4th of April 2023

Distributed Systems Seminar

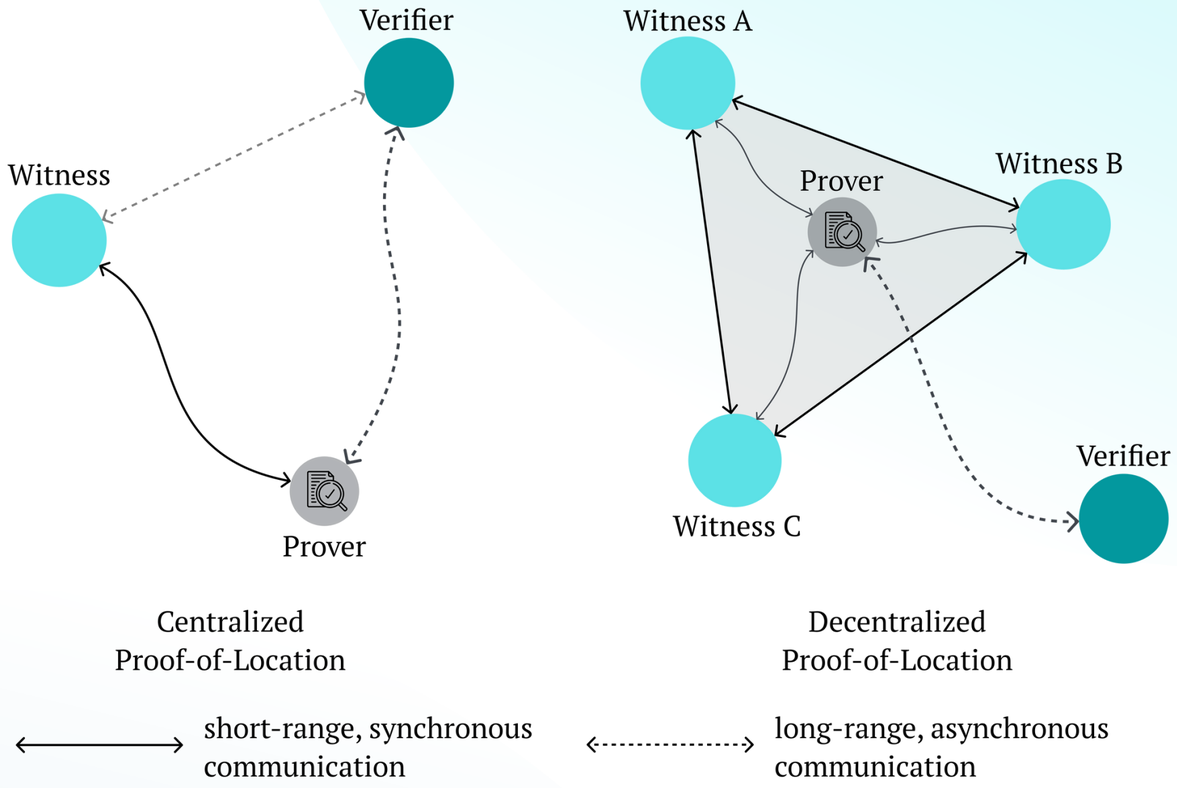
Towards Decentralized Proof-of-Location

Eduardo Ribas Brito

UNIVERSITY OF TARTU
Institute of Computer Science

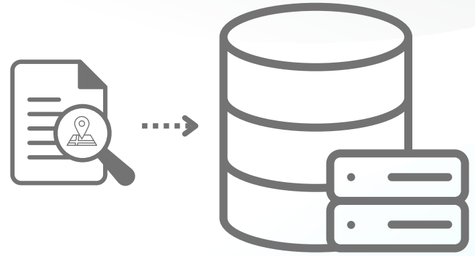
A digital Proof-of-Location

Is an electronic certificate that attests one's relative position in both space and time [1].



[1] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, "Blockchain-based proof of location"

The evolution of Location Proof Systems



2002 - 2013

The first proof of location schemes in a centralized setting.

[2] Brent R. Waters and Edward W. Felten, "Secure, Private Proofs of Location."

2014 - 2017

A distributed shift takes place with different infrastructure-dependent approaches.

[3] C. Javali et al, “I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol"

2018 - Future

Multiple decentralized and infrastructure-independent protocols start emerging.

