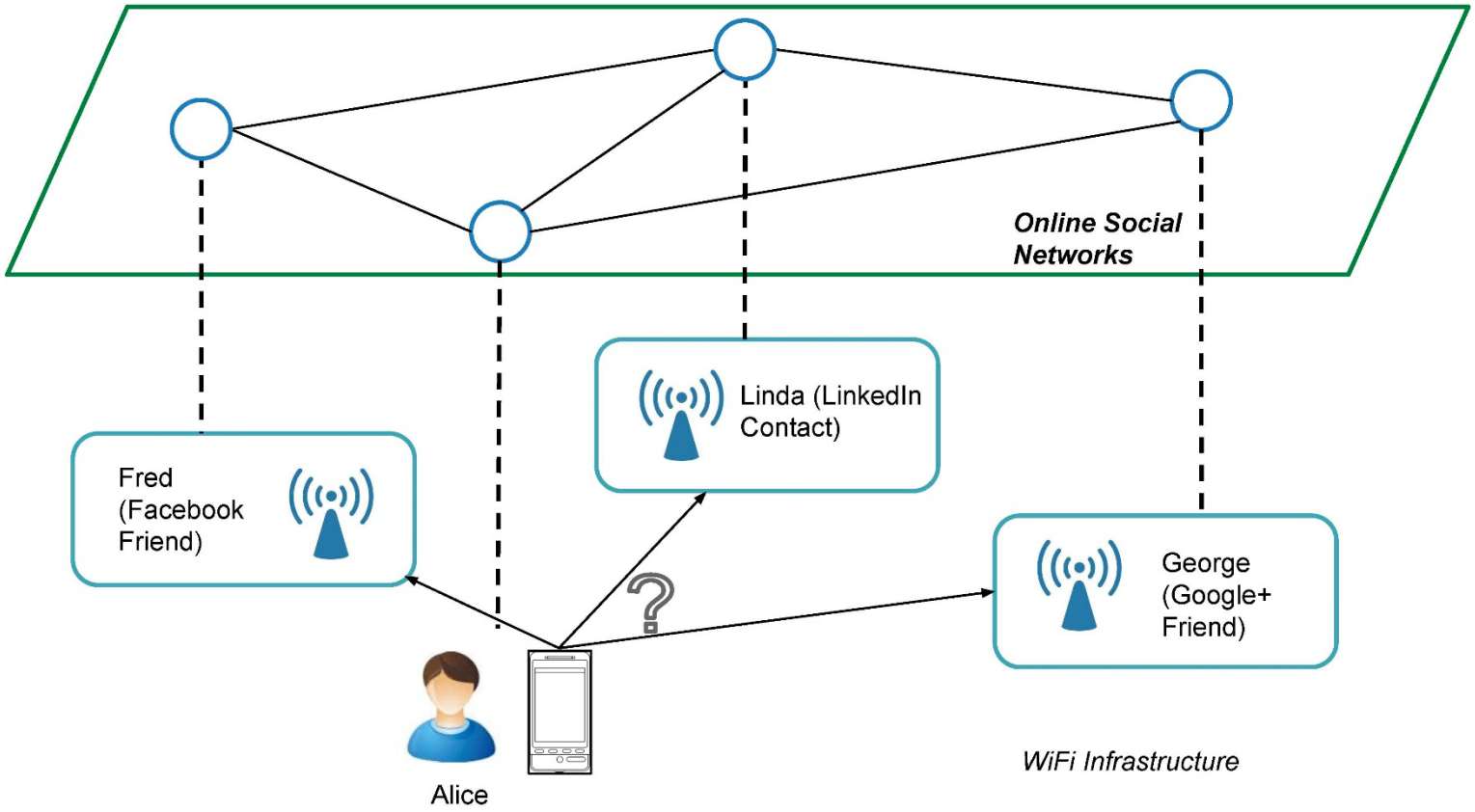
Motivation

- Hotspot sharing is mostly disabled

- Security issues
  - Fake SSIDs (reports from operators, e.g., FON)
  - Bogus DNS servers for phishing
- Liability issues
  - Sharers may be accountable for the illegal actions of guests

