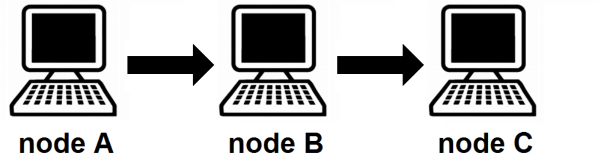
Limiting Byzantine Influence in Multihop Asynchronous Networks

Alexandre Maurer and Sébastien Tixeuil

March 12, 2012

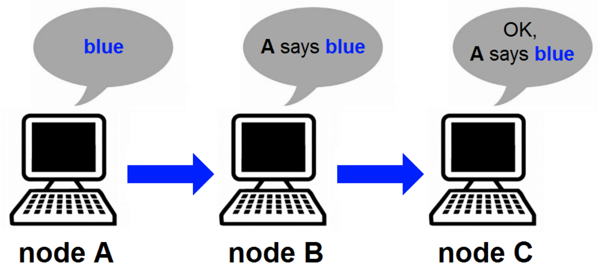
Table of contents

Introduction



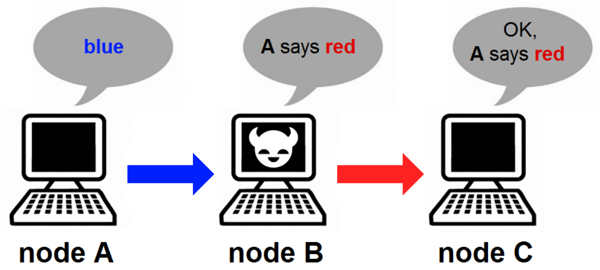
Broadcast in multihop networks

Introduction



Broadcast in multihop networks

Introduction



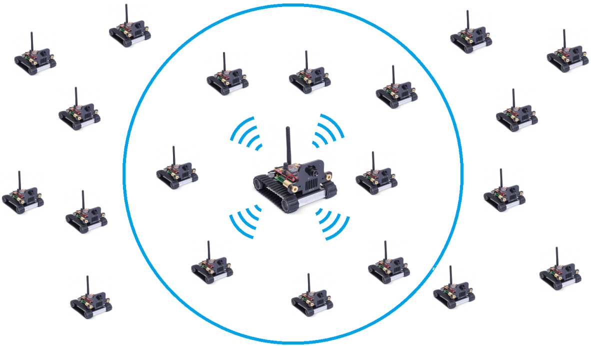
Problem: Byzantine failures

Different approaches

Cryptography

Voting system

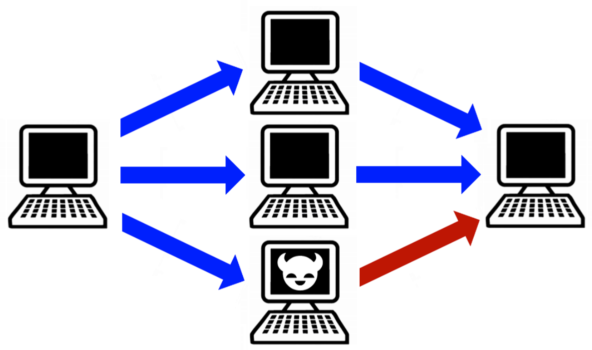
Local voting system



Certified Propagation Algorithm

Requires less than 1 on 12 Byzantine in each neighborhood

Voting on multiple paths



Explorer

Requires $(2k+1)$-connectivity to tolerate k Byzantine nodes

Our approach

Existing approaches

- *All* correct nodes communicate reliably
- Requires *strong* connectivity

