Device location certification for the Internet of Things

Miguel.Pardal@tecnico.ulisboa.pt

Universidade de Aveiro

Thursday, December 19th, 2019

Outline

- Research context
- SureThing project
  - Mobile ad-hoc witnesses
  - Wi-Fi Scavenging
  - Bluetooth proximity
- Current and future work

Research context

Distributed Systems Group

- Security & Privacy
  in the new *frontiers* of
  Information Technologies and Computer Science:
  - Internet of Things & Cloud

Security & Privacy

- CIA properties:
  - Confidentiality
  - Integrity
  - Availability
- TIU properties:
  - Transparency
  - Intervenability
  - Unlinkability

Digital Citizenship

From *distributed* to *ubiquitous* computing

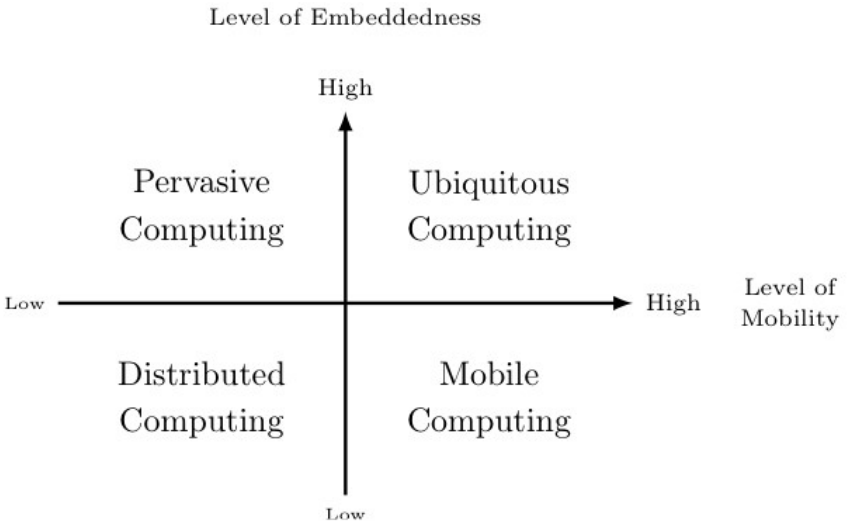


Figure credits: Marc-Oliver Pahl

Smart Spaces

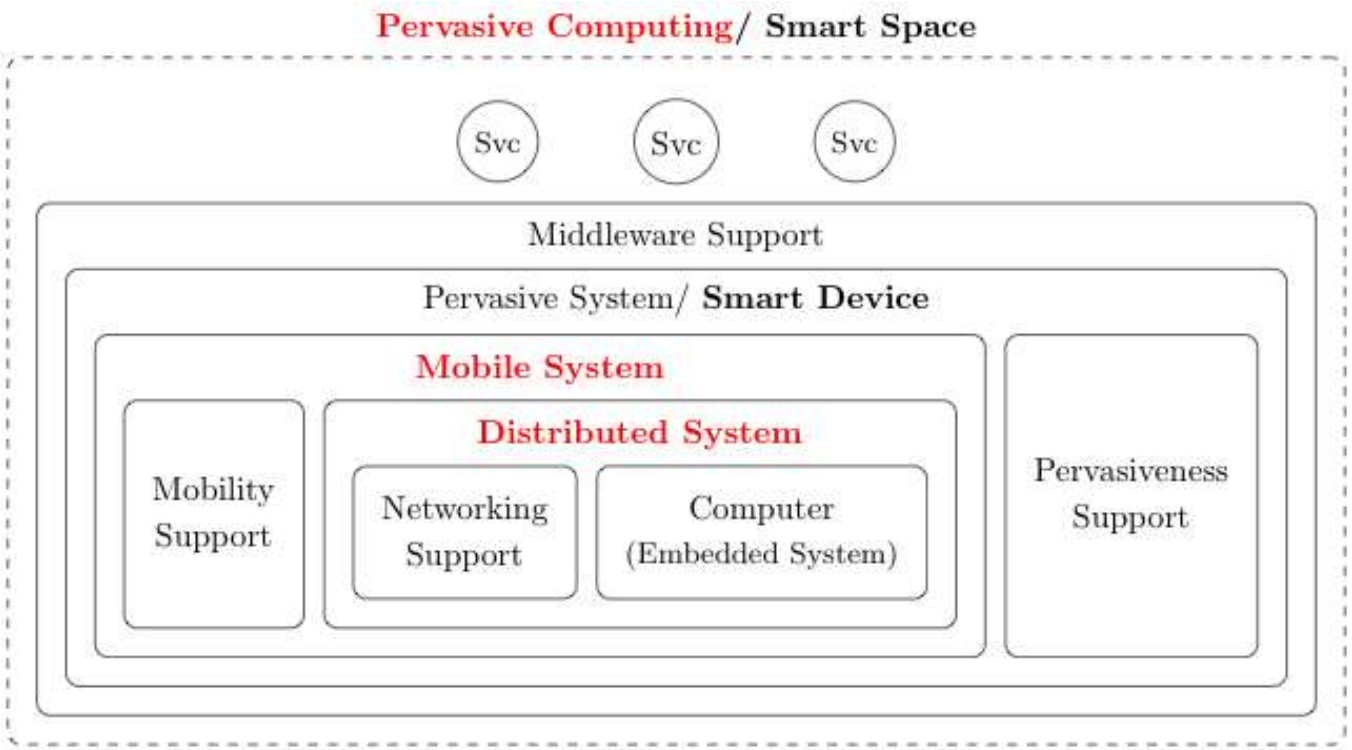


Figure credits: Marc-Oliver Pahl

The Internet of Things

The interface between the *physical* and *digital* world that allows one to gather data from everyday objects and also *control* them.

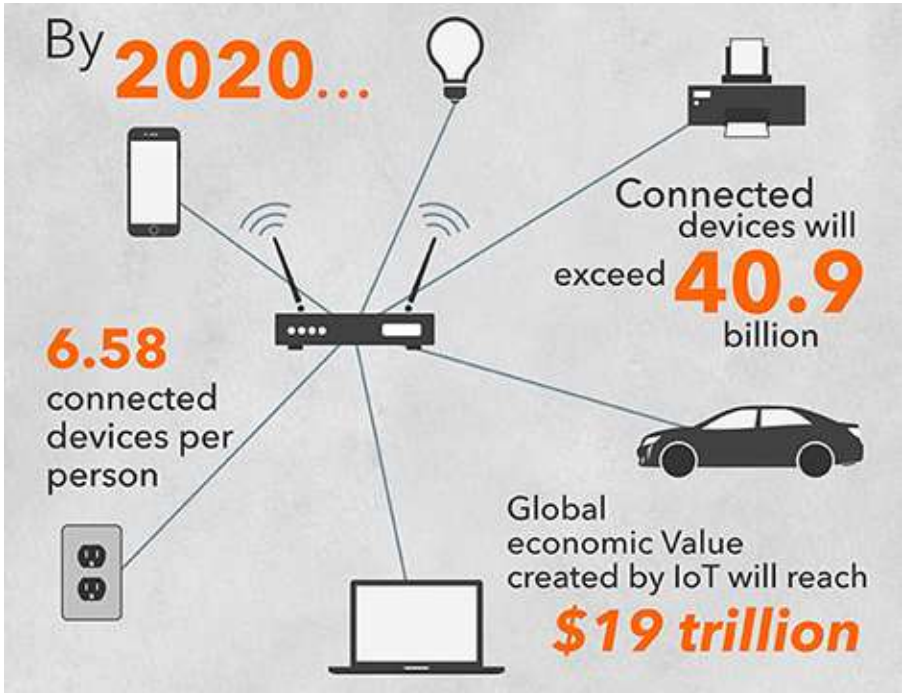
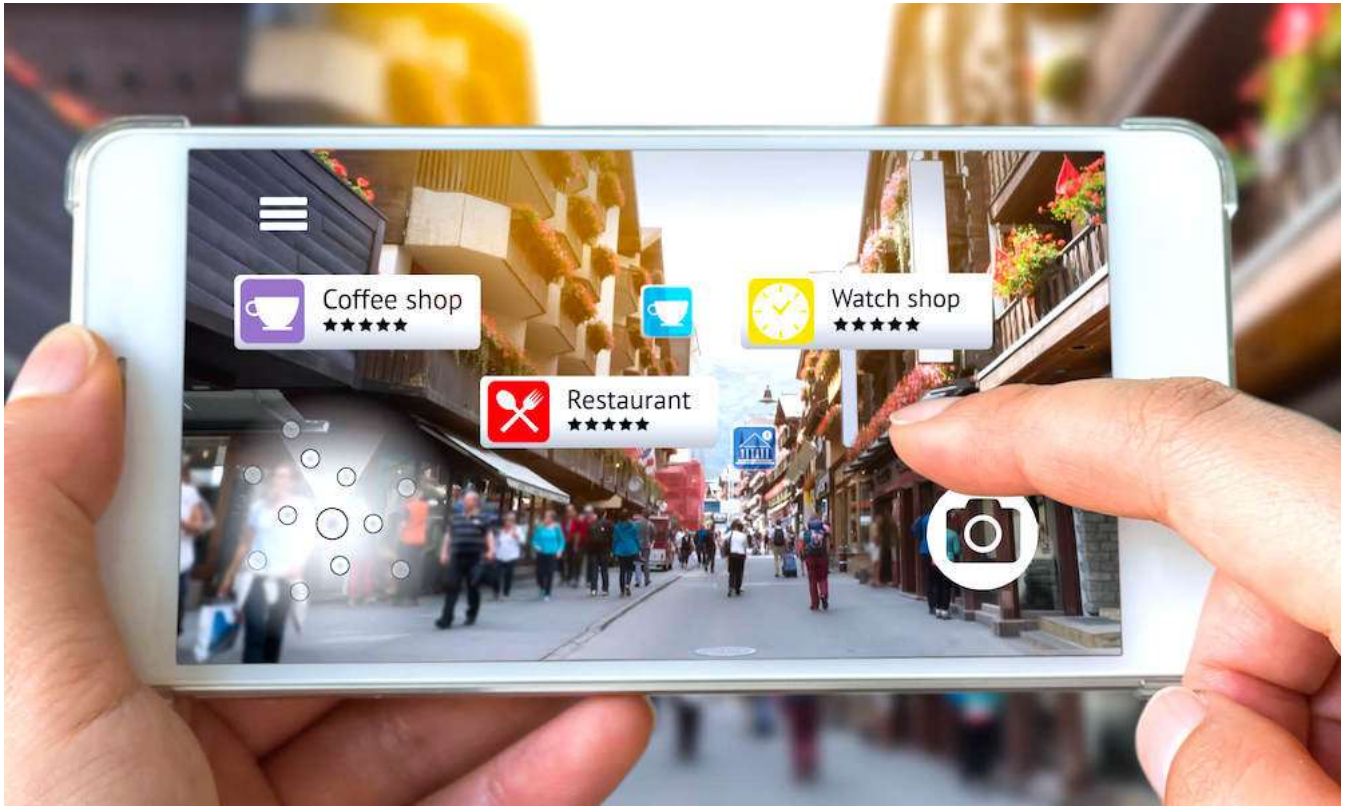