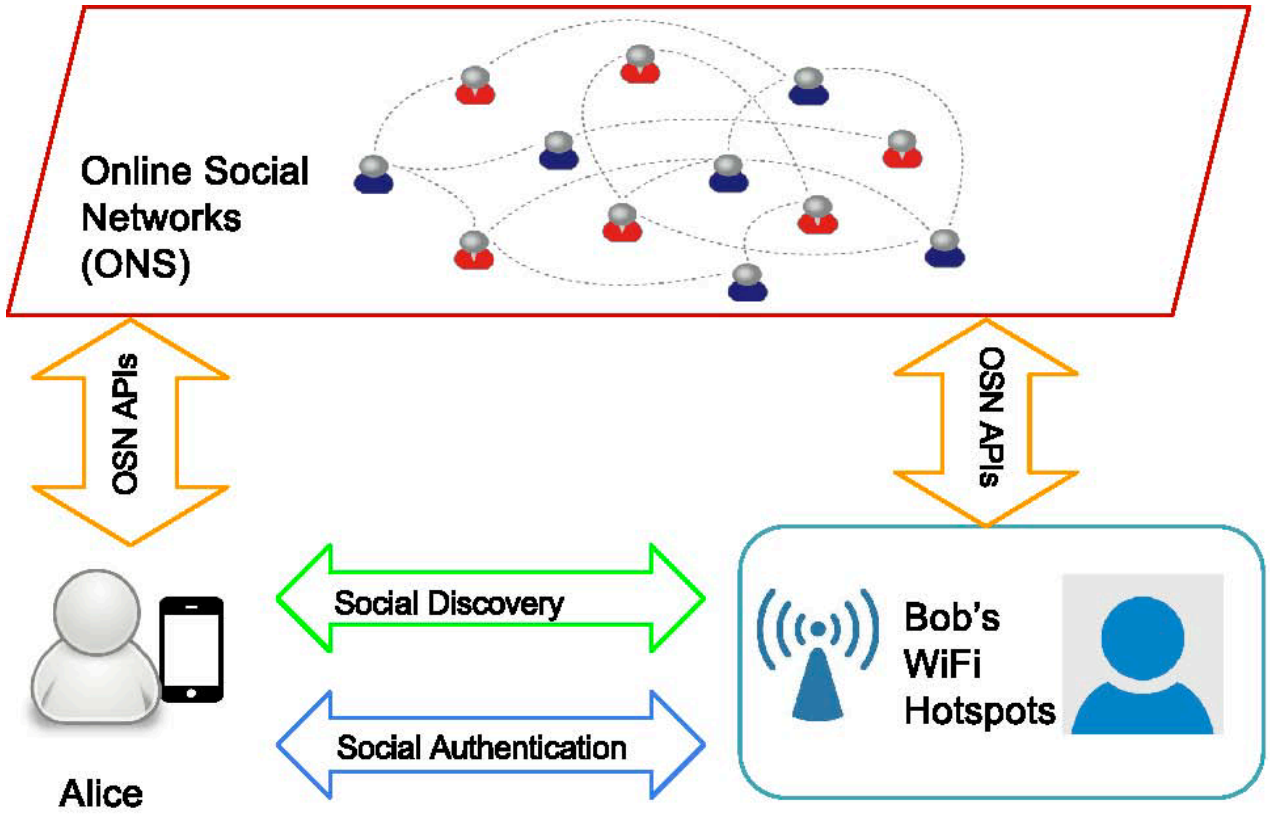
Hotspot Sharing with Online Friends

- High penetration of online social networks (OSNs)
  - Opportunities for hotspot sharing among online friends



Social WiFi Overview

- Discovery of hotspots owned by OSN friends
- Authentication via the validation of OSN relationship