Our approach

- *Most* correct nodes communicate reliably
- Enables *weak* connectivity

Preliminaries

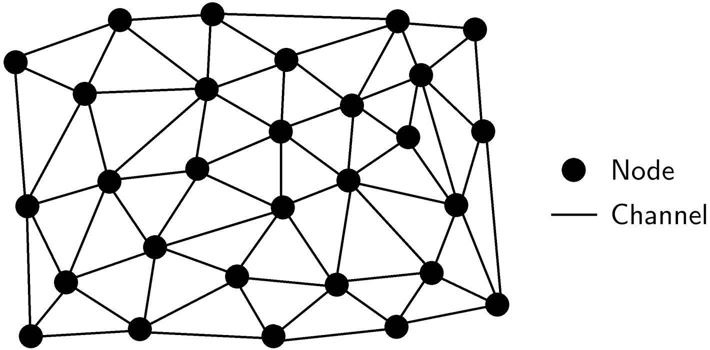
Hypotheses

- Asynchronous message passing
- Local topology knowledge

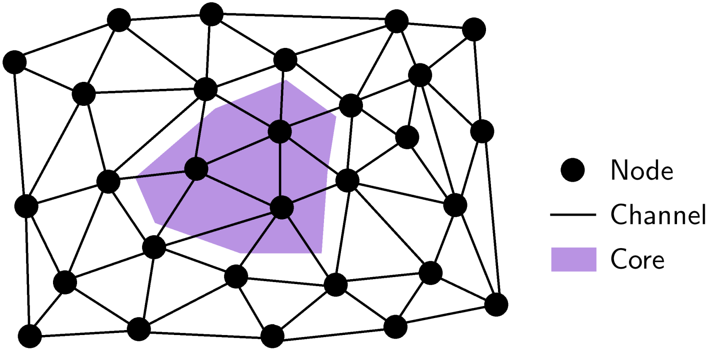
Main idea

- Filtering Byzantine messages with *Control Zones*

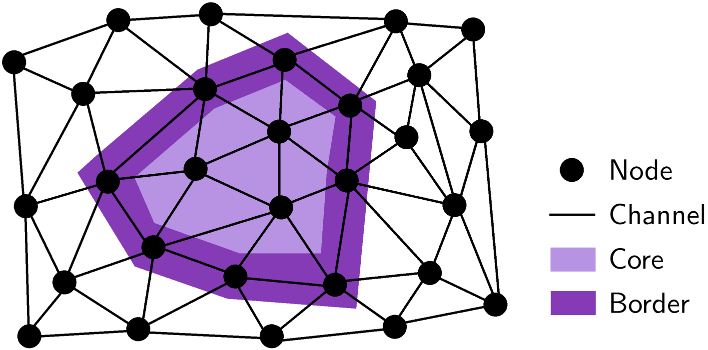
Control Zone



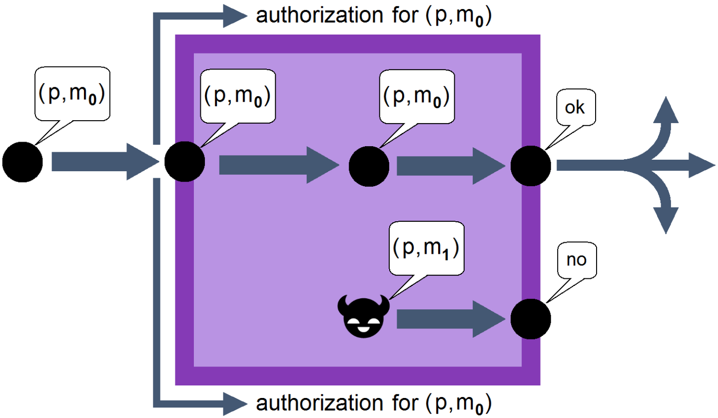
Control Zone



Control Zone



Principle of a Control Zone



Principle of the Protocol

- Defining a large number of Control Zones to limit the diffusion of Byzantine messages
- Protocol described in the paper

Definitions

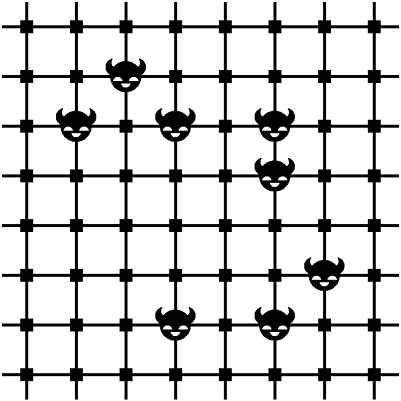
A set of nodes is

- **Safe** if no node accepts false messages
- **Communicating** if all nodes always communicate
- **Reliable** if both **safe** and **communicating**