Figure: IBM

Electronic business

Augmented reality



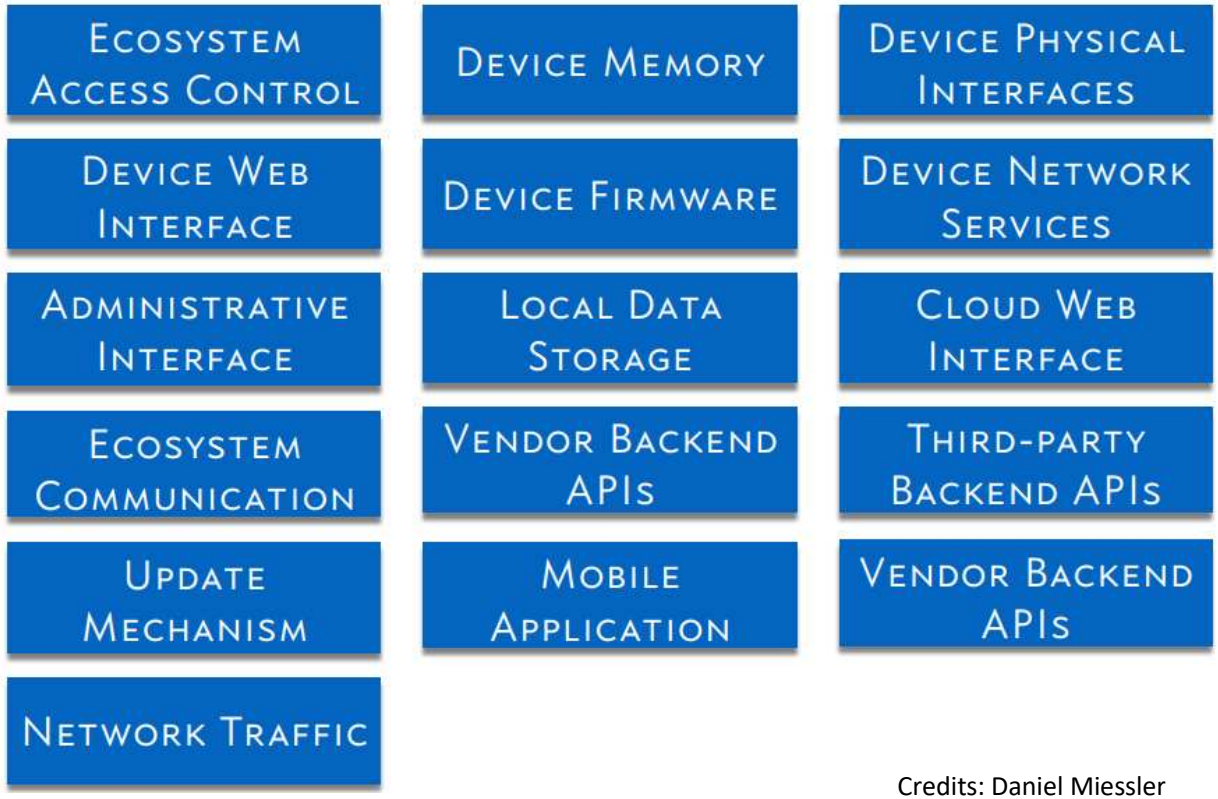
Hyper-reality

Concept video by Keiichi Matsuda:
https://vimeo.com/166807261

Hyper-reality (turned off)

Hyper-reality gone wrong

IoT
attack surfaces



Credits: Daniel Miessler

The Internet of *ransoms* ?

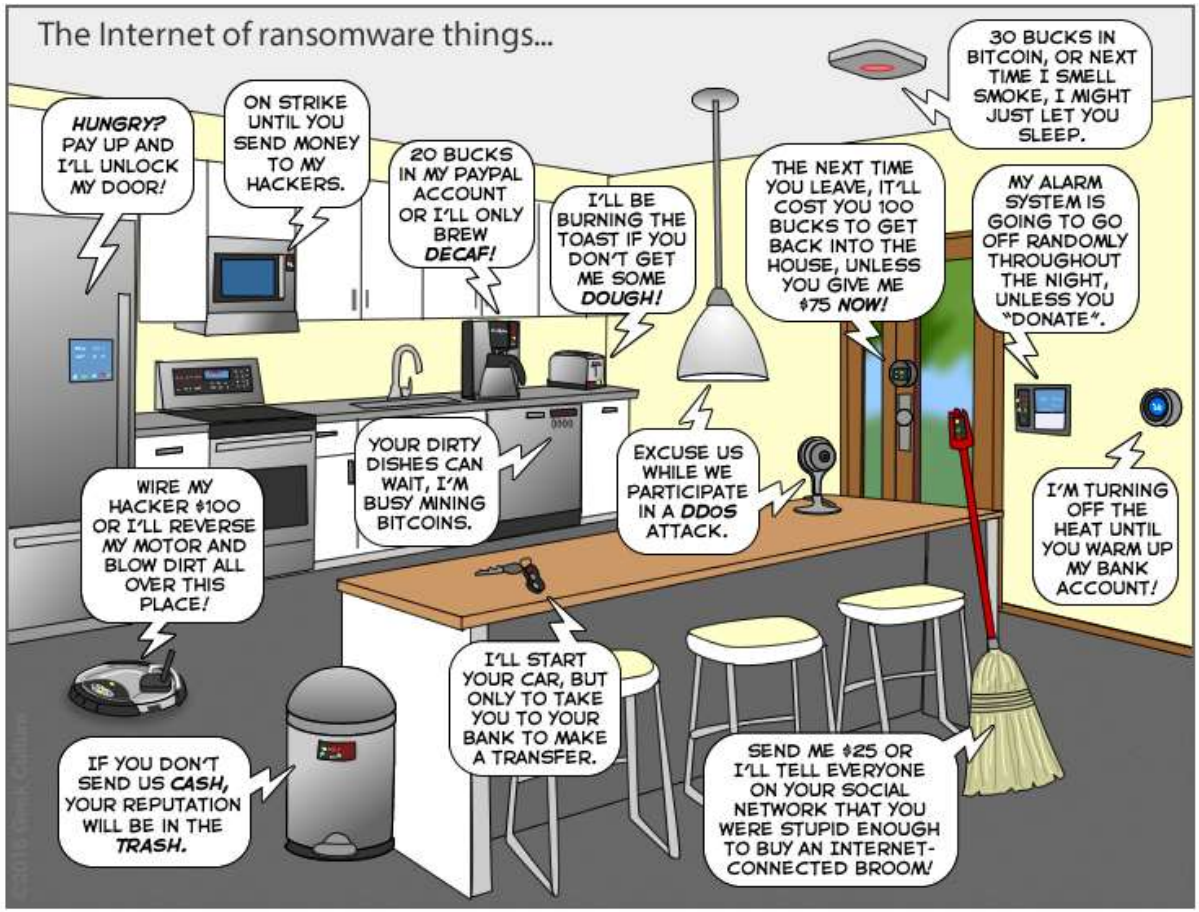


Image credits: Joy of Tech

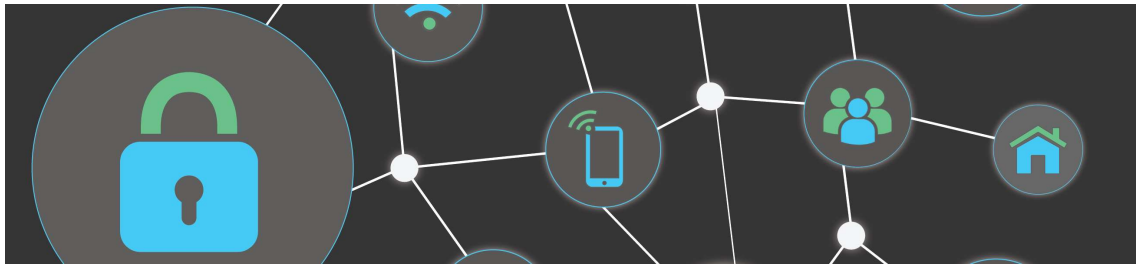
Why new research is necessary

- Internet threats so far have been most about *confidentiality*
  - Bad things happen to our data
  - Most problems today are not solved, only mitigated
- On the Internet of Things, attackers now have *"hands and feet"*
  - The ability to directly affect the physical world
  - Attacks against *flesh, steel, and concrete*

Bruce Schneier to Motherboard Magazine

"The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters"

SureThing project



Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

Project goal

- Create and validate location certificates
  - Devices can make proof of their location or ask proofs from other devices
  - Proofs can be used to make security decisions
    - E.g. strong attributes for policy decision in ABAC solution
- For Internet of Things applications
  - Smart Spaces
  - Mobile devices
  - Limited devices

From location detection to location proofing

Is the device *really* there?

Idea

Let us use the device *diversity* and *scale* of the Internet of Things for cyber-defense

Inspiration: PUFs
Physically Uncloanable Functions

Main Threat

- **Location spoofing**
- How to be sure that the device is present?

