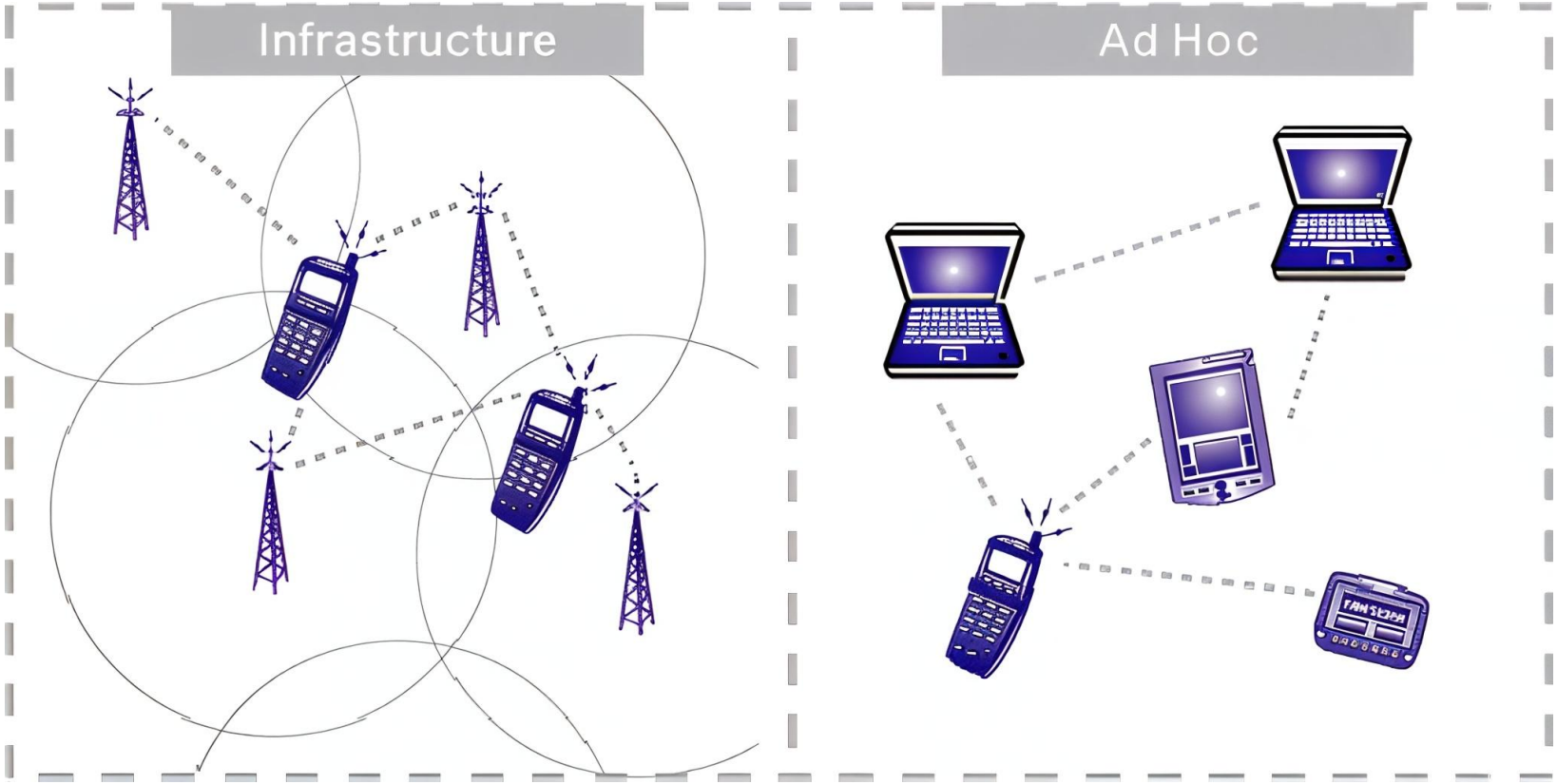
IEEE NCA 2025

Rûm: Multivalued Loss-Tolerant Byzantine Consensus for Mobile Ad-Hoc Networks

João Pedro B. M. B. Leite (presenting)
David Rogério Póvoa de Matos
Guilherme Henrique Caçador Ramos

Mobile Ad-hoc Networks (MANETs)



Consistency Guarantees

- Weak Consistency
  - Eventual Consistency
    - Distributed counter
  - Causal Consistency
    - Chat App
- Strong Consistency
  - Atomic Broadcast
    - State Machine Replication
  - Atomic Compare & Swap
  - Leader Election
  - Locking

Need Consensus for Stronger Consistency

- **Defining Properties**
  - Validity:
    - If all correct processes propose the same value v, then any decision is of v.
  - Agreement:
    - No two correct processes decide different values.
  - Termination:
    - Each correct process eventually decides a value.