Objective: For a given set of Byzantine nodes, determine a reliable node set

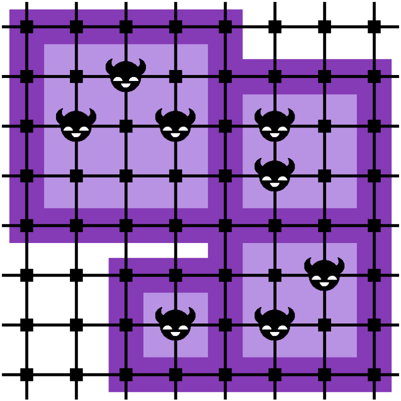
Safe node set

Theorem 1
If all Byzantine nodes are surrounded by a correct border, there exists a safe node set



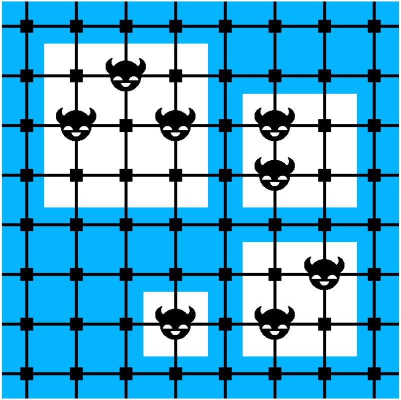
Safe node set

Theorem 1
If all Byzantine nodes are surrounded by a correct border, there exists a safe node set



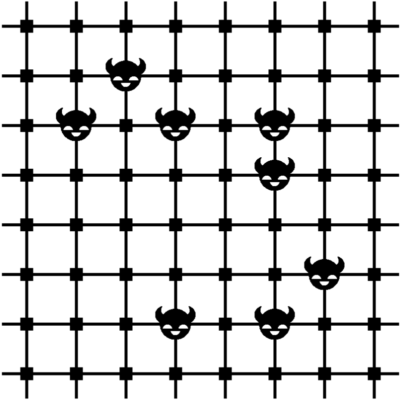
Safe node set

Theorem 1
If all Byzantine nodes are surrounded by a correct border, there exists a safe node set



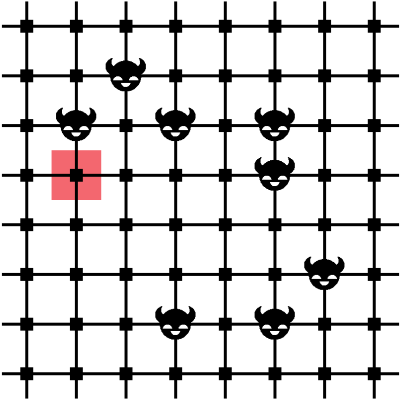
Communicating node set

Theorem 2
A communicating node set can be constructed node by node



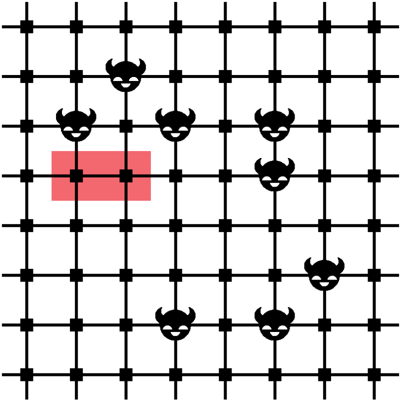
Communicating node set

Theorem 2
A communicating node set can be constructed node by node



Communicating node set

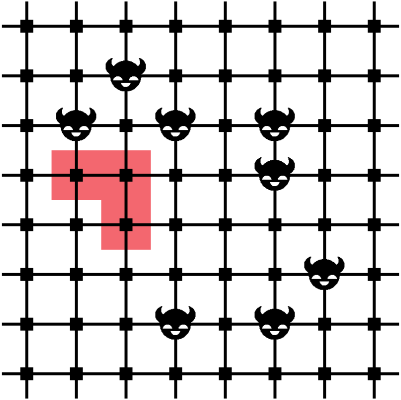
Theorem 2
A communicating node set can be constructed node by node