SureThing prototypes

- Mobile ad-hoc witnesses
- Wi-Fi Scavenging
- Bluetooth proximity

SureThing for mobile devices

with ad-hoc witnesses

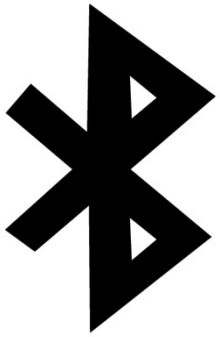
João Ferreira

Location Proof Techniques

- Based on the used location estimation technique

GPS

Wi-Fi



Bluetooth

Witness Models

- Two main models:
  - **Master** – *trusted* witness
  - **Mobile** – *circumstantial* and *partially trusted* witness

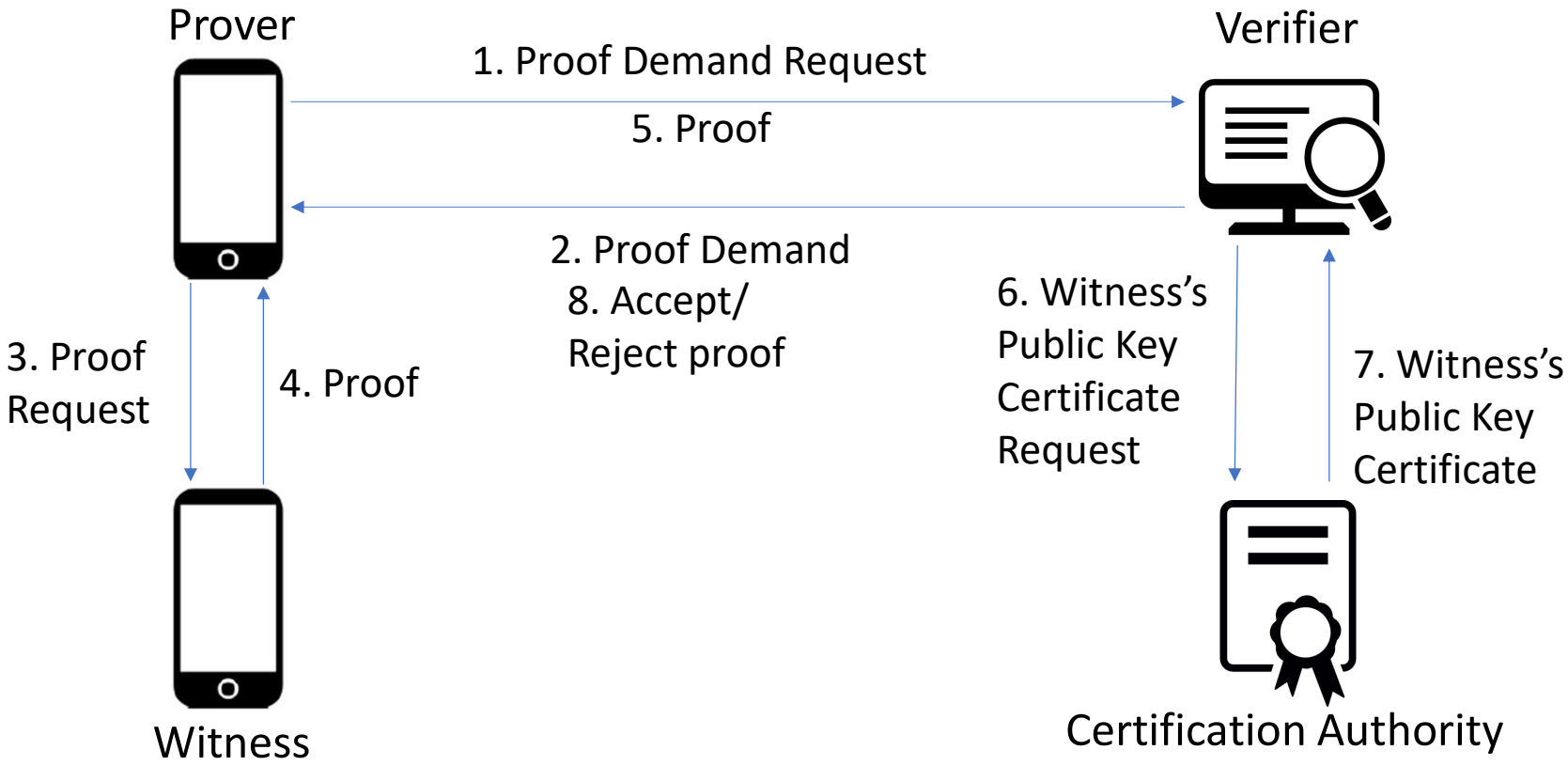
Location Proof

Prover ID	Witness ID	Location of the Prover	Location of the Witness	Nonce	Signature

Location Proof in JSON format


```
{
  “proverId”: “Alice”,
  “witnessId”: “Bob”,
  “proverLocation”:
    {
      “latitude”: 38.0123456,
      “longitude”: -9.9876543,
    },
  “witnessLocation”:
    {
      “latitude”: 38.0123489,
      “longitude”: -9.9876541,
    },
  “nonce”: 1234,
  “signature”: H9xa1hDAsHaS…”
}
```

Communication Protocol



Implementation

- Android mobile application for both Prover and Witness
  - Java programming language
- Verifier and Certification Authority
  - RESTful web services
  - JSON messages

Evaluation

- How accurate are the location estimation techniques?
- How long does it take to issue a location proof?