Assumptions and Impossibility

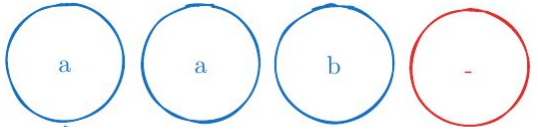
Asynchronous Network, Deterministic Algorithm, Process Crashes

Fischer, Lynch, and Paterson (FLP)

Synchronous Network, Deterministic Algorithm, Message Loss

Santoro and Widmayer

Rûm: Consensus for MANETs

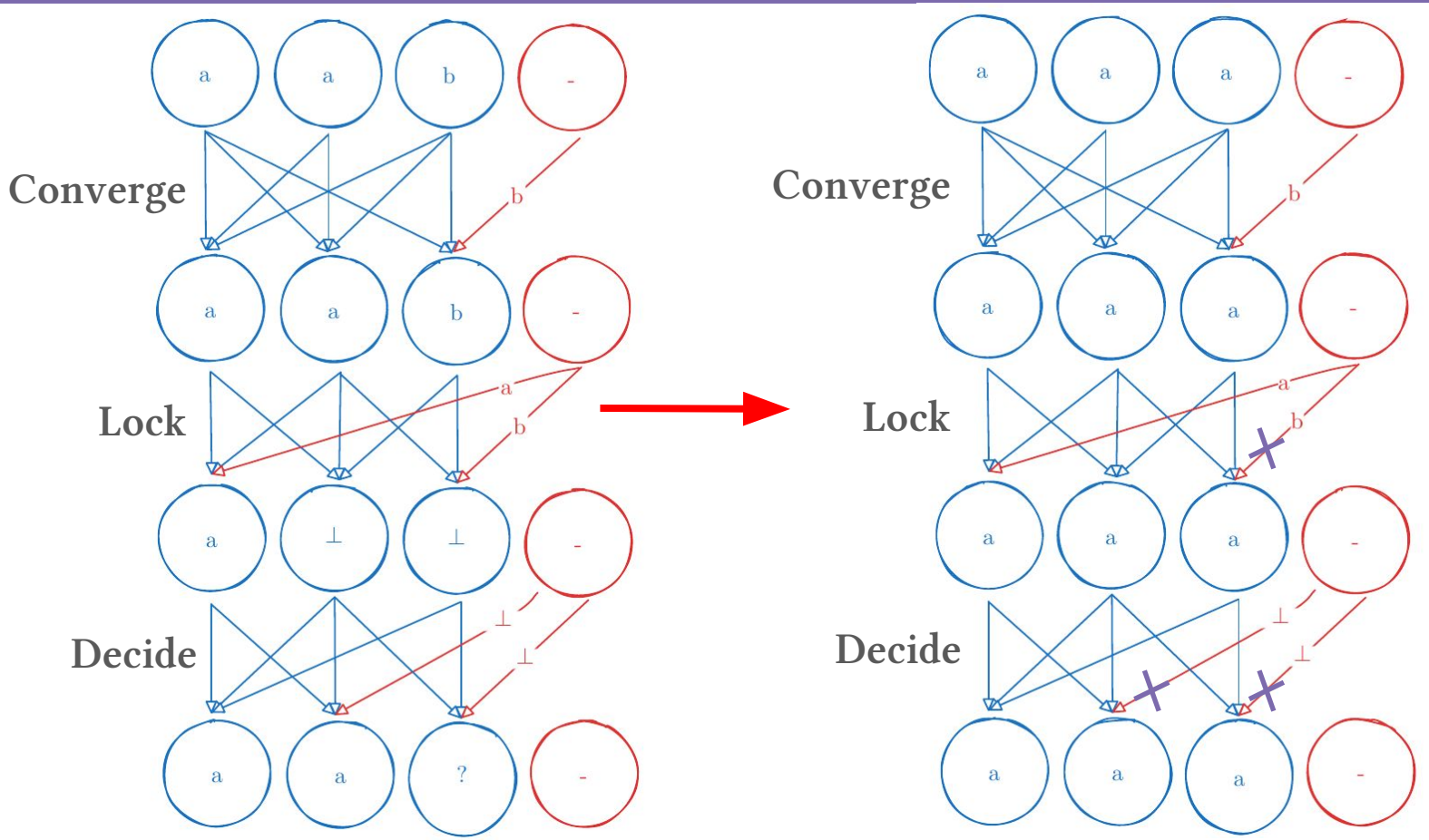


- Designed for MANETs
  - Arbitrary valued
  - Asynchronous
  - Message-Loss Tolerant
  - Byzantine Fault Tolerant
    - 1/3 fault tolerance
  - Broadcast-Based