[4] B. Nasrulin, M. Muzammal, and Q. Qu, “A robust spatio-temporal verification protocol for blockchain"

Secure

[5] A. Dupin, J.-M. Robert, and C. Bidan, “Location-proof system based on secure multi-party computations"

Decentralized

[6] Mohammad Reza Nosouhi, Shui Yu, Wanlei Zhou, Marthie Grobler, Habiba Keshtiar, "Blockchain for secure location verification"

Private

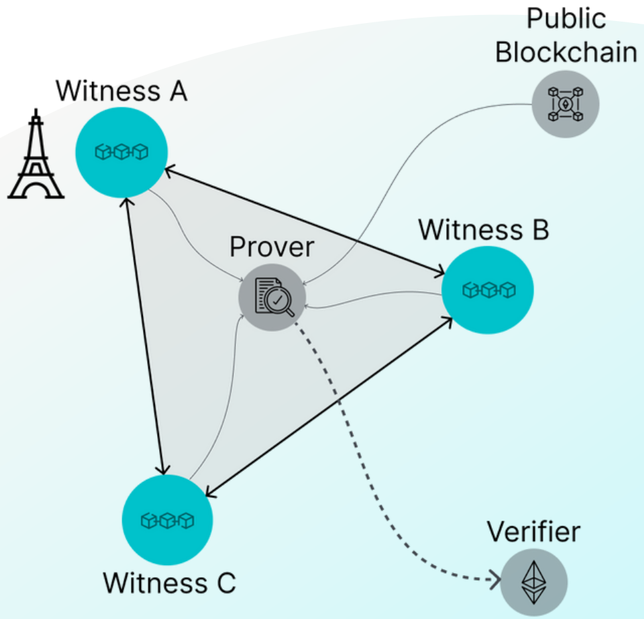
[7] Mamunur Akand et al, "Privacy-preserving Proof-of-Location With Security Against Geo-tampering"

Trustless

[8] Foamspace Corp, "FOAM: Technical Whitepaper - a decentralized Proof of Location protocol"

A Proof-of-Location protocol may be considered secure if:

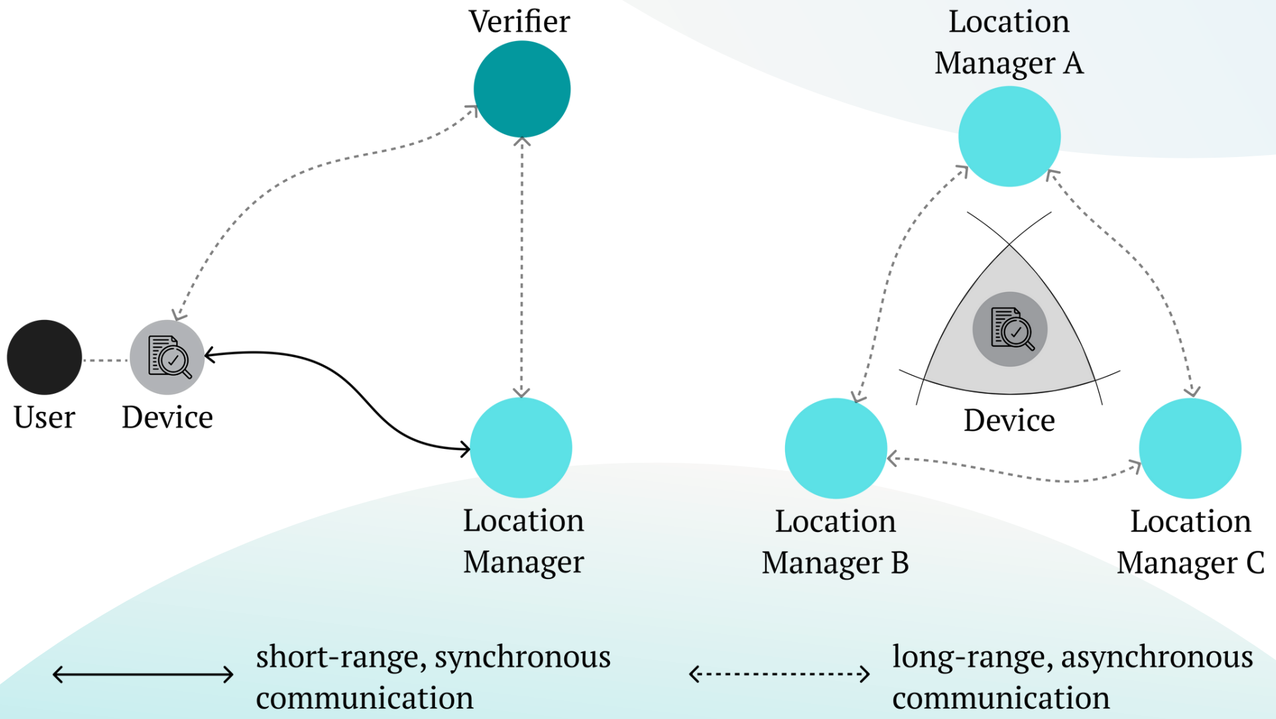
- complete,
- spatio-temporally sound,
- non-transferable.



