Performance Evaluation of Blockchain-based Proof of Location

Michele Amoretti, Francesco Zanichelli

Department of Engineering and Architecture - University of Parma, Italy
Distributed Systems Group
http://dsg.ce.unipr.it
Contact: michele.amoretti@unipr.it

Motivation

- **Location-Based Service (LBS)**

--> geographic locations claimed by users must be factual

- **Proof of Location (PoL)**:
digital certificate of presence (time + space)

- **Problem:** define a robust decentralized proof-of-location scheme

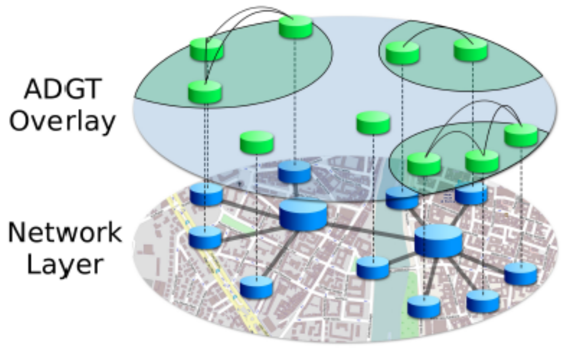
Proposed scheme

M. Amoretti, G. Brambilla, F. Medioli and F. Zanichelli, "**Blockchain-based Proof of Location**," in Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, July 2018

- Store PoLs into a **blockchain**
  = cryptographically secure distributed ledger

- **Proof of Stake** approach for creating new blocks
  - reduced energy consumption
  - wider array of solutions for discouraging Sybil groups
  - reduced centralization risk
  - economic penalties against malicious players

System architecture

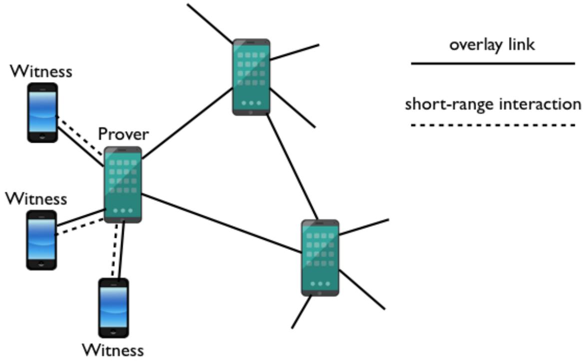


- **LBS-oriented peer-to-peer network** (e.g., ADGT or Overdrive)
- Mobile nodes with short-range communication technologies (e.g., Bluetooth)

- **Prover** = peer that collects proofs of (its own) location from neighbors

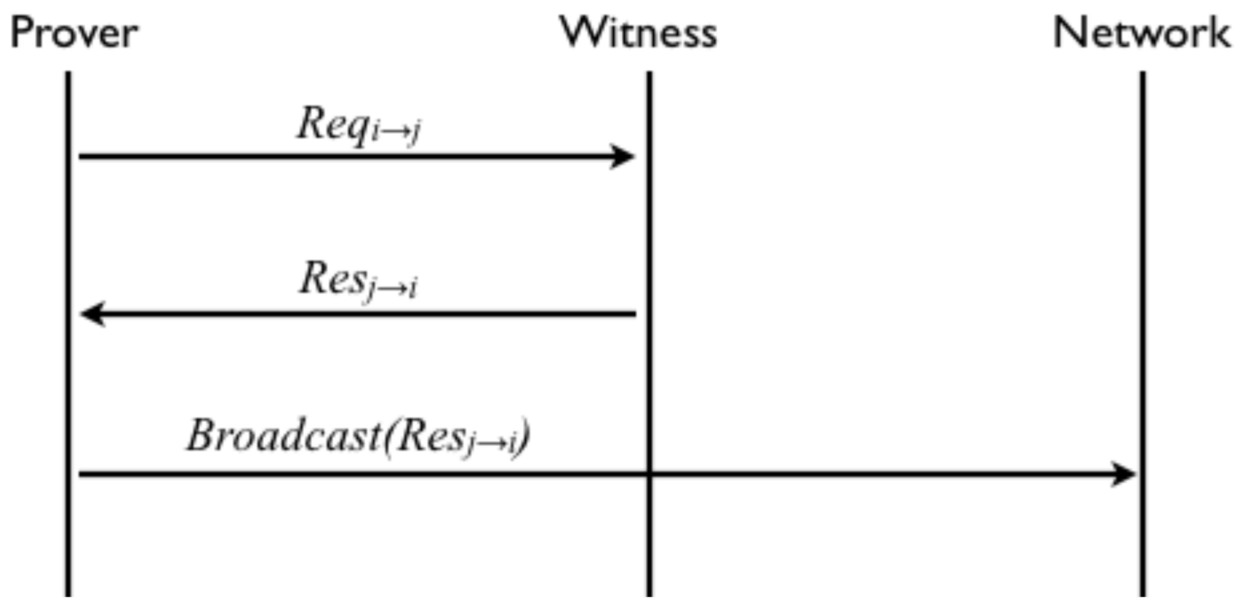
- **Witness** = peer that provides PoLs to neighbors

