Tolerating Common-Mode Faults in Byzantine Consensus

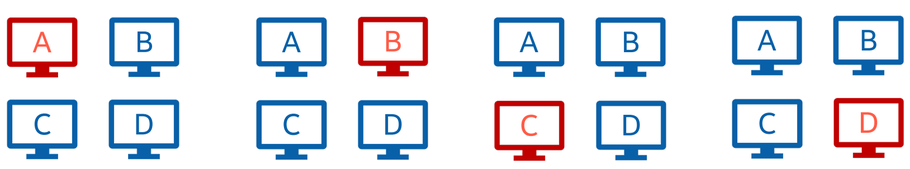
Lachlan J. Gunn, Pooja Yadav, N. Asokan

Aalto University

- Current BFT protocols tolerate any *f* out of *n* replicas faulty.
- Problem: In real systems, some combinations of failures are more likely than others.
- Solution: incorporate knowledge of failure-modes into consensus protocols.

Existing Consensus protocols

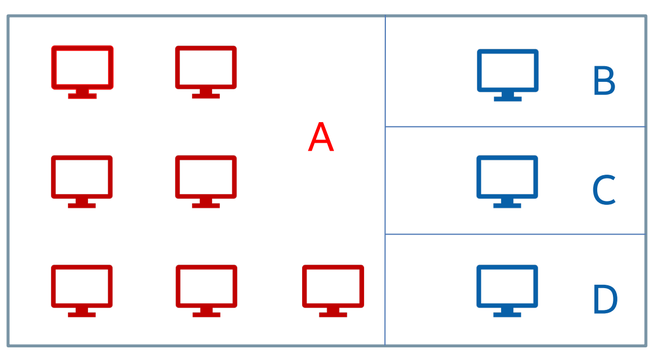
- *f* out of *n* fault model: any *f* faults possible out of n replicas.
- Best when faults are independent and identically distributed.
- Maximum fault-tolerance: $\lfloor (n-1)/3 \rfloor$ faults.



Tolerable faults under *f* out of *n* model. The failure of any one replica does not cause a failure of the replicated system.

Common-mode faults

- Example: each replica is run by a different company.
- System can tolerate the compromise of any one company.
- What if A wants to *add more replicas* for reliability?



- Now, the system can tolerate more faulty replicas overall.
- But compromise of A's network now causes 7 faults:
  - no longer tolerable under the *f* out of *n* model.

Our goals

- Incorporate failure mode knowledge into BFT protocols.
- Generalize the $\lfloor (n-1)/3 \rfloor$ limit.

Quorum rules

- BFT protocols include *quorum rules* of the form

  "after receiving *t* consistent messages, <do something>"

- We can incorporate *failure-mode knowledge*.

Example

Rule:

"after receiving responses from a 2/3 majority of replicas from each of 2/3 of participating companies"

Result:

The protocol tolerates faults of:

- every replica of up to a third of companies, and
- up to a third of replicas run by each other company

Composition of quorum rules

We show which faults are tolerated by rule combinations:

- (Rule A) AND (Rule B)
- (Rule A) OR (Rule B)
- *t* of the following hold:
  - Rule A for replicas in set A
  - Rule B for replicas in set B
  - …

Open questions

- Do these combinations cover all interesting quorum rules?
- Can we select quorum rules to maximize fault-tolerance based on e.g. fault-trees?
- Is there a limit that generalizes $f < \lfloor (n-1)/3 \rfloor$?

Research Institute for Collaborative Autonomous and Resilient Systems