Trusted and Centralized Architectures

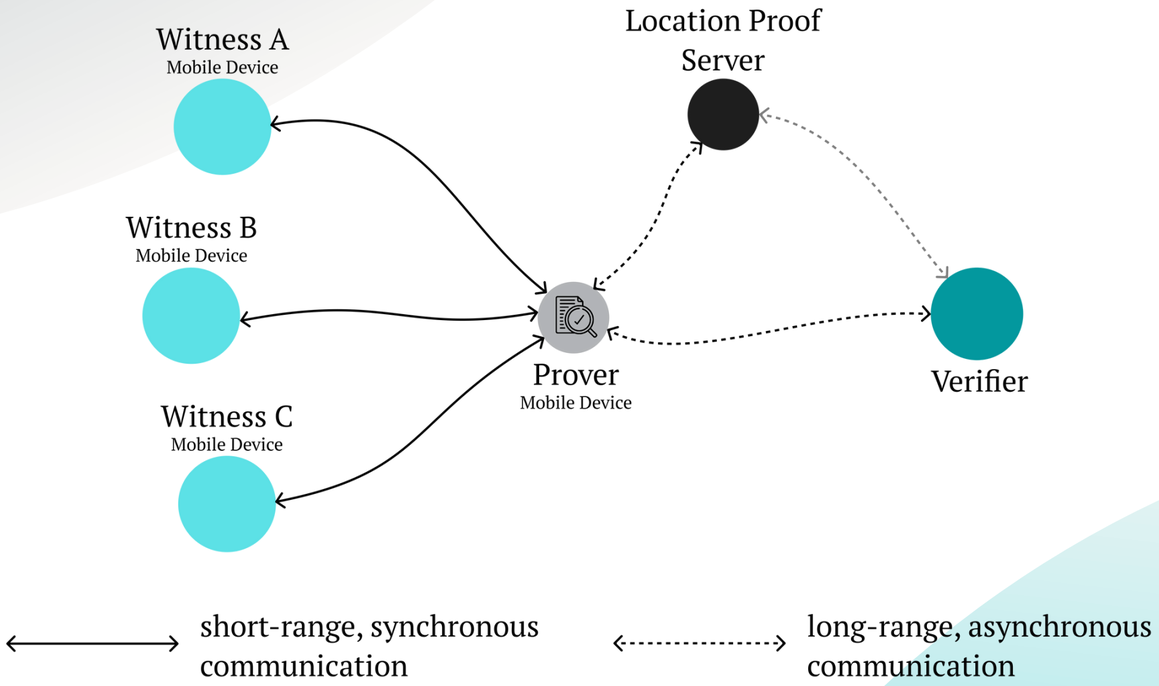
A location-proving system:

- By proximity, with integrity and privacy guarantees.
- Assuming
  - a trusted verifier, device and location manager,
  - an untrusted user.
- Using round-trip and signal propagation latency metrics.



[9] Brent R. Waters and Edward W. Felten, "Secure, Private Proofs of Location."

Progressively Distributed and Decentralized Protocols



A privacy-aware distributed protocol:

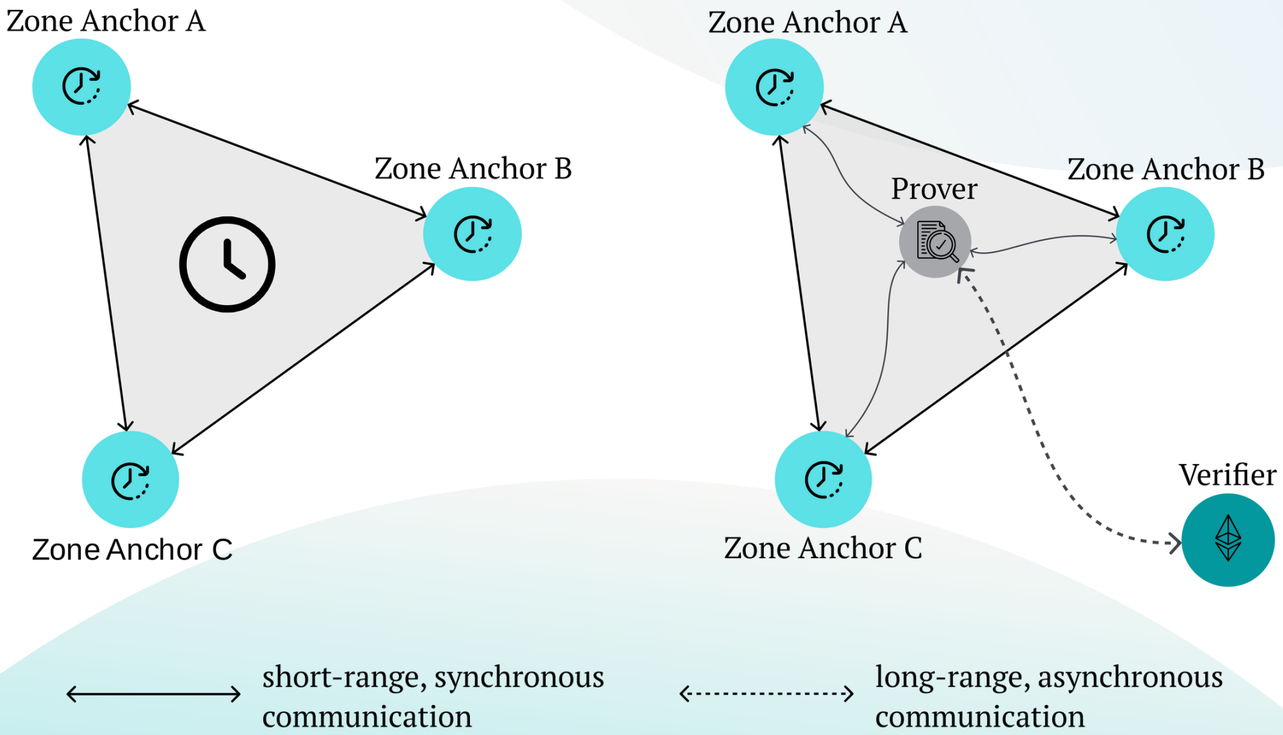
- Using Bluetooth-enabled mobile devices for proof generation.
- Assuming trusted prover, verifier, and witnesses.
- Following a user-centric privacy model through statistical pseudonym changing.
- Storing location-proof records in a trustless manner.

[10] Z. Zhu and G. Cao, “Applaus: A privacy-preserving location proof updating system for location-based services”

Fully Trustless Environments

A decentralized protocol that:

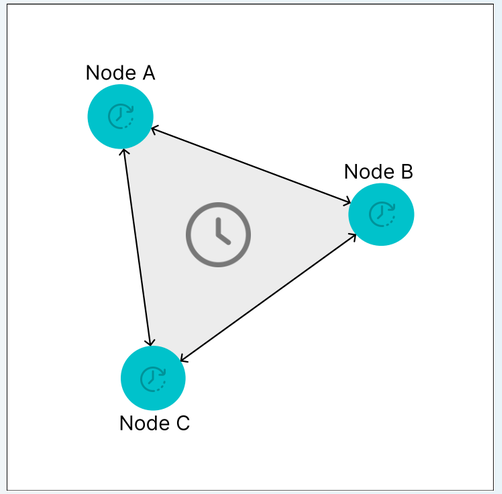
- Is based on dynamic clock synchronization for trustless, spatio-temporally sound location services.
- May include token-curated registries, and crypto-economic incentives.
- Aims to create a consensus-driven map of the world.



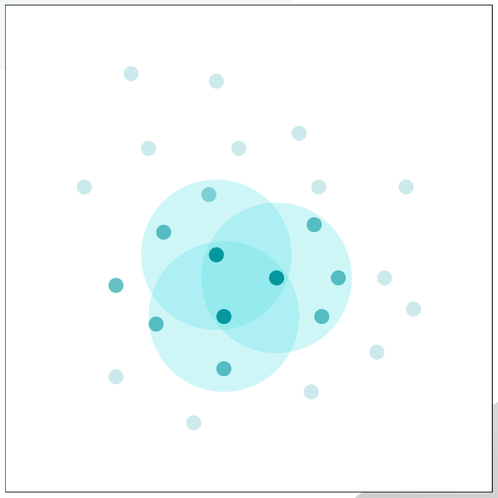
[11] R. J. King, “Foam: The importance of time synchronization.”

From dynamic and non-hierarchic Mesh Networks . . .