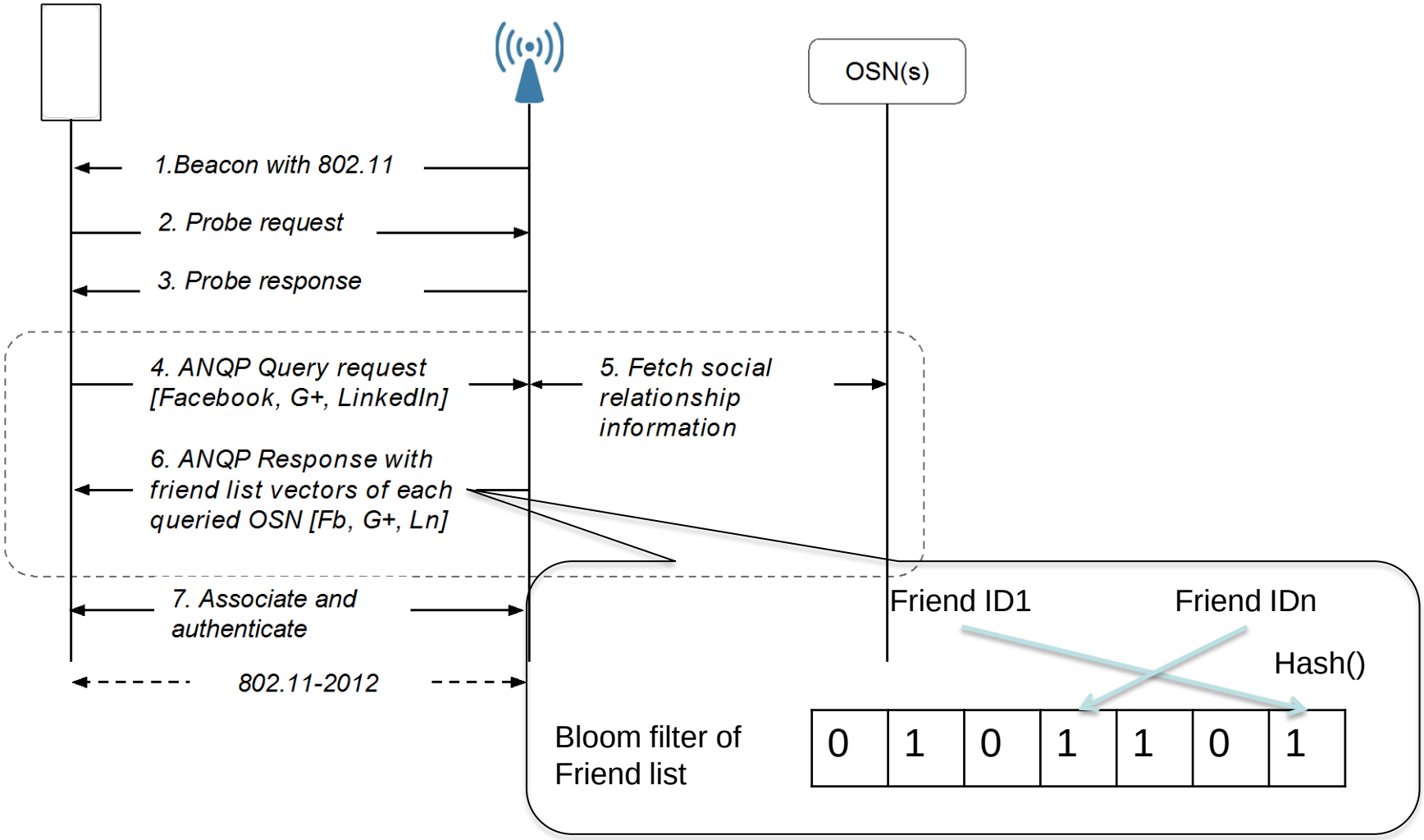


Social WiFi Discovery

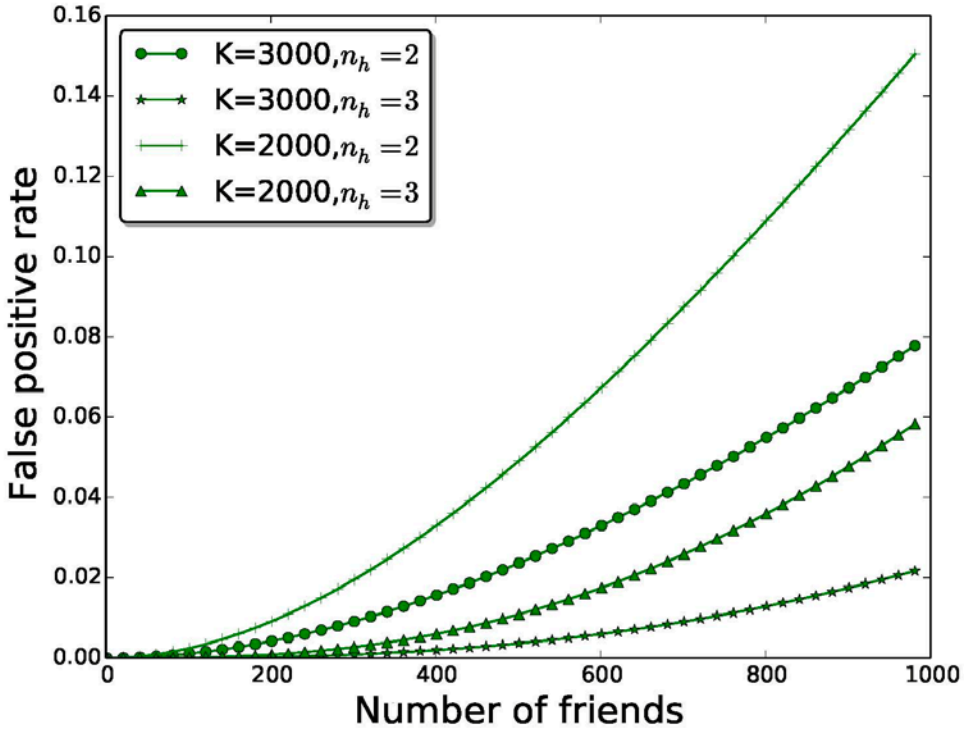
- Challenges:
  - SSID-based discovery is not secure
  - Limited length of SSID (32 Bytes)
    - Insufficient to encapsulate OSN information
  - OSN information confidentiality