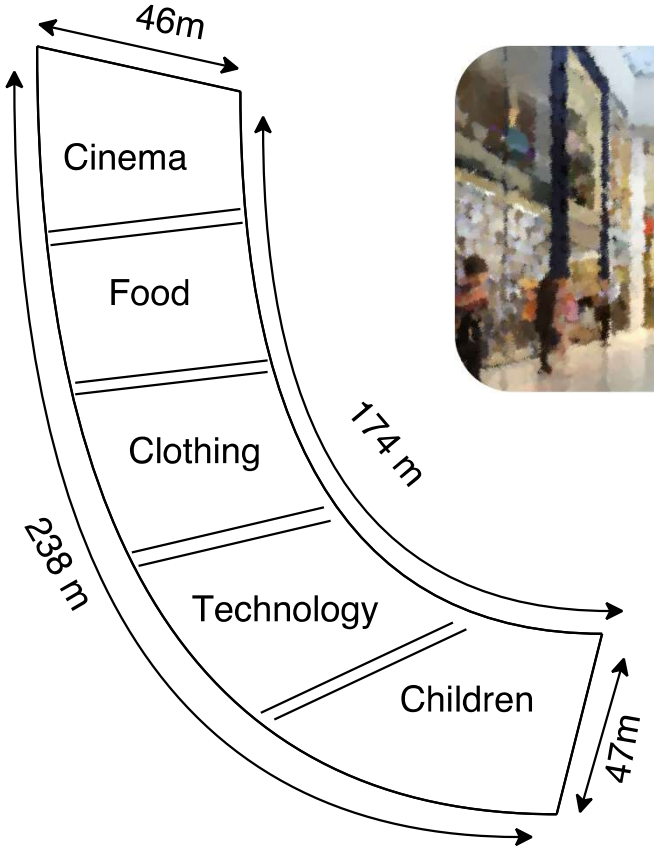
Evaluation Setup

- Building with

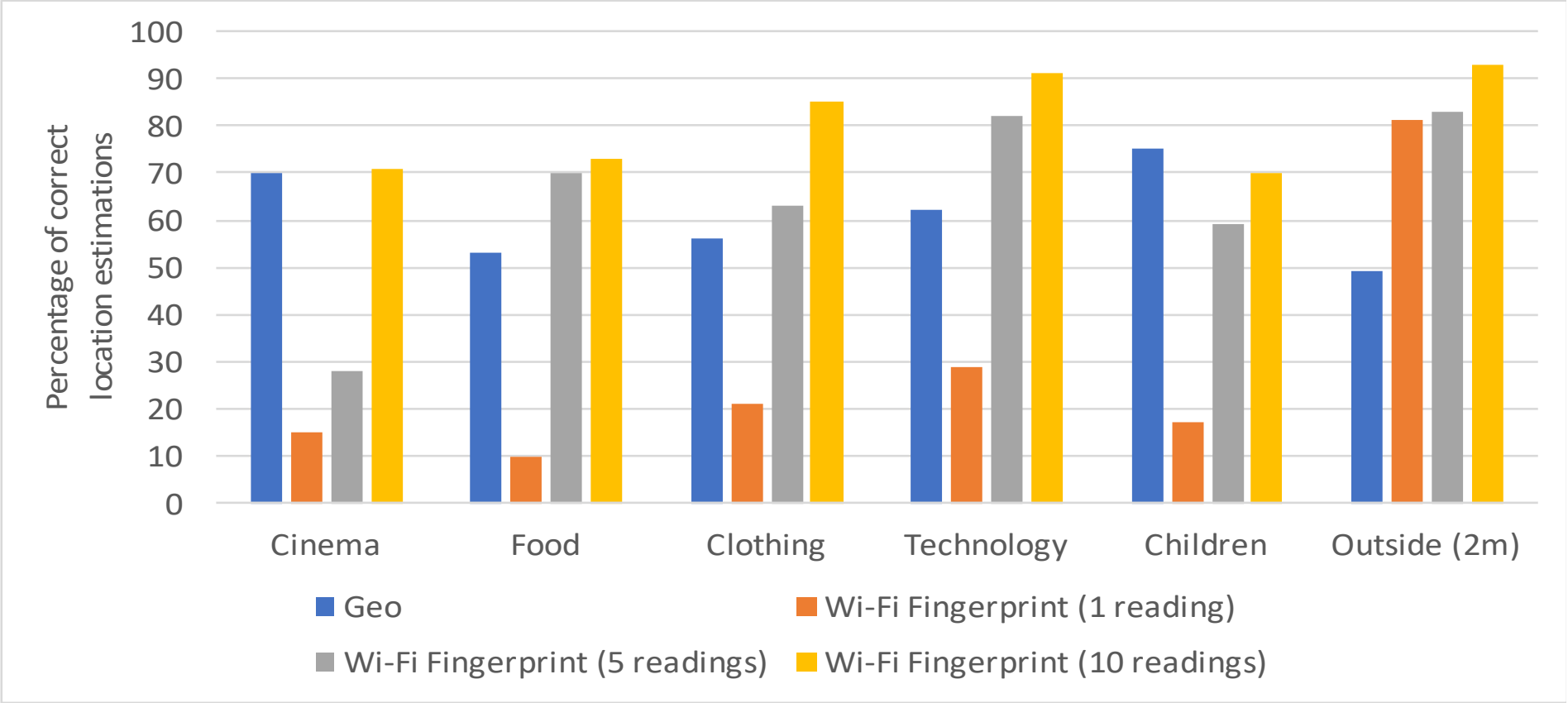
  five different areas

  - Shopping center
  - Testing Geo and

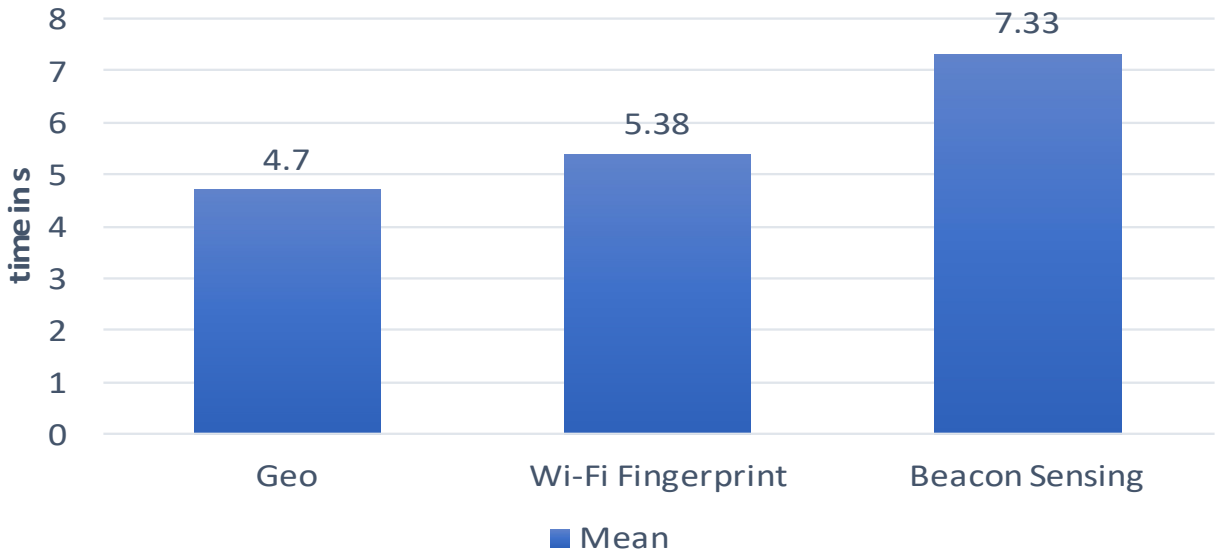
    Wi-Fi techniques precision



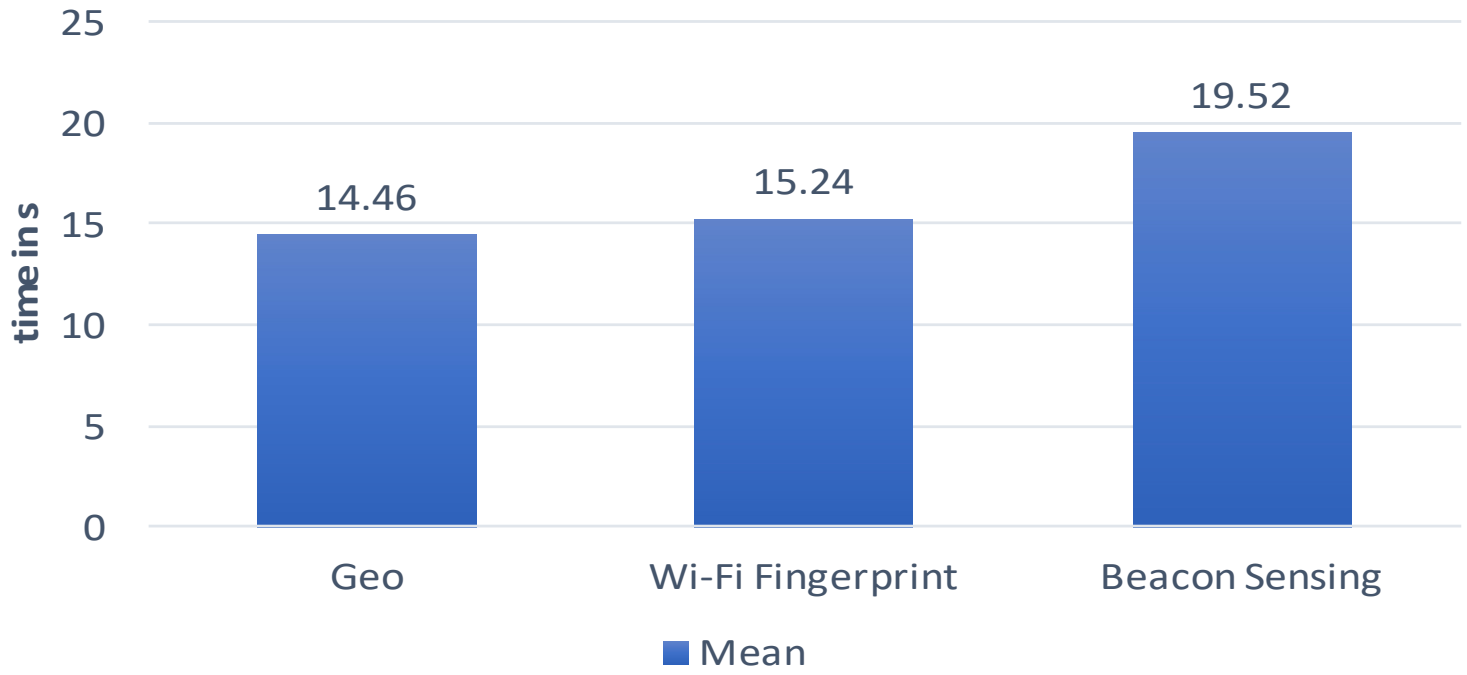
Evaluation – Location Estimation



Location estimation time



Total proof time

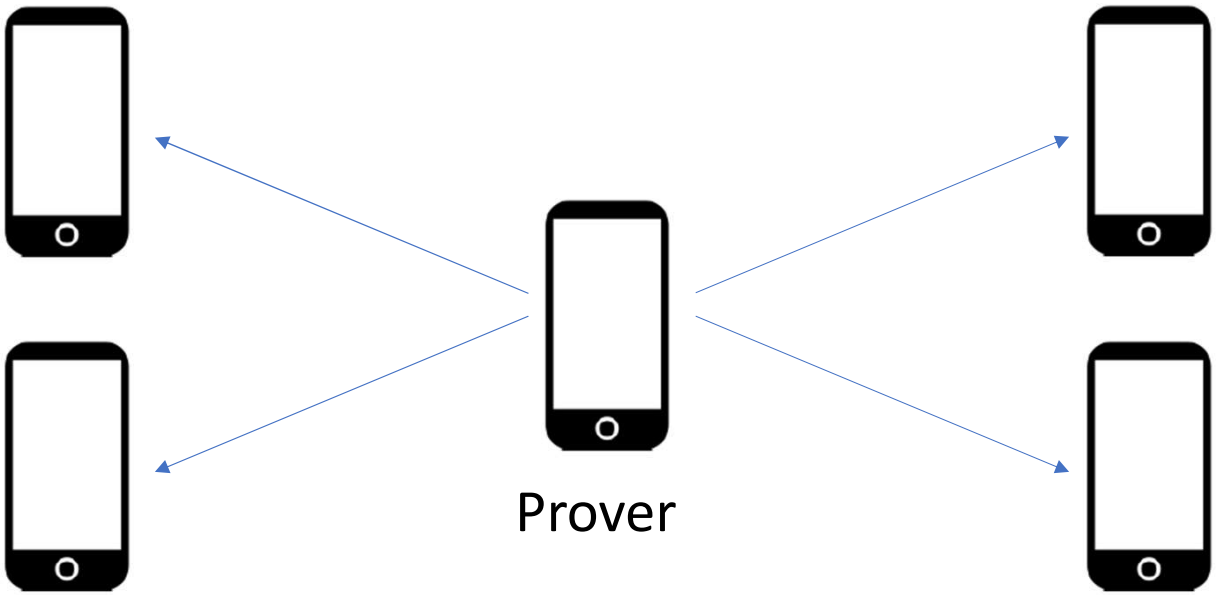


Collusion avoidance mechanisms

- Provers can be colluding with false witnesses
- Verifier has to use mechanisms to avoid successful collusions

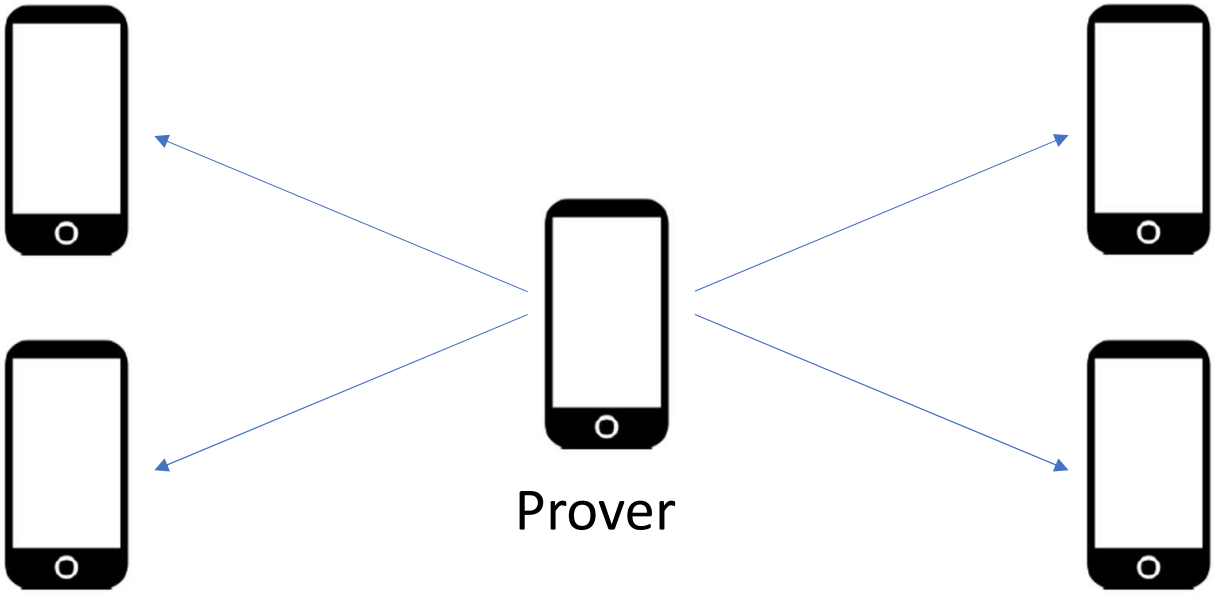
Witness redundancy

- Prover has to gather proofs from multiple witnesses



Witness decay

- Proofs given by repeated witnesses become less valuable



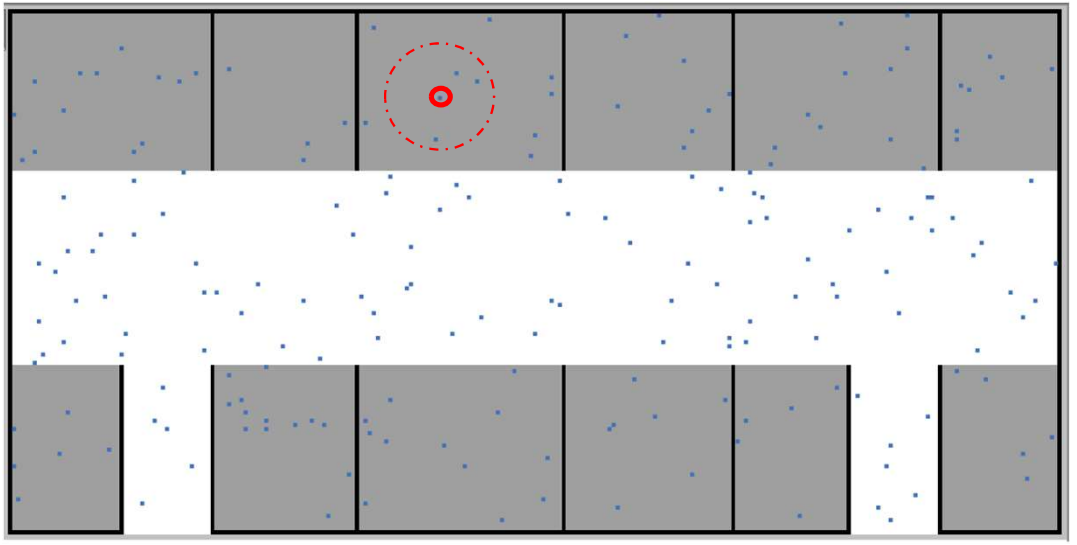
$$V_{xy} = \begin{cases} V & \text{if } N_{xy} = 0 \\ V - \frac{{N_{xy}}^k}{U} & \text{if } N_{xy} > 1 \end{cases}$$