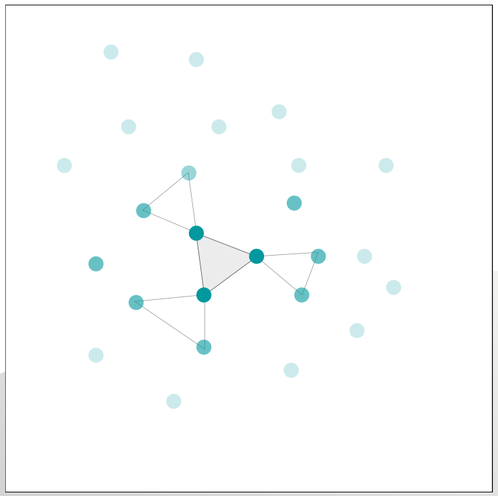
Zone Synchronization



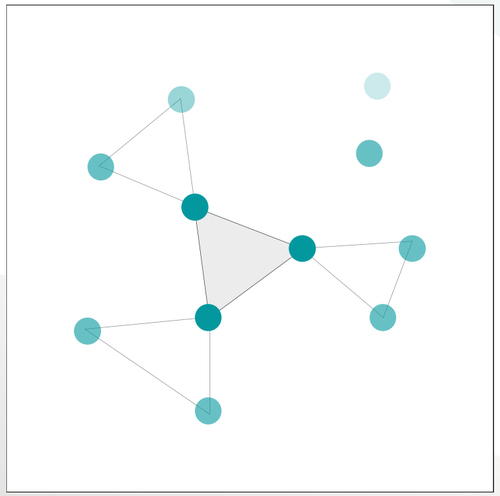
Mesh Network

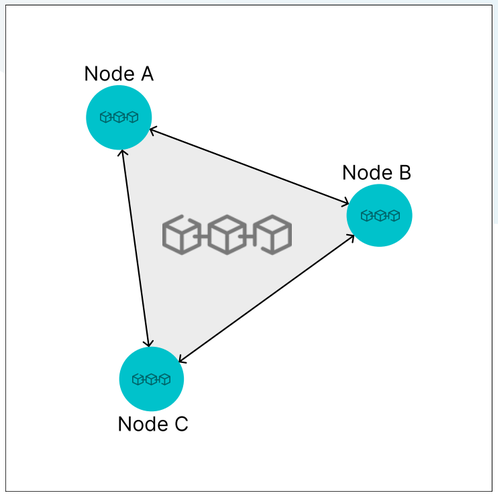


Zone Establishment



Zone Affinity

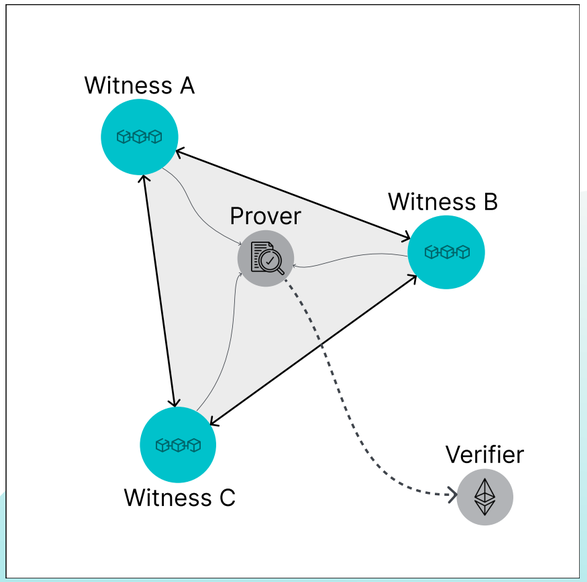




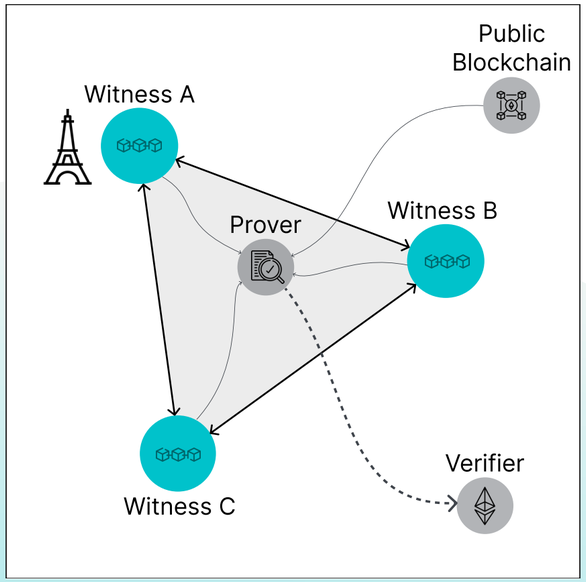
. . . To Absolute Proof-of-Location

Witness Presence

Relative PoL



Absolute PoL



4th of April 2023

Distributed Systems Seminar

Towards Decentralized Proof-of-Location

Eduardo Ribas Brito

UNIVERSITY OF TARTU
Institute of Computer Science