- Peer with public key K_i^{pu} as unique identifier
- Peer with private key K_i^{pr} for digital signatures



Blockchain construction

- Construction and diffusion of a PoL:



Blockchain construction

- Structure of a **request** issued by a Prover toward a Witness:

$$Req_{i \to j} : \left\{ \begin{array}{c} K_i^{pu} \\ \langle latitude, longitude \rangle_i \\ h(Block_{t-1}) \\ timestamp \end{array} \right\}_{K_i^{pr}}$$

- Structure of a **response** issued by a Witness toward a Prover:

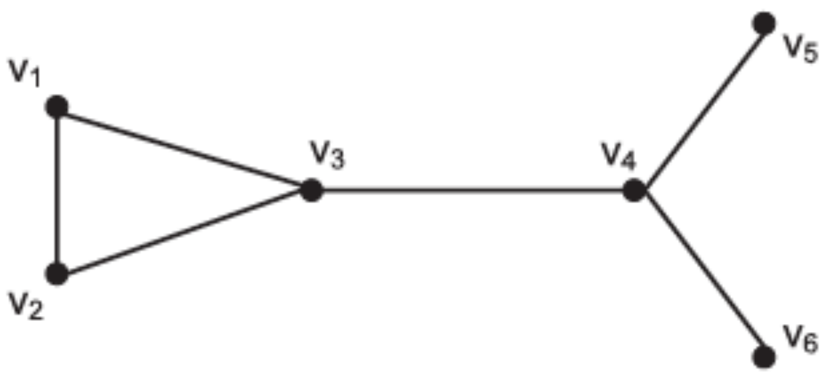
$$Res_{j \to i} : \left\{ \begin{array}{c} Req_{i \to j} \\ K_j^{pu} \\ \langle latitude, longitude \rangle_j \\ timestamp \end{array} \right\}_{K_j^{pr}}$$

- Both parties perform **validity checks** on received messages.

Blockchain construction

- Generic peer that receives a PoL:

- if the declared location is within short-range communication area
    - validate if target is reachable
- else
    - either discard immediately (conservative approach)
    - evaluate the **betweenness B** of the Prover and Witness, in the pseudonym correlation graph (using the blockchain!)