Collusion avoidance simulation

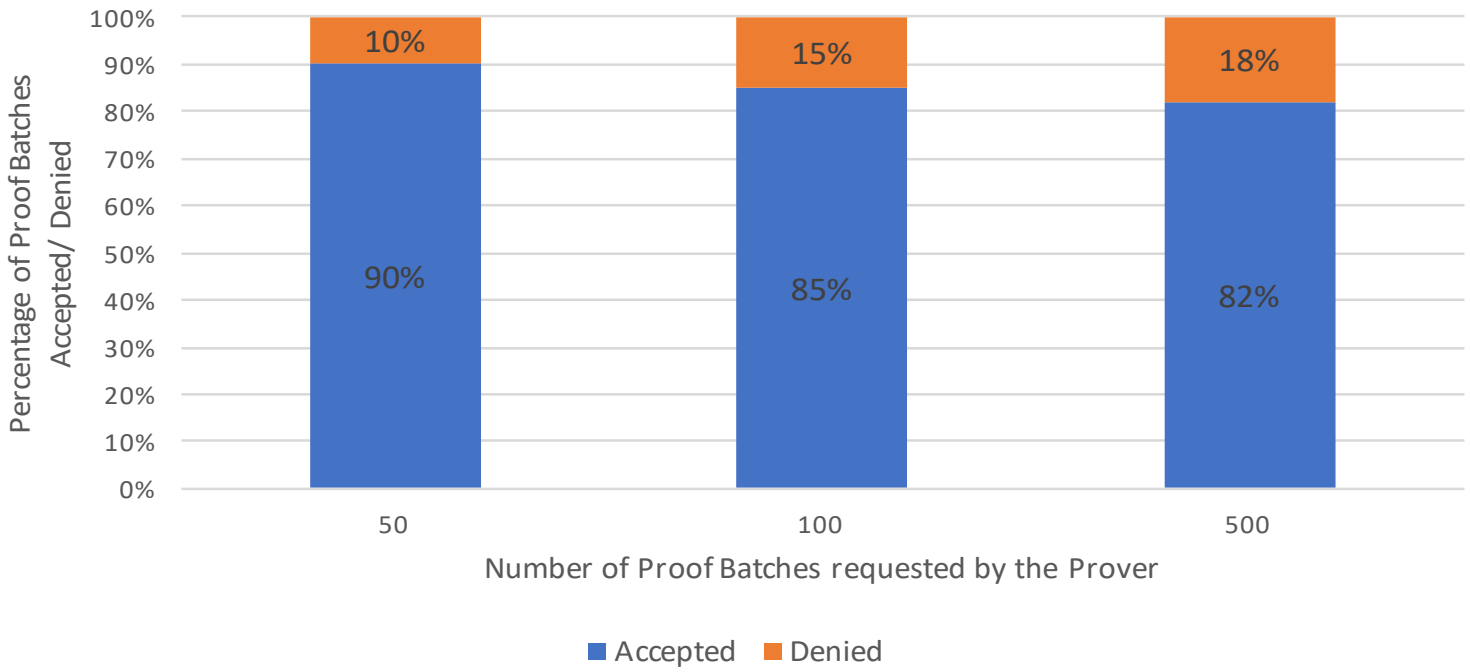
- Simulated shopping center
- 250 users that behave as

  Provers and *Witnesses*

Netlogo simulation



Collusion avoidance simulation



Use case: smart tourism

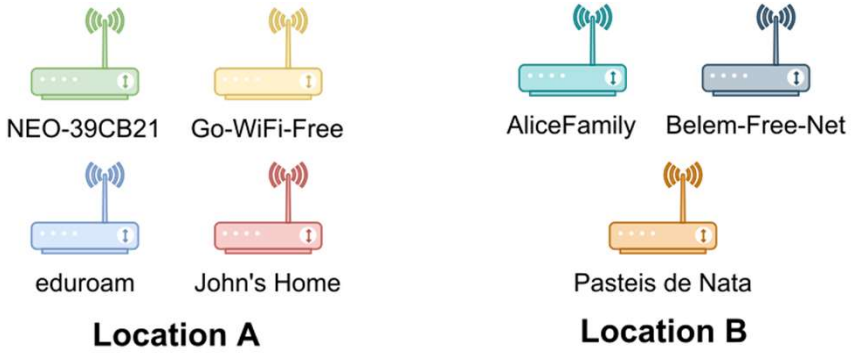
- App for tourists
  - Improve experience
- Reward visit to locations
- Challenges:
  - Open environment
  - Reuse infrastructure