- Our approach:
  - Extension of 802.11u ANQP (Access Network Query Protocol)

Social WiFi Discovery



Bloom Filter False Positives



K: vector length (bits)

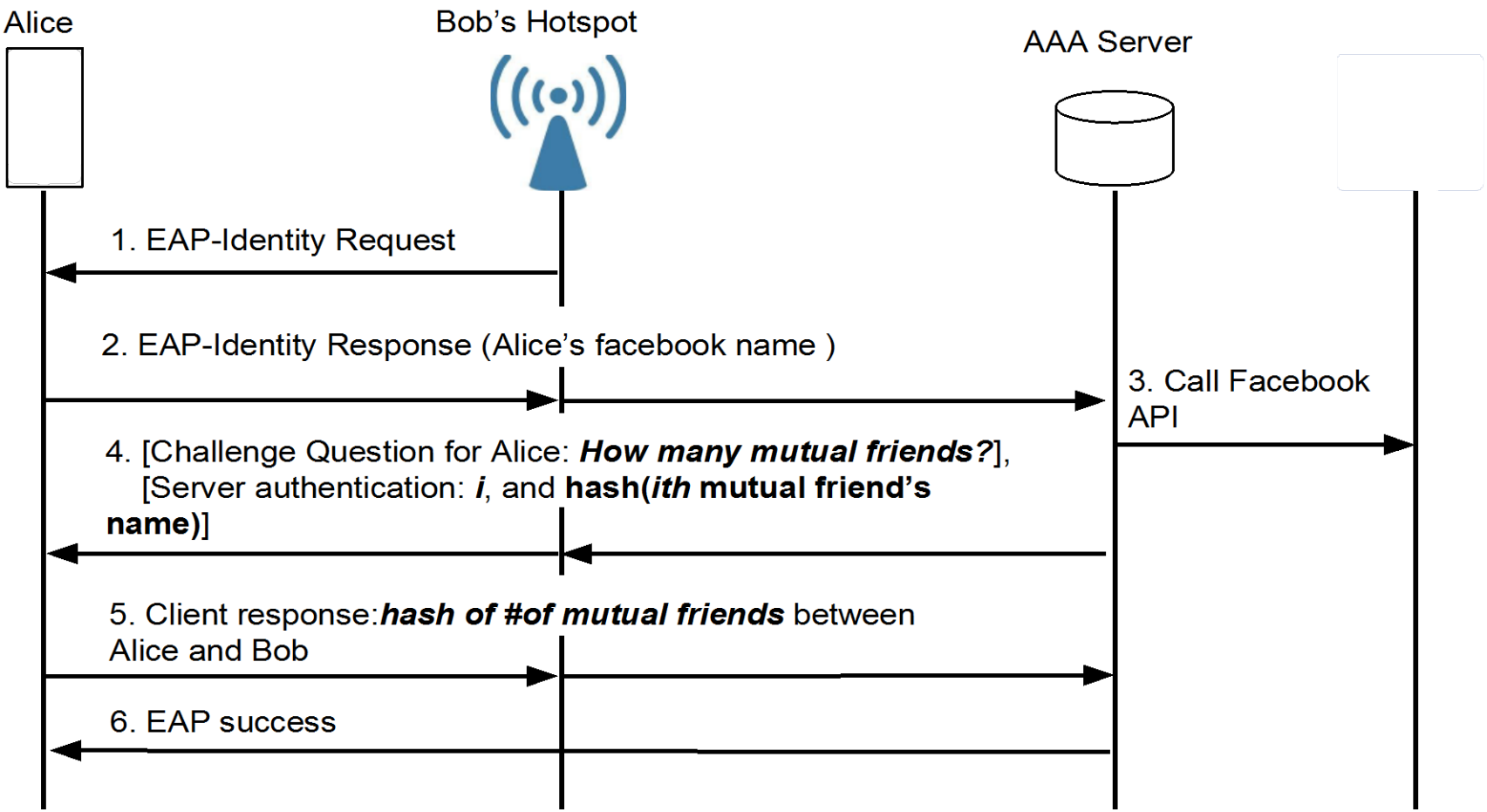
n_h: # hash functions

- 95% percent of users have less than 1000 friends (Facebook)
- K ≥ 3000, n_h ≥ 3 → false positive rate < 3%

Social WiFi Authentication