Communicating node set

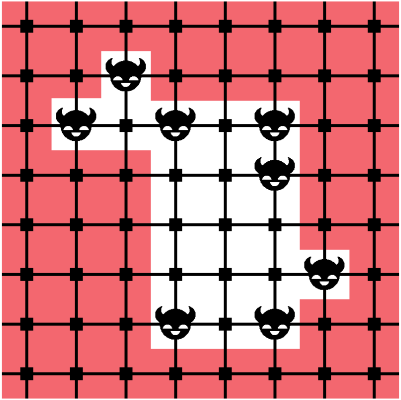
Theorem 2

A communicating node set can be constructed node by node

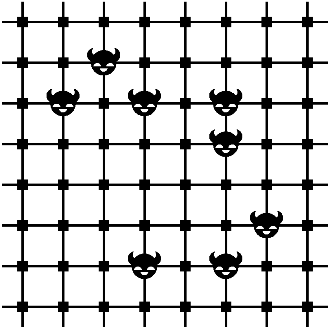


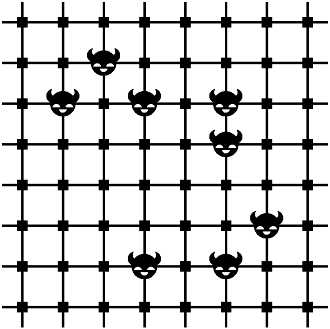
Communicating node set

Theorem 2
A communicating node set can be constructed node by node

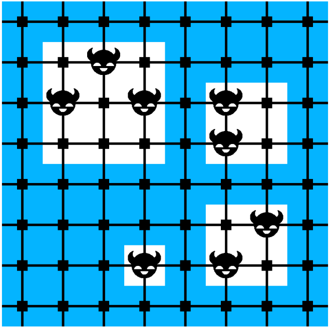


Reliable node set

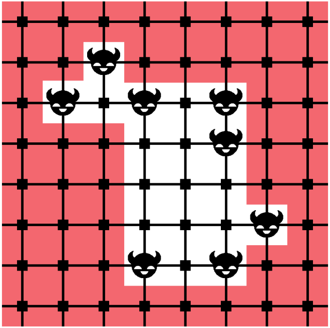




Reliable node set

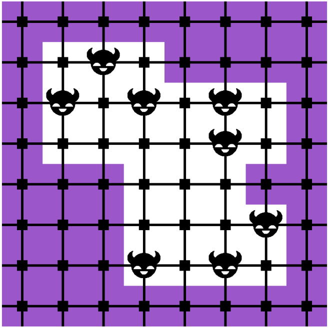


Safe



Communicating

Reliable node set



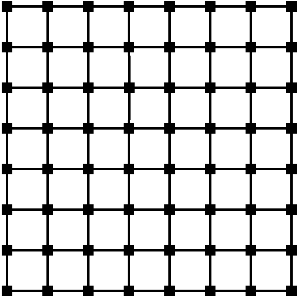
Reliable

Experimental evaluation

To perform the evaluation, we need to:

- Choose a network topology
- Define a set of control zones

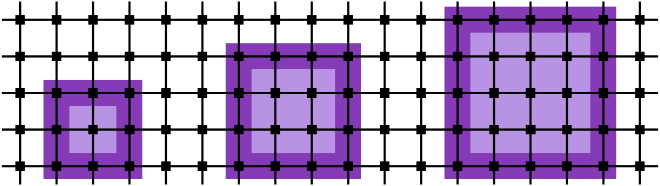
Network topology



100 × 100 grid network

Control zones

Square control zones



Order N: all zones of width $\leq N$

Evaluation

- **Input:** n randomly distributed Byzantine failures
- **Output:** $P(n)$, probability that 2 randomly choosen correct nodes communicate reliably