$$\langle i, \phi_i, v_i, status_i \rangle$$

ID Phase Value Decision status

Rûm: Loss-Tolerant Asynchronous Consensus



Message Validation: Curbing Byzantine Behaviour

- **Authenticity Validation**
  - Stop impersonation
  - Stop corruption
  - Digital Signatures
    - 3rd party verification

- **Semantic Validation**
  - Logical validation
    - No contradictions
    - Correct trace
  - Justification Messages
    - Piggybacked
    - Or retransmitted

$$\langle i, \phi_i, v_i, status_i \rangle$$

ID Phase Value Decision status

- Leverage Asynchrony
  - Adopt higher phase messages
  - Slow processes can catch up
  - Improves convergence
- Increase loss tolerance
  - One message can catch up
  - Must block all fast forward messages

$$\langle i, \phi_i, v_i, status_i \rangle$$

ID Phase Value Decision status

Rûm: Message Loss Bound

$$\sigma < \left\lfloor \frac{n+f}{2} \right\rfloor \left(n - f - \left\lfloor \frac{n+f}{2} \right\rfloor \right)$$

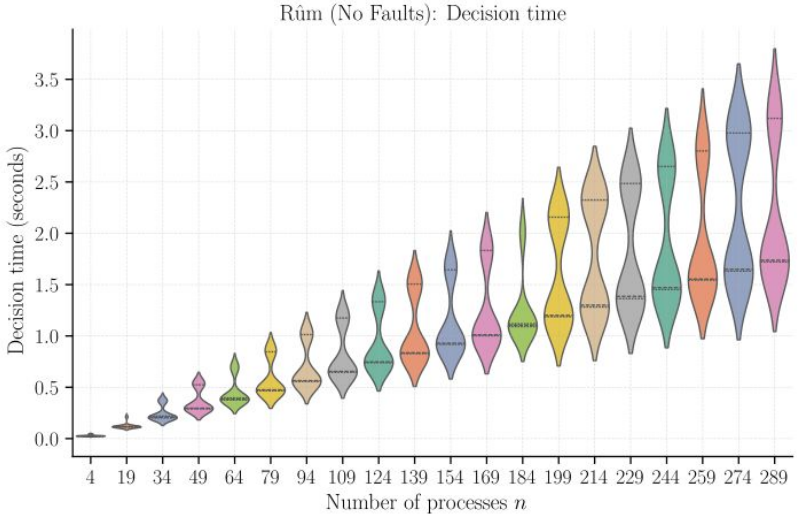
Quorum - 1 ⟷ Correct - (Quorum - 1)