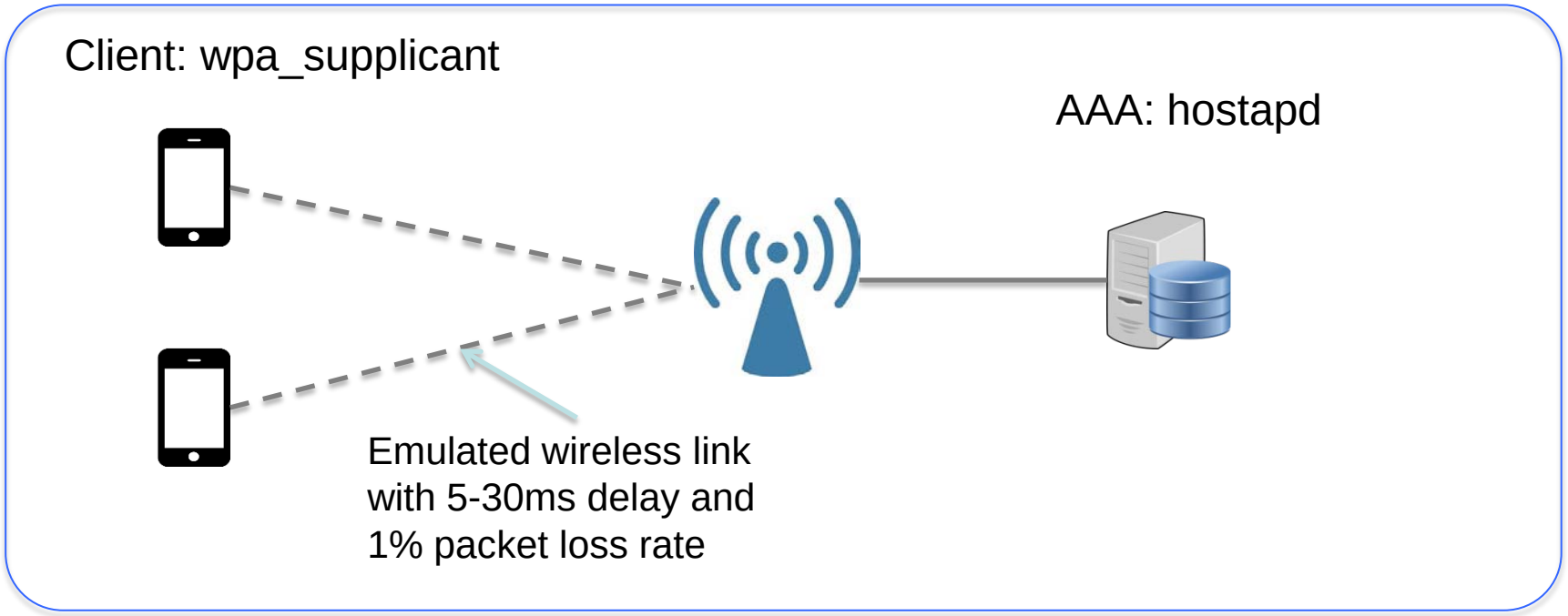
- Challenges:
  - Lack of pre-shared or pre-disseminated credentials
    - Cannot rely on existing EAP methods for mutual authentication
- Our approach:
  - Mutual authentication via validation of OSN relationship
  - Challenge question for authentication:
    - e.g., # mutual friends
    - hashing for privacy

