LAMP: Towards efficient audit protocols for network and distributed systems

Lamyae Hassini - Laurent Réveillère, Joachim Bruneau-Queyreix

PROGRESS - Univ. Bordeaux, LaBRI, France

Fault-detection in distributed systems

Requirements:

Completeness: Faulty nodes are exposed or suspected forever

Accuracy: no correct node is falsely exposed

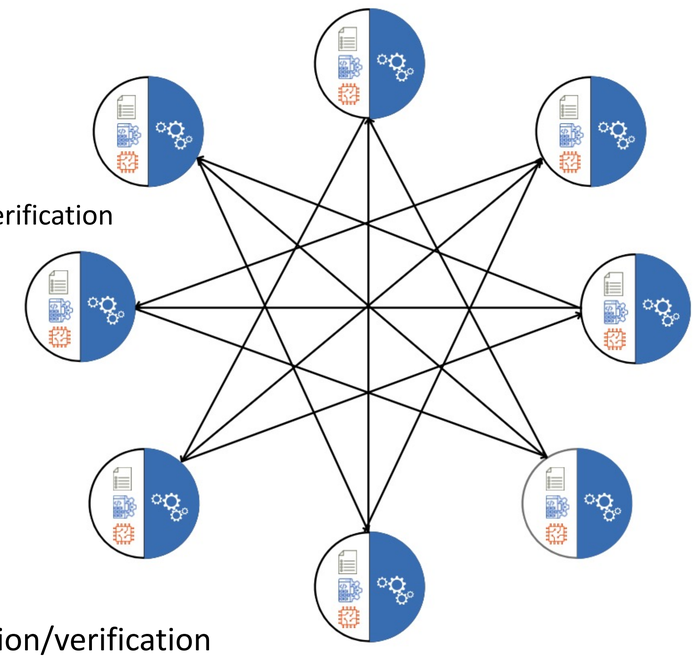
Applications:

- Routing
- Banking systems
- Distributed Databases

Problem statement

Regular node operates:

- Application
- Fault-detection protocols:
  - consistency checks
  - tamper-evident logging & verification
  - Execution auditing



with fault-detection mechanisms:

- Multiple witness' association
- Log reporting
- Execution replay
- Crypto. commitment generation/verification

Problem: fault-detection incurs substantial resource-consumption, degrading performance

LAMP: efficient and lightweight fault-detection protocol

Lightweight nodes

- Application
- Fault-detection mechanisms
  - Log reporting
  - Commitment generation

Trusted and reliable auditor

Trusted audit service

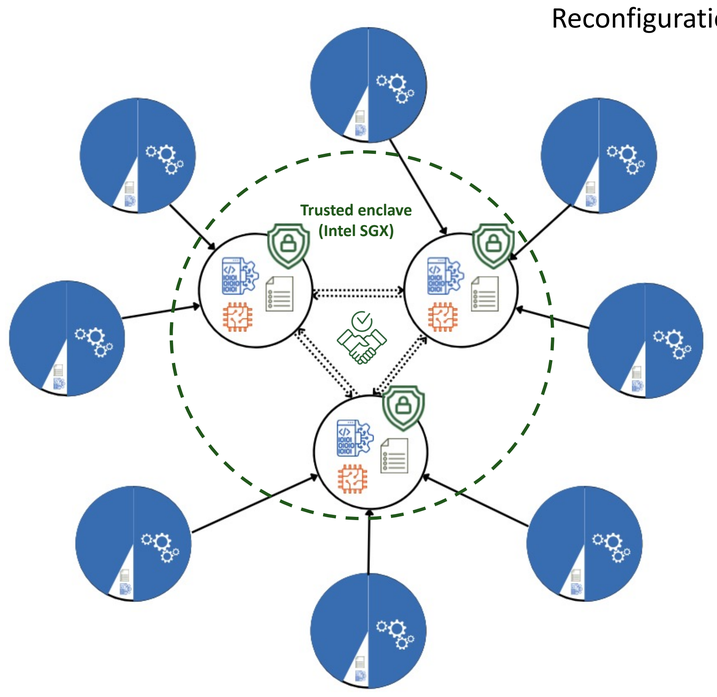
- Commitment verification
- Execution replay