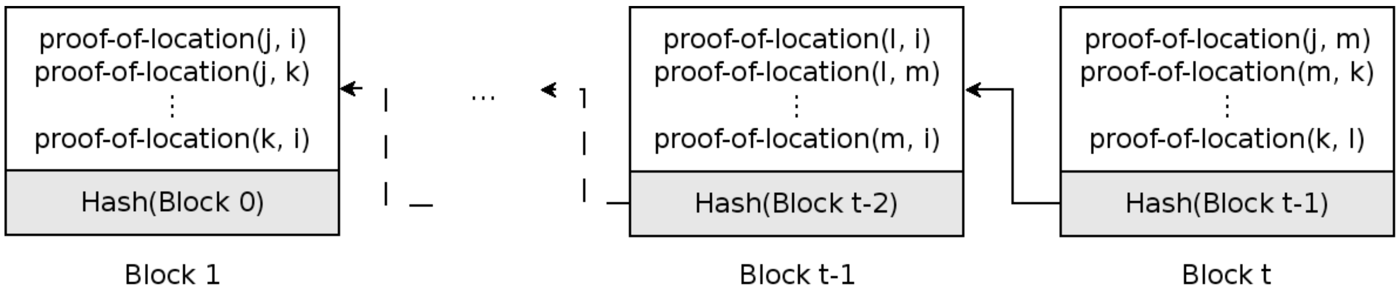


B(v4) = 7 good!
B(v6) = 0 bad!

Blockchain construction

- Block construction (any peer can do it):

$$Block_t : \left\{ \begin{array}{c} Res_{j\to i} \\ Res_{j\to k} \\ \vdots \\ Res_{k\to i} \\ K_i^{pu} \\ h(Block_{t-1}) \end{array} \right\}_{K_i^{pr}}$$



Distributed consensus

- A peer may receive several blocks concurrently

- **Pseudo-random decision** on which block to add to the blockchain

--> choose *WHP* the block produced by the peer with the largest number of PoLs in the latest *T* valid blocks

Distributed consensus

- **Malicious peers can be penalized** by honest peers
- They can **loose their stake**
- They can get a **mark of infamy** (stored into the blockchain)

Robustness Analysis

- The proposed blockchain-based PoL scheme is **robust against all major LBS-related attacks**, namely:

- cheating on own geographic location
- cheating on another peer's geographic location
- replaying proofs of location
- colluding with other peers to generate false PoLs
- determining real identities of peers

For details:

M. Amoretti, G. Brambilla, F. Medioli and F. Zanichelli, "**Blockchain-based Proof of Location**," in Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, July 2018

Penalizing cheating peers

- **Upon receiving a PoL, honest peers**..

  1) create check if the distance between the two peers that produced the PoL is consistent with short-range communication; if not, mark both peers as infamous and produce a **denial of location (DoL)**;

  2) check if one or both peers that declare to be in the neighborhood are within short-range reach; if not, produce a DoL;

  3) look into the blockchain for the latest PoLs related to the peers; if the received PoL is not consistent with one or both those ones, **mark one or both peers as infamous** and produce a DoL.

Performance evaluation

G. Brambilla, M. Picone, M. Amoretti, and F. Zanichelli, "**An Adaptive Peer-to-Peer Overlay Scheme for Location-Based Services**," in Proceedings of the 13th IEEE International Symposium on Network Computing and Applications (NCA), 2014

- Simulated scenario:
  - **ADGT** overlay network
  - number of peers n
  - wandering velocity v [m/s]
  - square area with side S [m]
  - each peer monitors a circular area of radius ρ [m]
  - coverage percentage CP [%]
  - short-range communication distance σ [m]
  - PoL rate for each peer r [s^{-1}]
  - set of cheating peers --> fraction P [%] of n

- $n = 100$
- $v = 1$ m/s
- $S = 1500$ m
- $\rho \in \{500, 1000\}$ m
- $CP \in \{25, 50, 75\}$ %
- $\sigma \in \{50, 100, 150\}$ m
- $r = 1/60\ s^{-1}$
- $P \in \{25, 50, 75\}$ %

DEUS

Performance evaluation

- **Cheating behavior**:

  1.a) create a proof for a false location (help from cheater located nearby the false location)

  1.b) geocast the proof of location

  2.a) discard received denials of location

  2.b) always propagate proofs of location produced by cheaters

  2.c) propagate proofs of location from honest peers if they are consistent with the blockchain (otherwise turn them to denials of location)