EAP-Social


Alice
Bob's Hotspot
AAA Server
1. EAP-Identity Request
2. EAP-Identity Response (Alice's facebook name)
3. Call Facebook API
4. [Challenge Question for Alice: How many mutual friends?], [Server authentication: i, and hash(ith mutual friend's name)]
5. Client response:hash of #of mutual friends between Alice and Bob
6. EAP success

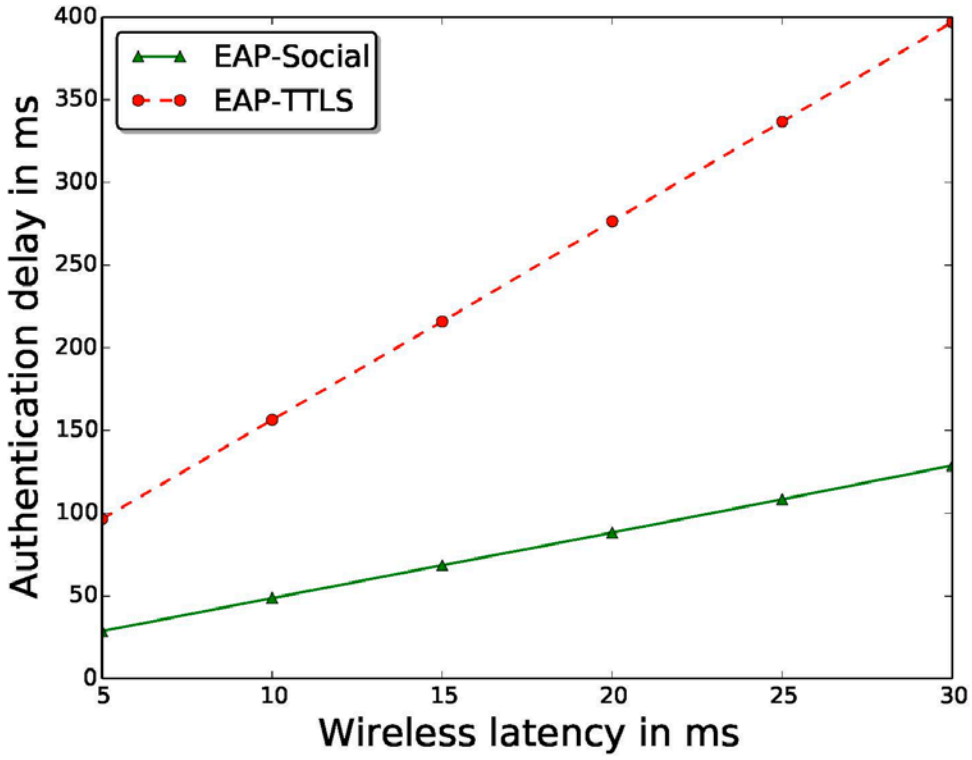
Evaluation Setup

- Evaluation in Mininet



Authentication Delay

- EAP-Social completes authentication within 100 ms
  - 10 ms authentication processing time for EAP-Social
  - 37 ms authentication processing time for EAP-TTLS



Conclusions

- Social WiFi:
  - Extension of ANQP for hotspot discovery
    - Bloom filter for data compression and privacy protection
  - EAP-Social for mutual authentication
    - No need for pre-shared secrets
    - OSN relationship validation

- EAP-Social evaluation:
  - Faster authentication than EAP-TTLS

Thank you!

Panagiotis Papadimitriou

E-mail: panagiotis.papadimitriou@ikt.uni-hannover.de

WWW: http://www.ikt.uni-hannover.de/

Backup Slides

Related Work

	Target users	Authentication	Approach
FON	Fon members	Web portal with user intervention	Member participatory
Facebook WiFi	Facebook users	Web portal with user intervention	Facebook initial participatory program
Eduroam	Academic	EAP compatible	Agreement pre-setup
OpenWiFi	Guest WiFi	Portal based with user intervention	Open-ID
VPuN	Community	Web	SDN
Social WiFi	ONS users	EAP compatible and automatic	Social discovery and authentication