Reliable service

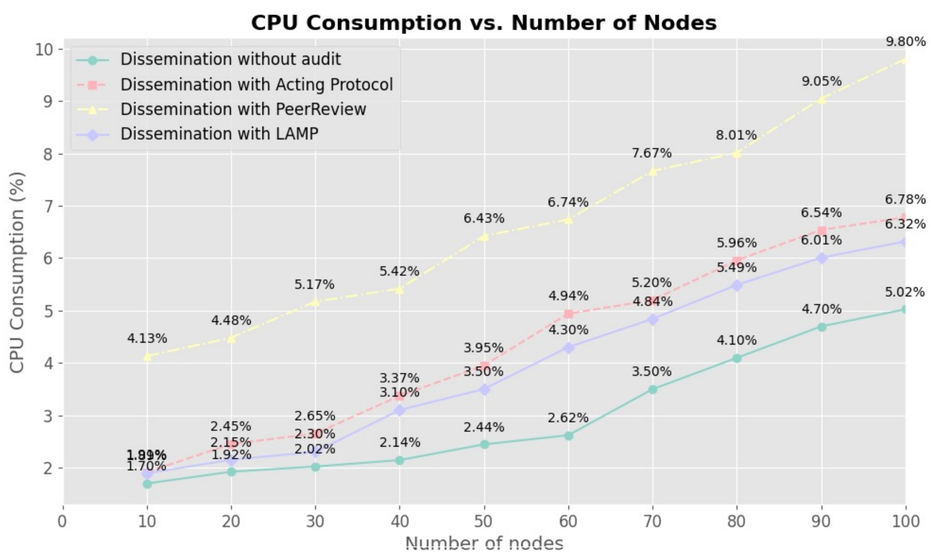
State reliable broadcast

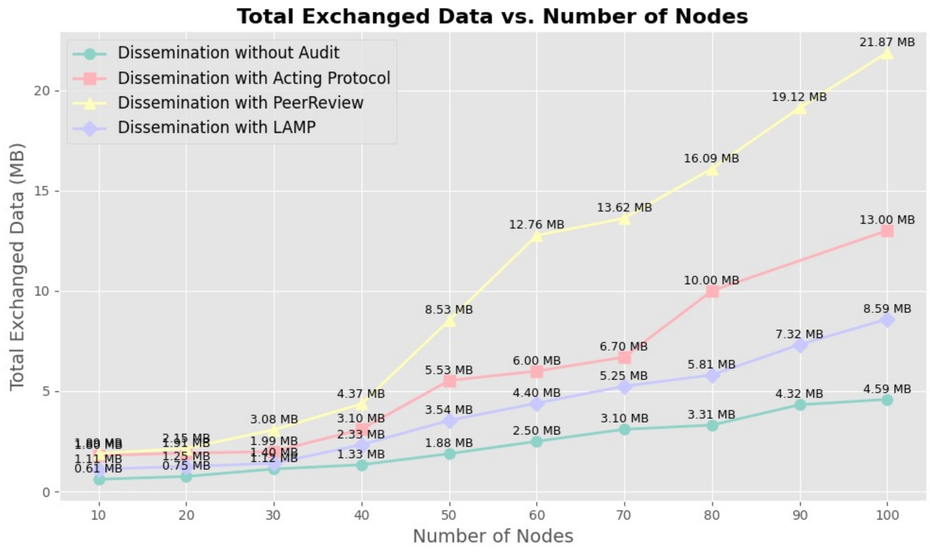
Deterministic auditor association

Reconfiguration under faults



Performance comparison between LAMP and state-of-the-art fault-detection protocols





- Gossip-based data dissemination protocol
- Cluster of 10 machines, scaled to 1–100 nodes
- Evaluated fault-detection Protocols: PeerReview, Acting, and LAMP

- Experimental metrics on consumption, fault detection quality, and audit service impact.

Future work

- **Performance Evaluation:** LAMP's performance evaluation on network-intensive and CPU-intensive applications
- **Privacy Enhancement:** Zero-Knowledge Proof (ZKP) for privacy and confidentiality

Scientific cooperation

LIRIS Laboratory (UMR 5205, CNRS, INSA Lyon)

Dr. Sonia Ben Mokhtar, CNRS Research Director at LIRIS