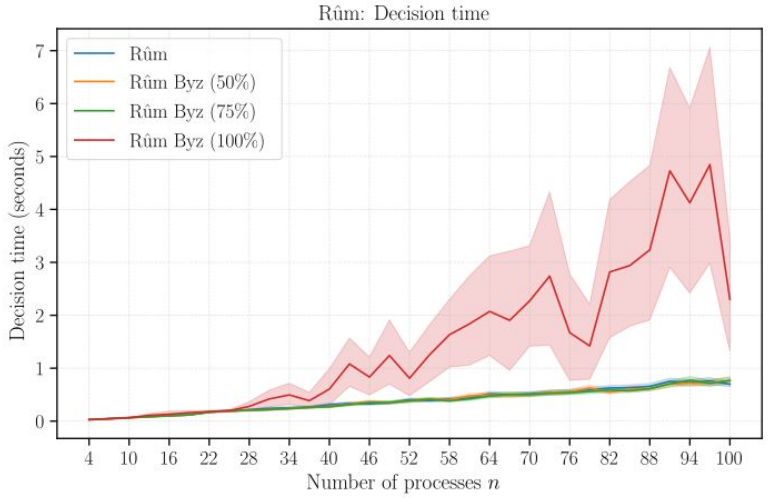
Block all messages between

Evaluation

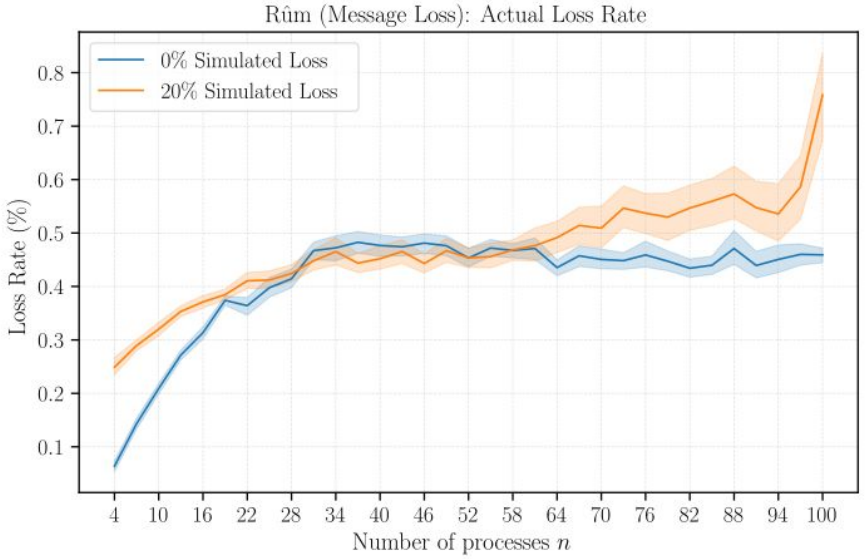
Rûm: Faults

Implemented and simulated Rûm in the ns-3 network simulator

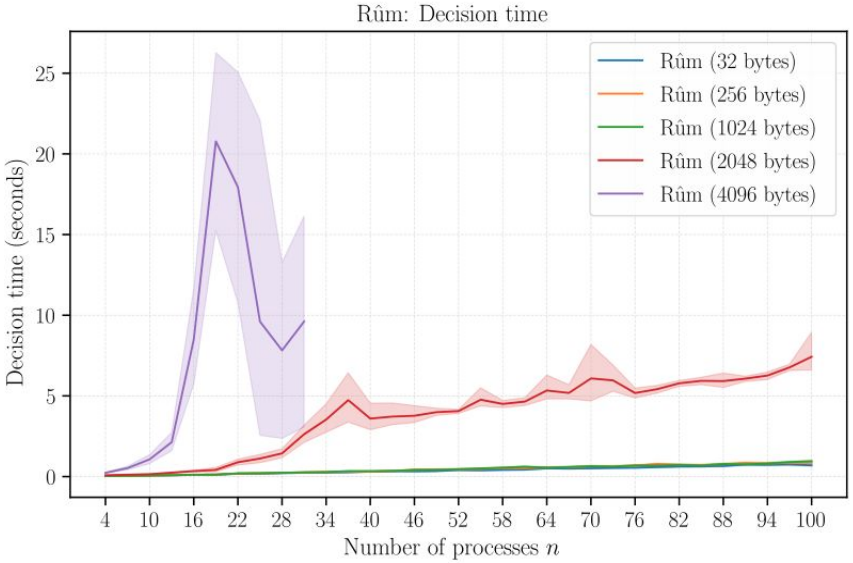


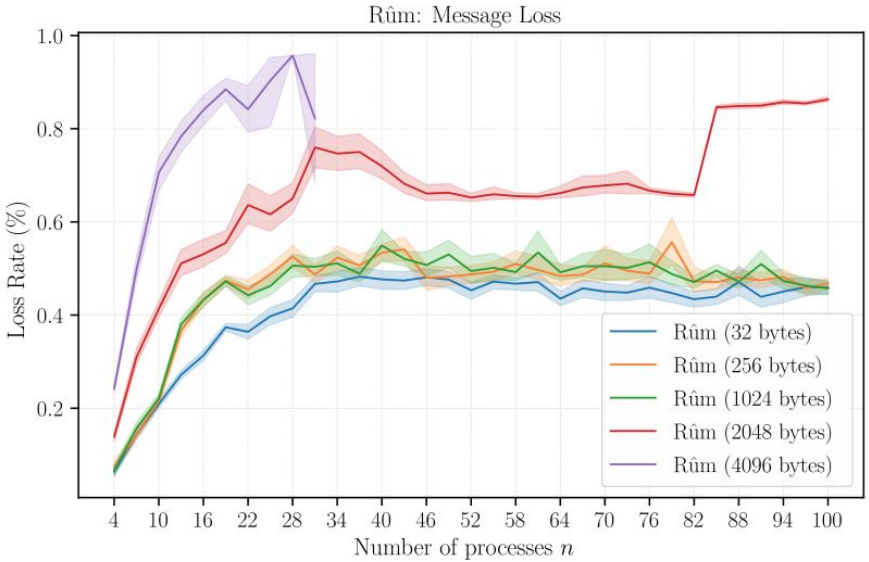


Rûm: Message Loss



Rûm: Proposal Size





Finishing up

Takeaways

Message Loss is stronger than Crash Faults

Nondeterminism allows for Loss Tolerant Consensus

Leverage Asynchrony

Leverage Broadcast-Based Communication

Q&A

Extra Slides

Rûm: Proposal Intersection

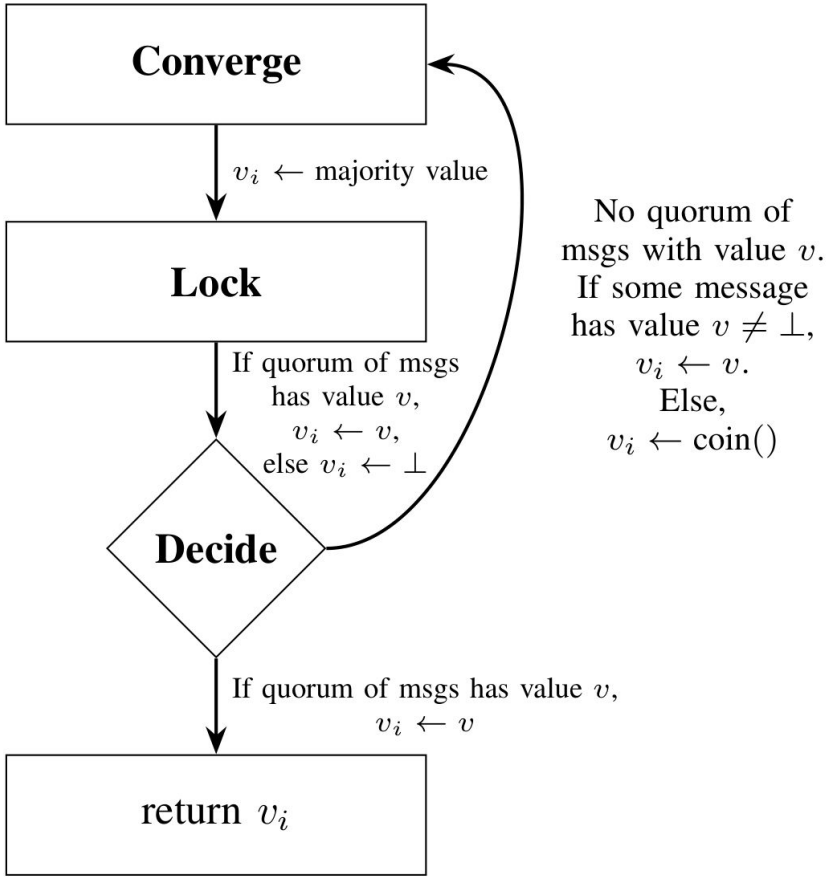
- 1 proposal
  - Trivial termination
- 2 values
  - Intersection in all processes.
- > 2 values
  - Any two processes intersect in one proposal.

- # distinct proposals must
  - stay constant
  - or decrease
- No change
  - processes must receive all proposals
  - non-null chance of all picking the same value
- Decrease
  - eventually reach only 2 distinct values

Theorem 5 (Adversarial Steering)**.** *Let $\mathcal{D}$ be the set of correct processes that proposes the value v. In general, with $t \leq f$ faults, it is sufficient that $|\mathcal{D}| + t > \frac{n+f}{4} + \frac{1}{2}$ for the colluding byzantine processes to force a correct process to choose v as its majority.*

Consensus for MANETs

- System Model
  - Asynchronous network
  - Digital Signatures
  - Have access to random choice
- Threat Model
  - Corrupt messages
  - Impersonate devices
  - Delay and reorder messages
  - Know internal state of all devices
  - At most 1/3 devices are evil


Converge
$v_i \leftarrow$ majority value
Lock
If quorum of msgs has value v, $v_i \leftarrow v$, else $v_i \leftarrow \perp$
Decide
No quorum of msgs with value v. If some message has value $v \neq \perp$, $v_i \leftarrow v$. Else, $v_i \leftarrow$ coin()
If quorum of msgs has value v, $v_i \leftarrow v$
return v_i