CROSS
location proofs for smart tourism in the city

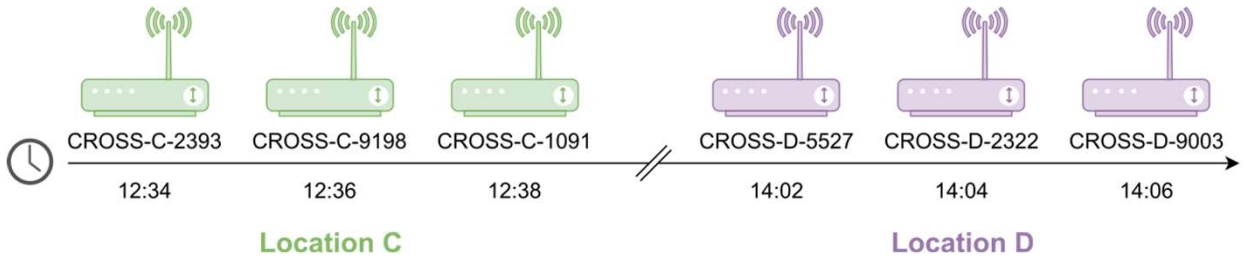
Wi-Fi scavenging

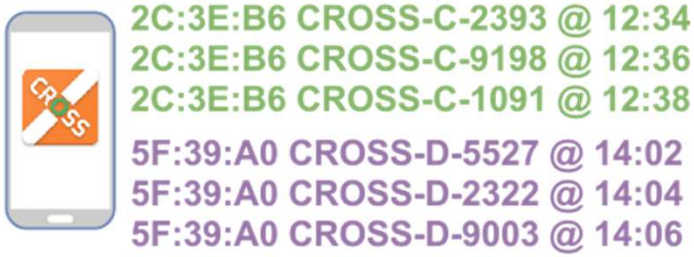
Gabriel Maia

Wi-Fi Scavenging

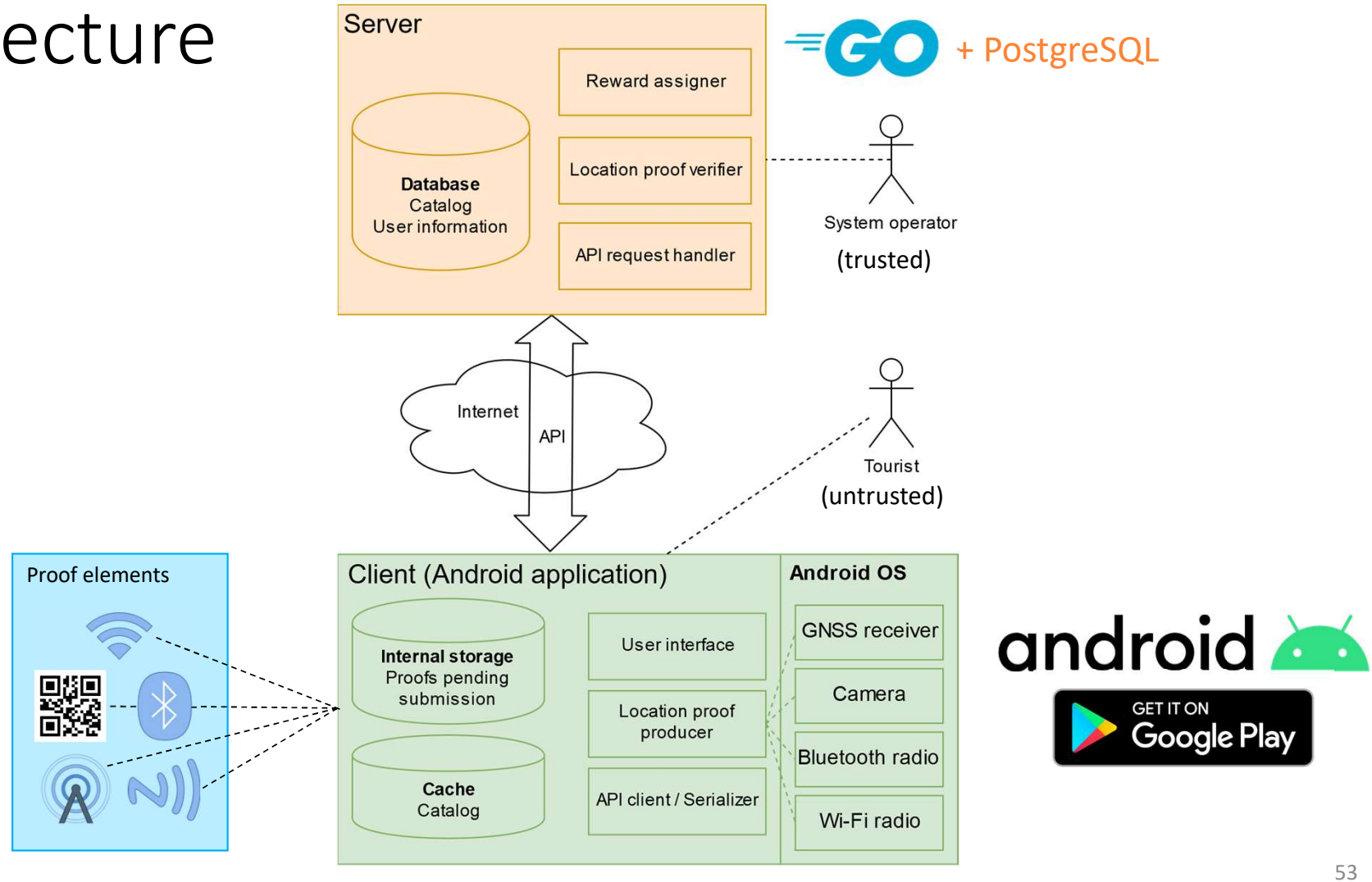


Wi-Fi Beacons with Time-based OTP



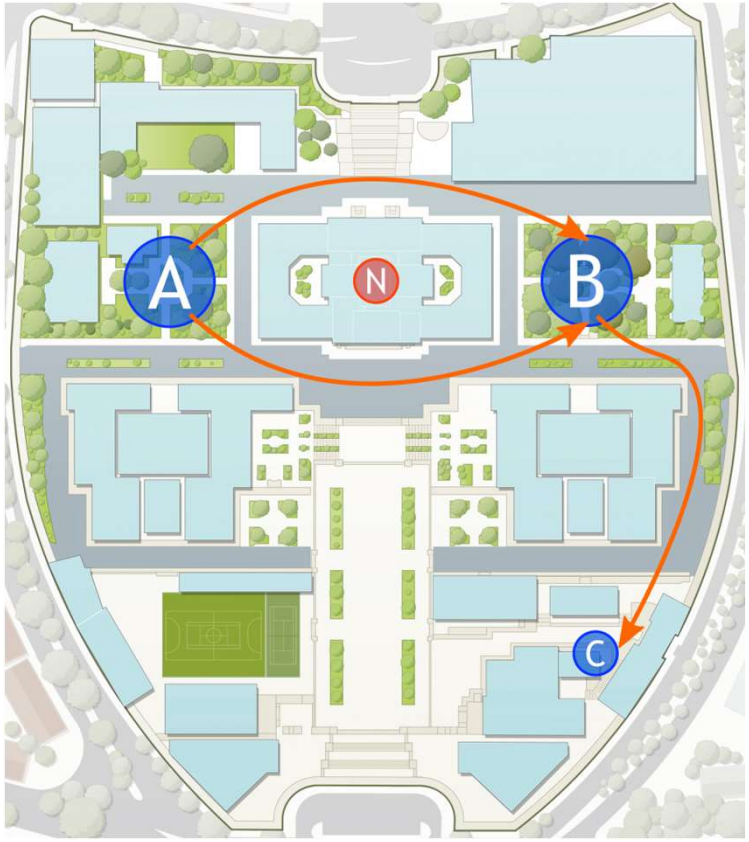


Architecture



Evaluation

- Android App
  - Available on the Play Store
- Tests with **30 users**
  - **34** different Android smartphones
- Test route with 3 locations (A, B, C, N)
  - Alameda campus of Instituto Superior Técnico

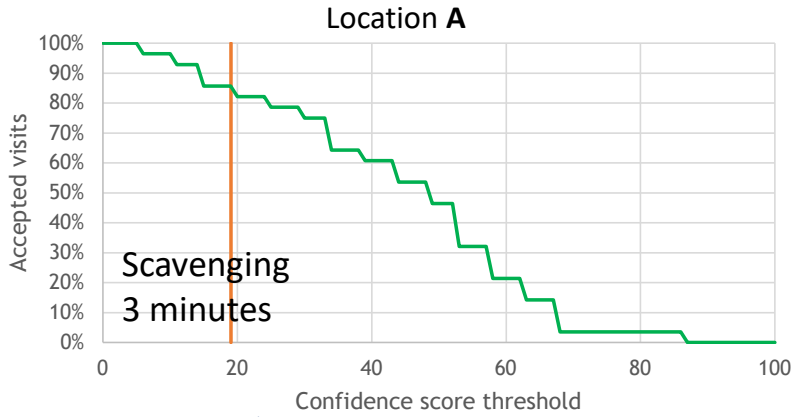


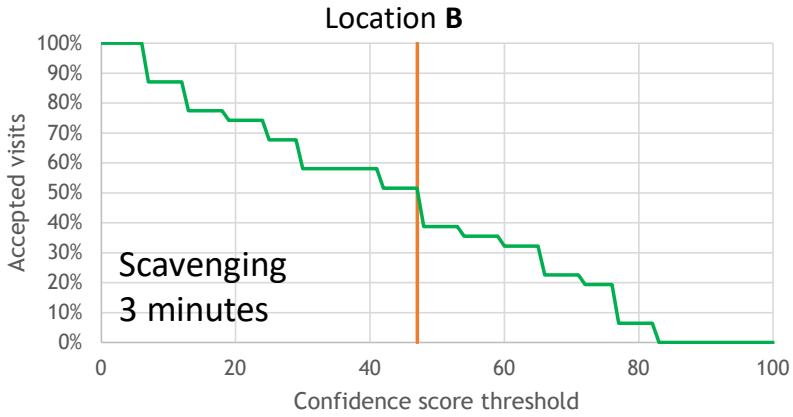
Results: Location detection performance

After 3 minutes at each location

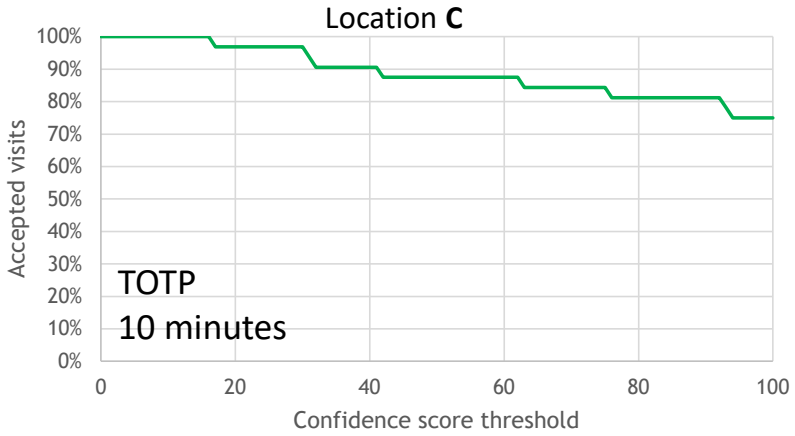
Location	Proof Strategy	Total visits	Total detections	Success rate
A	Scavenging	34	30	88%
B	Scavenging	34	33	97%
C	TOTP	34	34	100%
N (not visited)	Scavenging	0	0	100%

Results: Location proof performance





% of seen APs



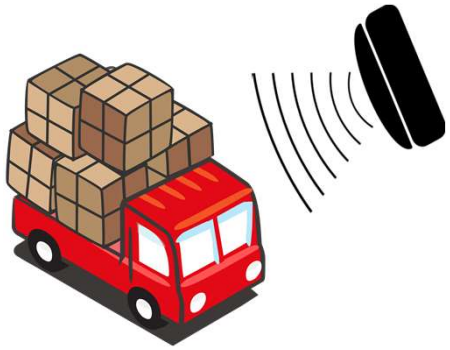
% of verified visit duration

Results: Scavenging feasibility

- Are there enough Wi-Fi networks for scavenging to work? **Generally, yes**
- Does the network list require constant updates? **No**

Wi-Fi networks present at urban locations in Lisbon					
Location	Initial total	After ten days		After one month	
		Present	New	Present	New
Alvalade	86	**74** (86%)	13	**73** (85%)	31
Pr. Comércio	133	8 (6%)	60	7 (5%)	43
Gulbenkian	80	**54** (68%)	92	**54** (68%)	55
Jerónimos	148	**34** (23%)	100	**24** (16%)	62
Oceanário	39	**22** (56%)	41	**24** (64%)	40
Sé	61	**25** (41%)	43	**22** (36%)	44

Use case: smart taxes



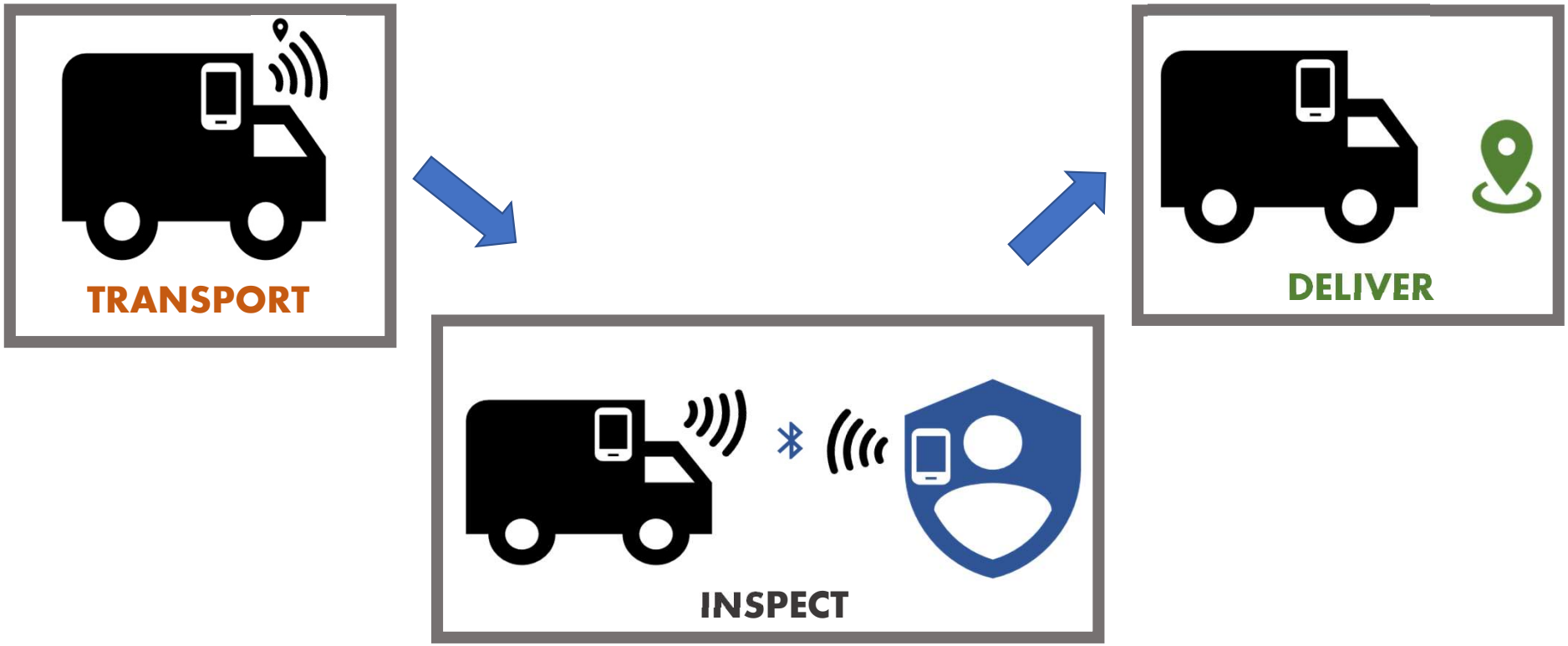
- Track movements of goods
  - Mitigate fake shipments
- Combine location proofs with digital notaries:
  - Time-stamping
  - Long-term archival
  - Tamper-resistance
- Extend existing infrastructure with dedicated devices