We evaluate $P(n)$ with a Monte-Carlo method

Simulations

One simulation

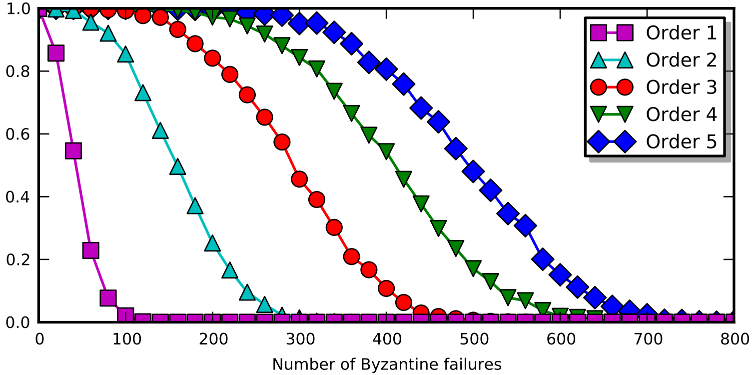
- Choose n Byzantine nodes (at random)
- Determine a reliable node set
- Choose 2 correct nodes (at random)
- If they are in the reliable set, the simulation is a succes

Many simulation

The fraction of successes converges to a lower bound of $P(n)$

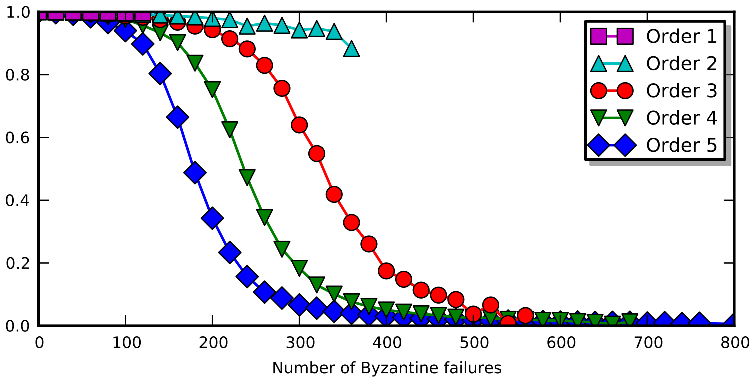
Results

Probability of *existence* of a reliable node set



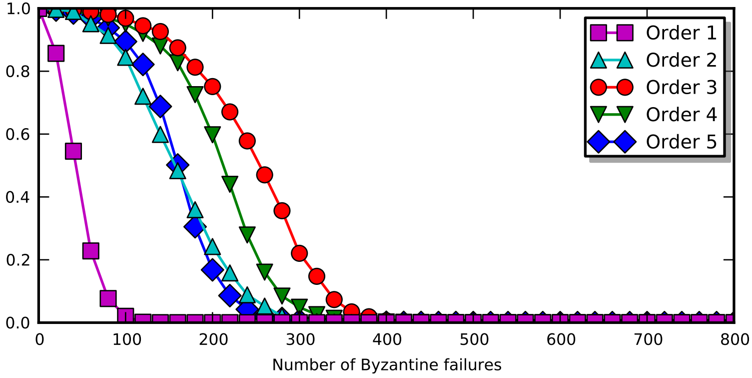
Results

Mean size of the reliable node set, when it exists



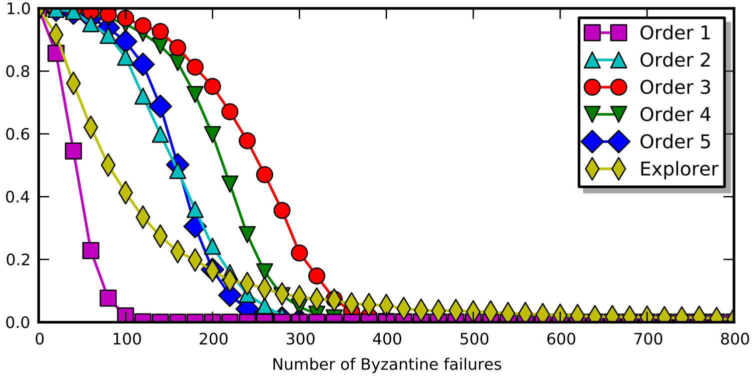
Results

Probability that 2 nodes communicate reliably



Comparison

Probability that 2 nodes communicate reliably



Comparison

For a probability ≥ 0.99, we can tolerate

- 5 Byzantine failures with *Explorer*
- 50 Byzantine failures with our protocol

Conclusion

- Our approach enables Byzantine resilience in sparse networks
- Open problems:
  - Defining optimal control zones in *any* network
  - Making the approach *scalable*

Questions ?