Performance evaluation

- Performance indicators:

  - **MC [%]** = percentage of marked cheaters

  - **TP [%]** = percentage of stored true proofs WRT the total number of true proofs of location;

  - **FP [%]** = percentage of stored false proofs of location WRT the total number of false proofs of location

  - **ACC [%]** = percentage of stored true proofs of location plus non-stored false proofs of location, versus the total number of true and false proofs of location

Performance evaluation

- Baseline approach (without mark of infamy):

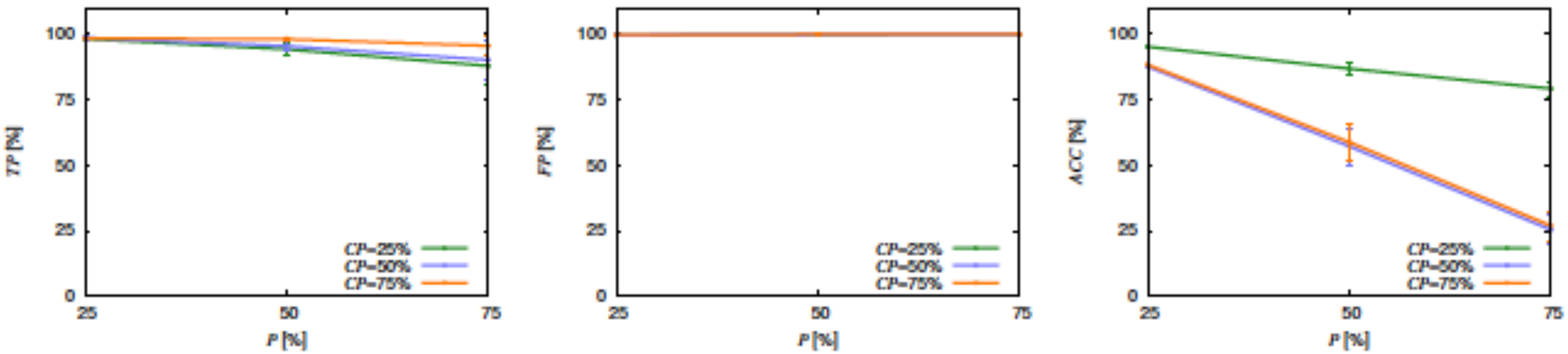


Fig. 1. Final TP, FP and ACC for different values of P and CP, with $(\sigma, \rho) = (100, 500)$ considering the baseline approach, where no mark of infamy is assigned to malicious peers.

Performance evaluation

- Proposed approach:

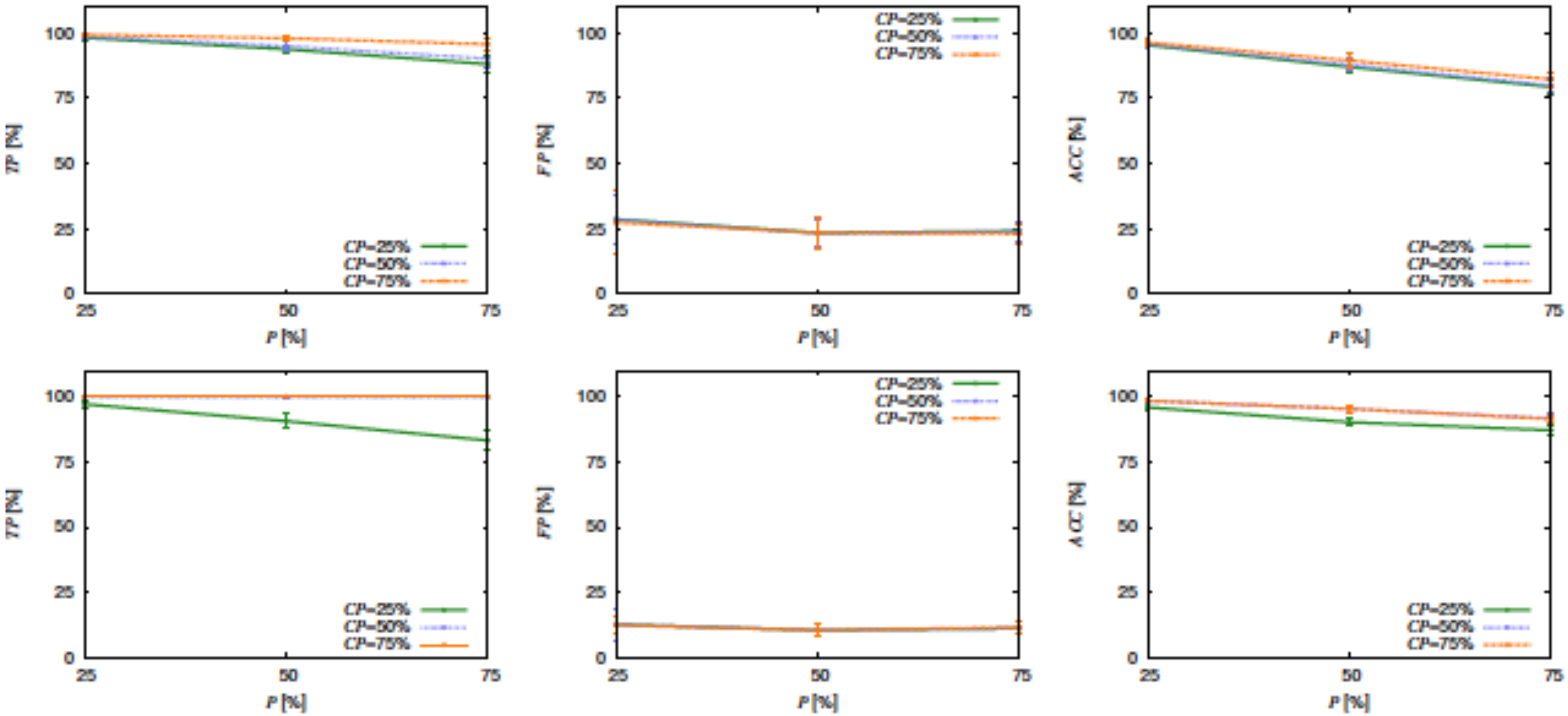


Fig. 2. Final TP, FP and ACC for different values of P and CP, with $(\sigma, \rho) = (100, 500)$ (top) and $(\sigma, \rho) = (150, 1000)$ (bottom).

Performance evaluation

- Proposed approach:

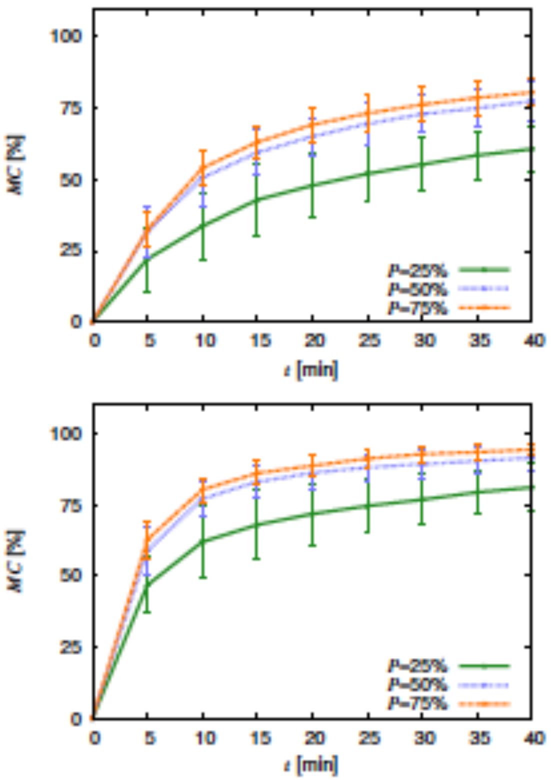


Fig. 3. MC growth, for different P values, with $(\sigma, \rho) = (100, 500)$ (top) and $(\sigma, \rho) = (150, 1000)$ (bottom).