STOP

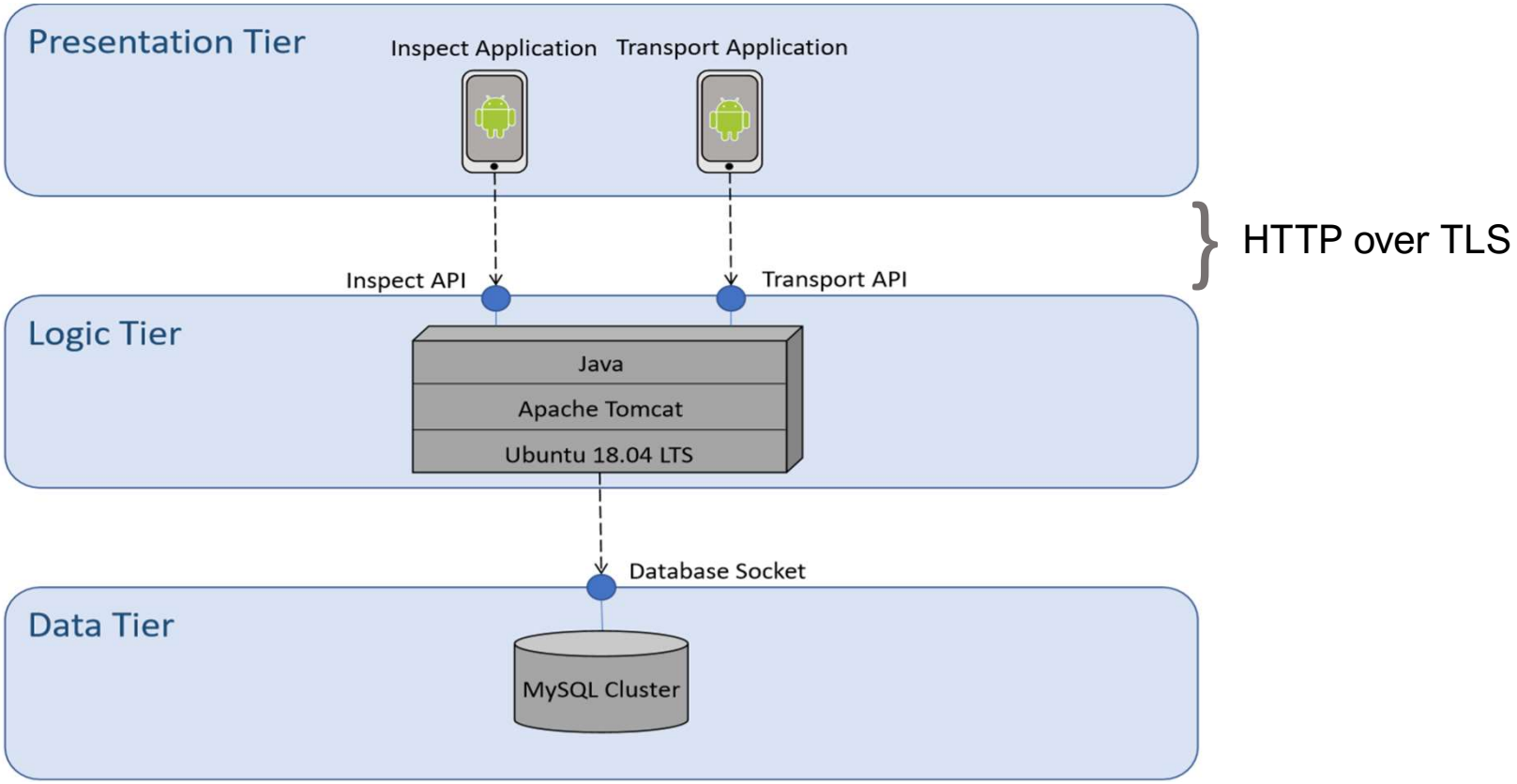
Secure **T**ransport l**O**cation **P**roofs for vehicle inspections

Henrique Santos

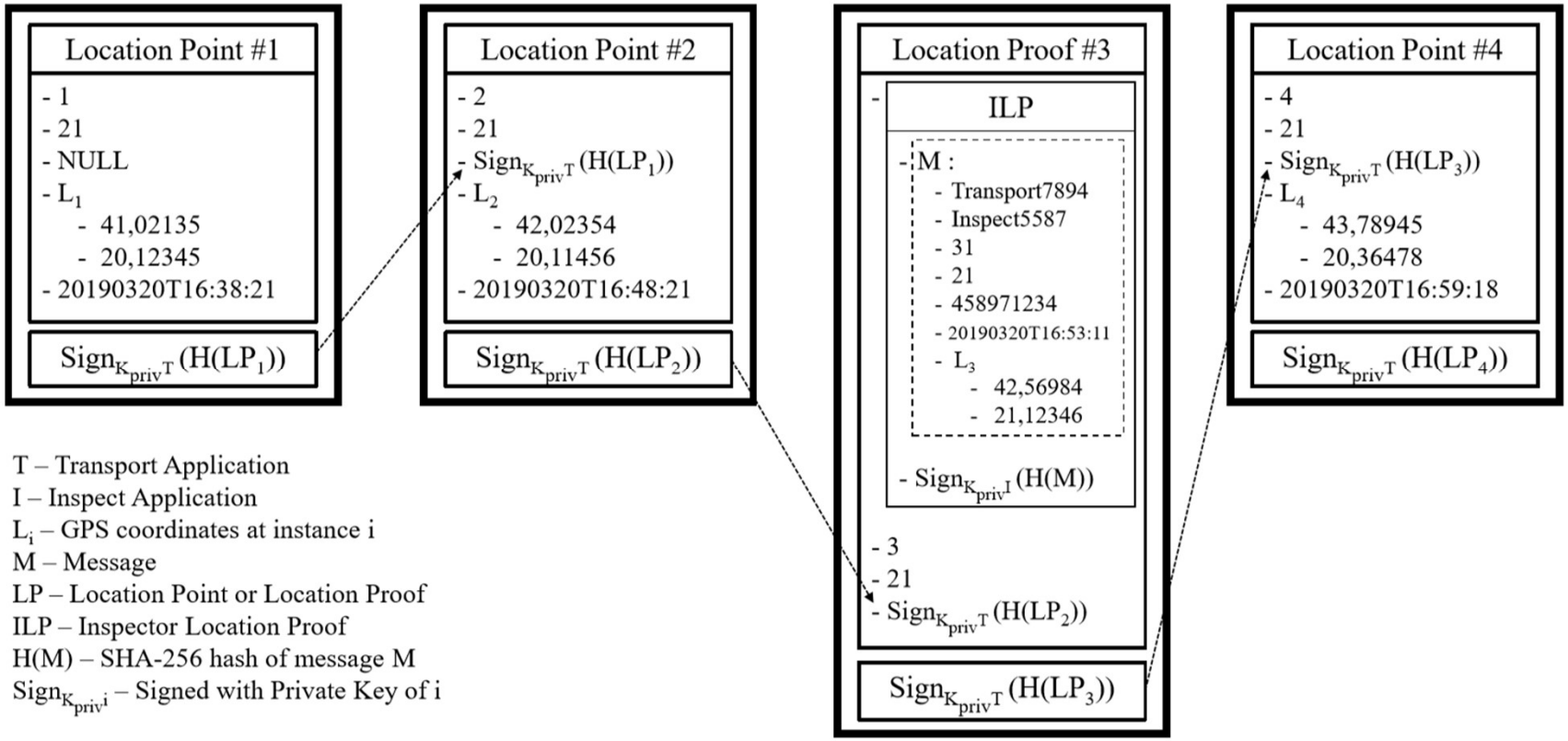
Process Overview



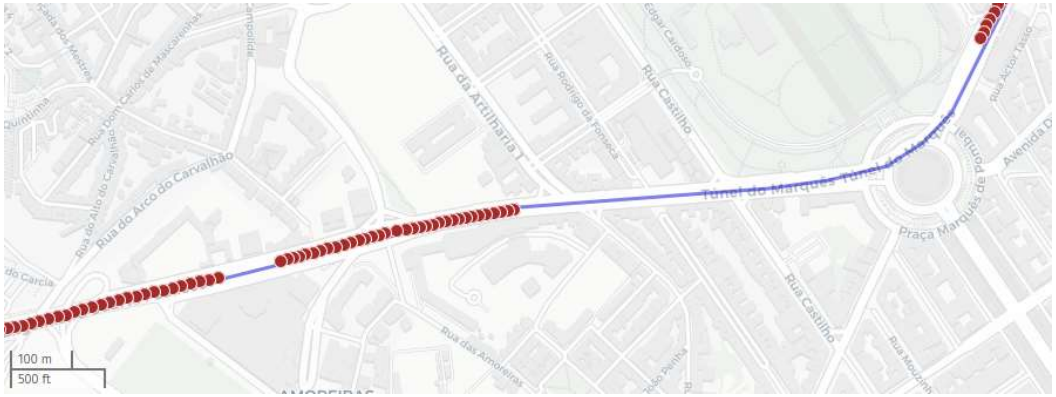
Architecture



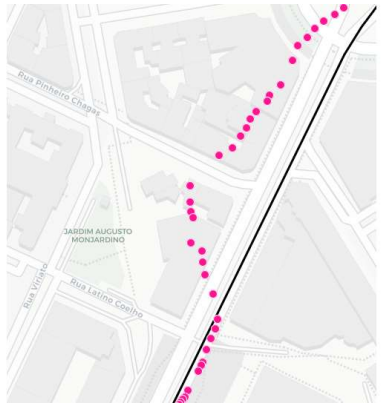
Location Chain

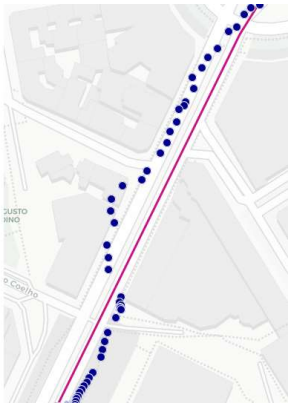


Location Accuracy



Issues inside of a tunnel



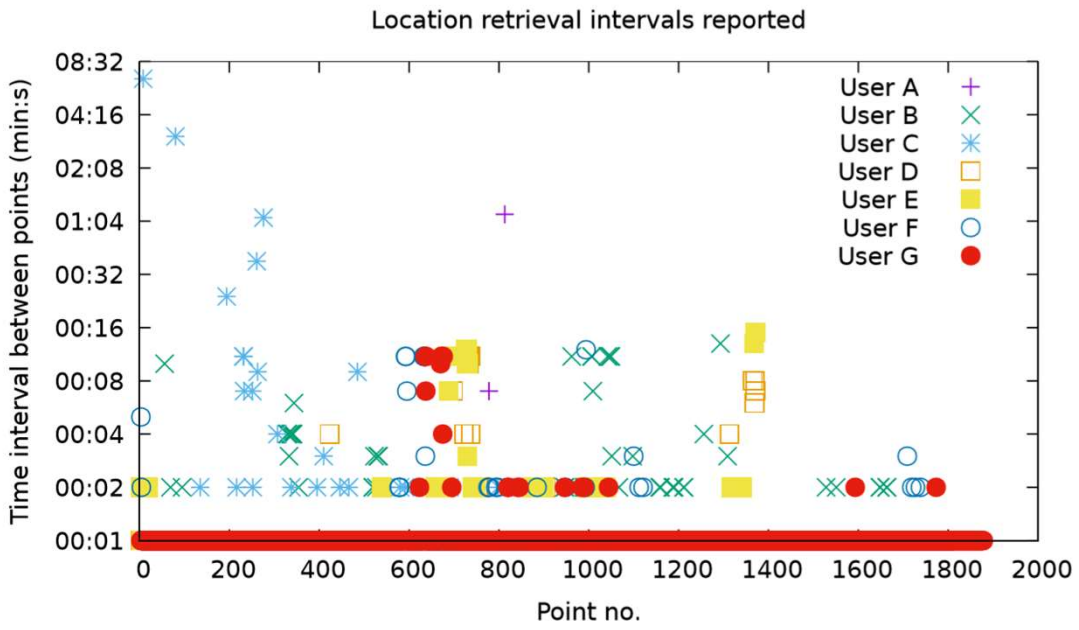


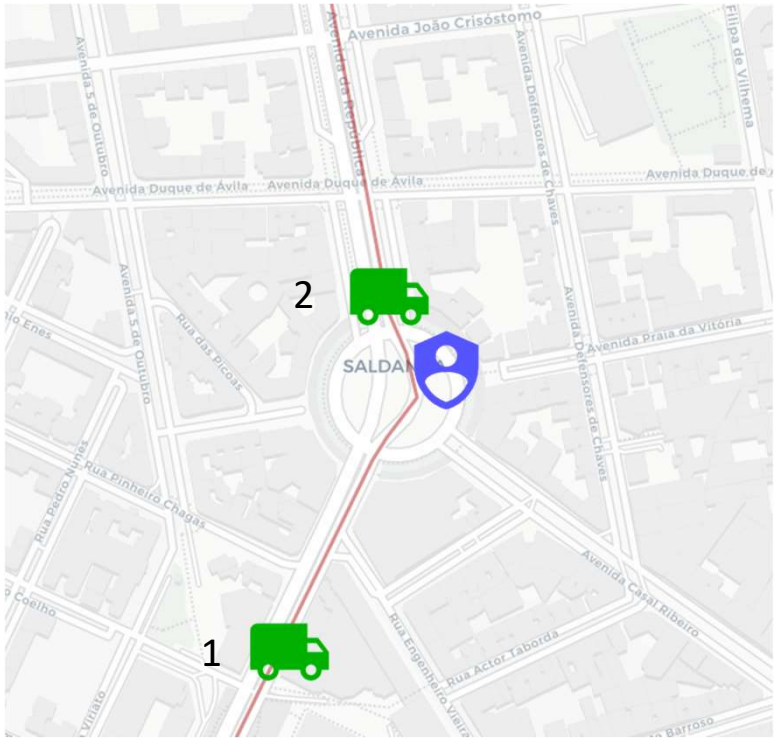
Issues with surronding buildings

Inspection Selection Parameters

Location Retrieval Rate: 1 second

Inspection Selection Range: 500 meters





Selection issue with user B

Bluetooth Interaction

- We assumed the Bluetooth connection would be maintained during the duration of the inspection procedure
  - This was proven wrong
  - Therefore we suggest a two-phase protocol

Standard Container in Truck

STOP prototype

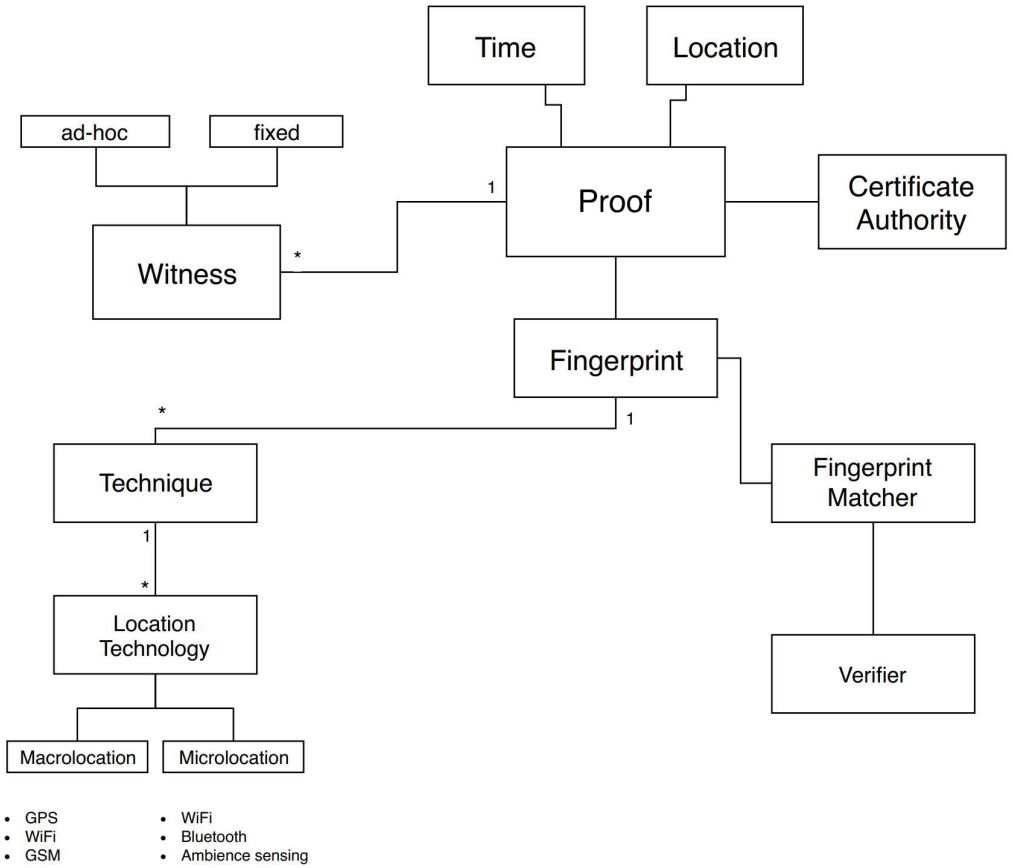
- Implemented Android applications and Central Ledger
  - Collects location information of transportation vehicles
  - Improves transportation inspection
  - Location Chain projects all location events of a transportation
- The evaluation showed:
  - Accurate location tracking
  - Reliable location retrieval rate and optimal selection rule
  - Feasibility of the inspection protocol

Ongoing work

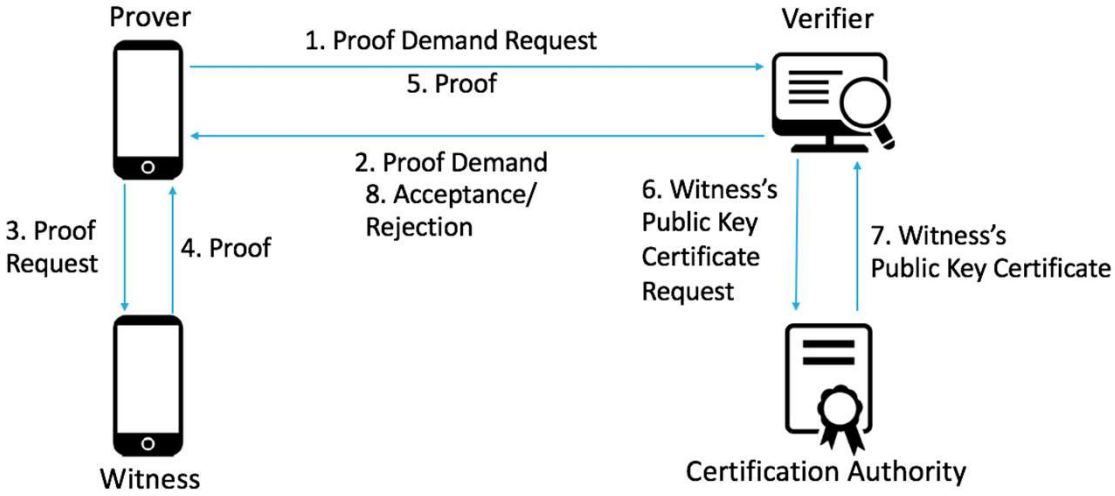
SureThing framework

- Open to diverse technologies
- Proof data format
  - Transport
  - Composition
  - Signature
- Proof assessment
  - Weight, rank, compare *strength* of proofs

SureThing conceptual model



Thank you!



Device location certification for the Internet of Things

http://surething-project.eu

miguel.pardal@tecnico.ulisboa.pt

Invitation SureThing Event
Advances in Internet of Things and Location

- Friday, January 10th, 2020
  - Hotel Roma, Lisboa
  - 09:00-17:00
- Keynote: Joshua Siegel (MIT, MSU)
- Panel Discussion: industry and academia
- SureThing project
  - Current prototypes and future work

- More information, and registration at:
  - http://surething.tecnico.ulisboa.pt/workshop/

SureThing publications (selection)

- Diogo Calado, Miguel L. Pardal. *Tamper-proof incentive scheme for mobile crowdsensing systems*. IEEE International Symposium on Network Computing and Applications (NCA), 2018.
- João Ferreira, Miguel L. Pardal. *Witness-based location proofs for mobile devices* (short). IEEE International Symposium on Network Computing and Applications (NCA), 2018.
- Gabriel A. Maia, Miguel L. Pardal. CROSS: loCation pROof techniqueS for consumer mobile applicationS. INForum, 2019.
- Henrique F. Santos, Miguel L. Pardal. Operation STOP: itinerary verification for smart vehicle inspections. INForum, 2019.
- Sheng Wang, Rui Claro, Miguel L. Pardal. SPYKE: Security ProxY with Knowledge-based intrusion prEvention. INForum, 2019.
- Pedro E. Carmo, Miguel L. Pardal. IoT Neighborhood Watch: device monitoring for anomaly detection (short). INForum, 2019