Performance evaluation

- Proposed approach:

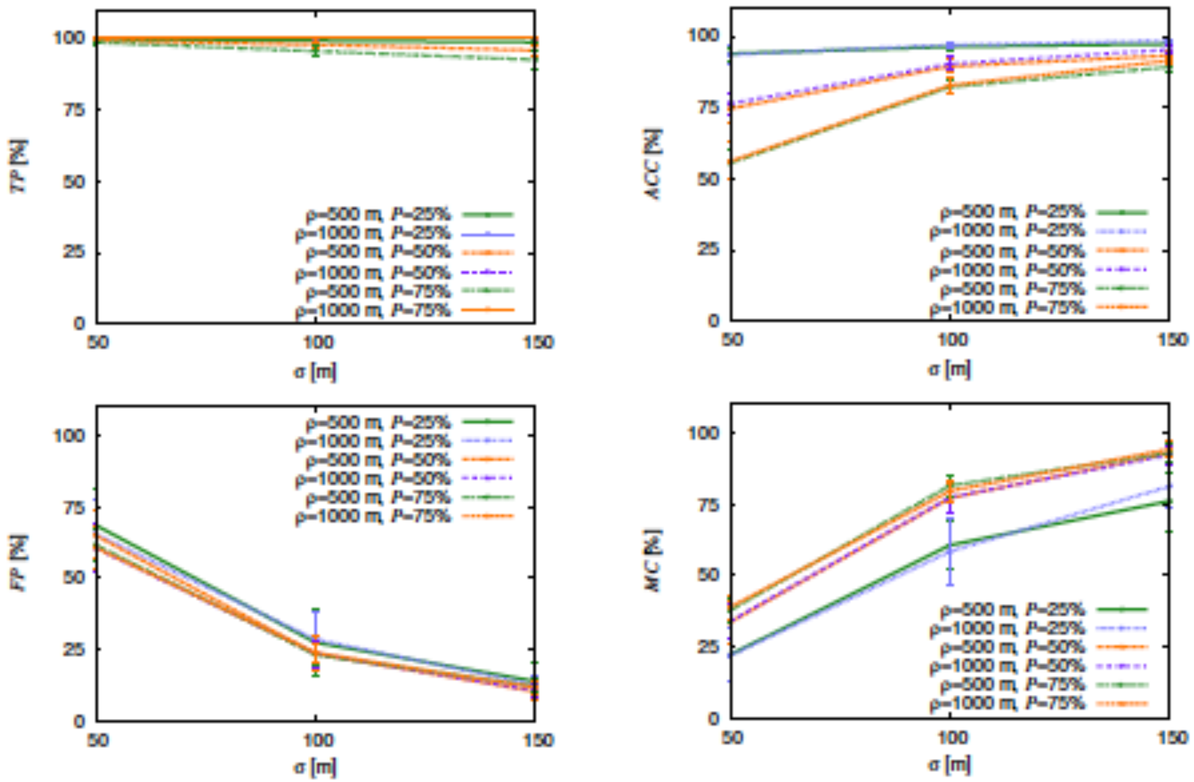


Fig. 4. Final TP, FP, ACC and MC for different values of σ, ρ and P, assuming $CP = 75\%$.

Conclusion and Future work

- Blockchain-based proof of location is possible!
- .. and very challenging

- Simulate other attack and defense strategies

- Study variants of the proposed scheme

- Evaluate advanced privacy preservation approaches (e.g., zero-knowledge proofs)

- Compare with commercial solutions (Platin, XYO, FOAM,..)

Thank you!