Paper presentation:
Limiting Byzantine Influence in Multihop Asynchronous Networks

Author:
Ben Ayad, Mohamed Ayoub

Supervisor:
Maurer, Alexandre

Outline

- **General context and problematic**
- **Related work**
- **Contribution**
  - The protocol
  - The guarantees
- **Evaluation**
  - Methodology
  - Testing topology
  - Results
- **Conclusion and perspectives**

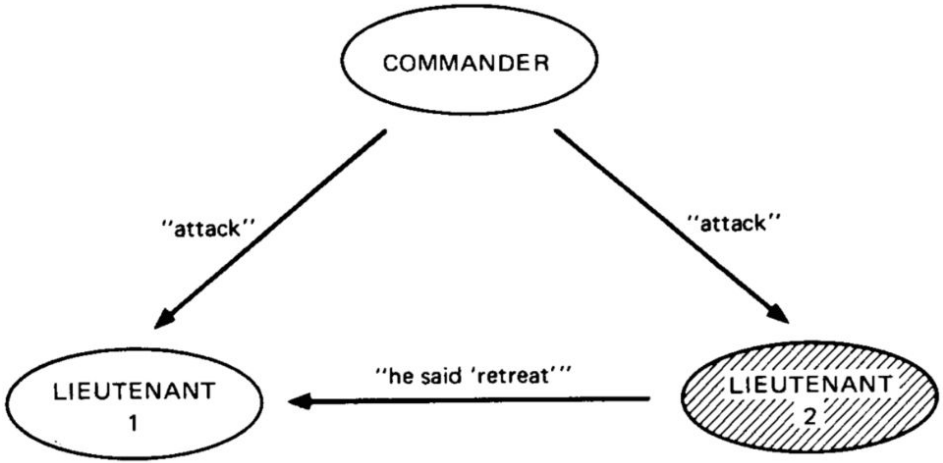
General Context and problematic

Modes of failures:

- Crash failure
- Performance failure (e.g Omission failure)
- *Byzantine Failures*

General Context and problematic

Byzantine Failures:



General Context and problematic

Why Byzantine Failures are dangerous.

Related Work

There are mainly two types of approaches to deal with this problem:

- Cryptographic operations
- Connectivity based approaches

Related Work - Cryptographic based

- Enabling nodes to use cryptographic operations

Cons:

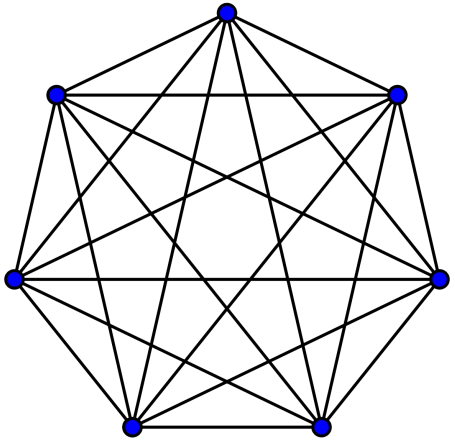
- High ressources.
- Trusted infrastructure.

Related Work - High connectivity based

- The graph needs to be highly connected (e.g 2k+1 connected)
- Graph topology knowledge

Cons:

- Not practical
- Heavy constraints



Related Work - Key points recap

Other methods:

- Cryptographic based
- Relies on high connectivity && Byzantine proportions assumptions

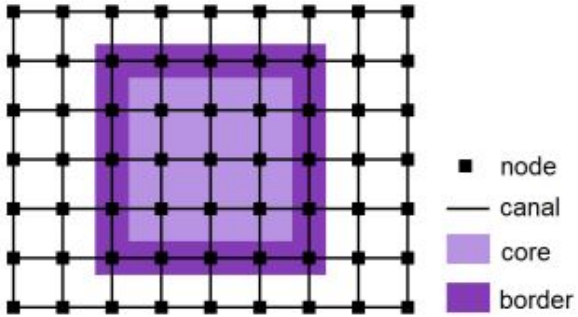
The Paper's method:

- Does not assume a trusted infrastructure
- Supports low-connectivity networks

Contribution - The protocol

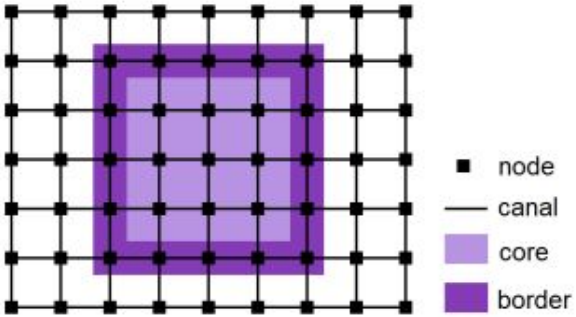
The protocol relies on the notion of **control zone** and **authorizations**:

- A **control zone** is acts like a filter.
- Each message leaving the control zone should be **authorized**.



Contribution - The protocol

Intuition ?



Contribution - The protocol

Intuition ?

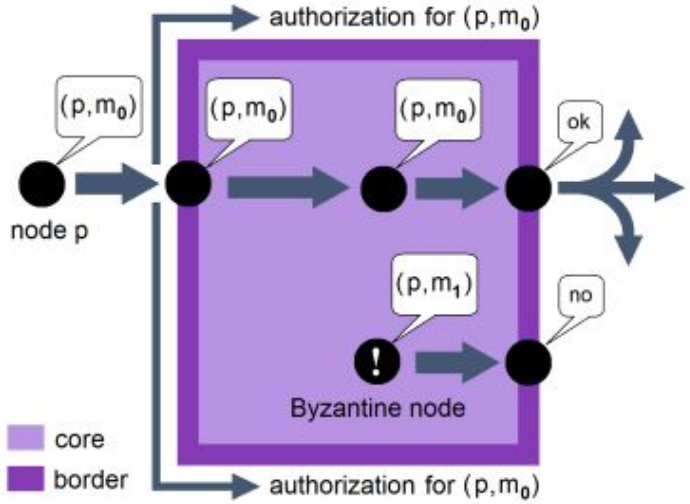
Contribution - The protocol

Intuition ?

Contribution - The protocol

Principal:

- Defining a large number of Control Zones.



Hypothesis:

- All sent messages are received
- Knowledge of local topology
- “Most”

Contribution - Guarantees

A set of nodes is **Reliable if:**

- **Safe:** no node accepts false messages
- **Communicating:** all its correct nodes always communicate (all correct messages are received)

Therefore the objective is to **determine** a **reliable set of nodes**.

Contribution - Guarantees

Three theorems are presented and proven in the paper:

1. Determining safe nodes
2. Constructing a communicating node set
3. A safe and communicating set achieved a reliable communication

Guarantees - Theorem 1

If there exists a set of control zones Z verifying:

1. The node sets Cores(Z) and Borders(Z) are disjoint.
2. All Byzantine nodes are in Cores(Z).

Then any node **out of Cores** is **safe**

Guarantees - Theorem 2

Incrementally constructing a communicating node set.

If S is a communicating node set and v is a correct node verifying:

- v has a neighbor u ∈ S
- Let Z be the set of control zones z ∈ Ctr, such that **(u,v) ∈ (core(z),border(z))**.
  - Then ∀ z ∈ Z, there exists a correct path on **border(z)** between v and a node w ∈ S.

Then S ∪ {v} is also communicating.

Guarantees - Theorem 3

The **intersection** of a **safe node** set and another **communicating node set** is a **reliable set.**

Evaluation - Methodology

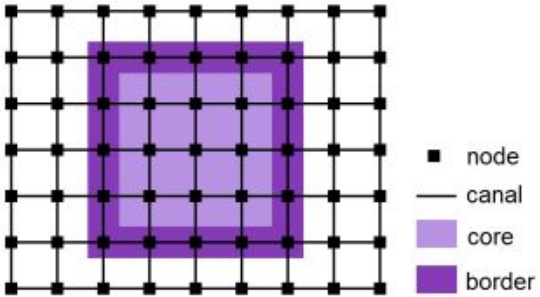
To **evaluate** a network, we need to **define**:

- The **network topology**
- The **sets of control zones**

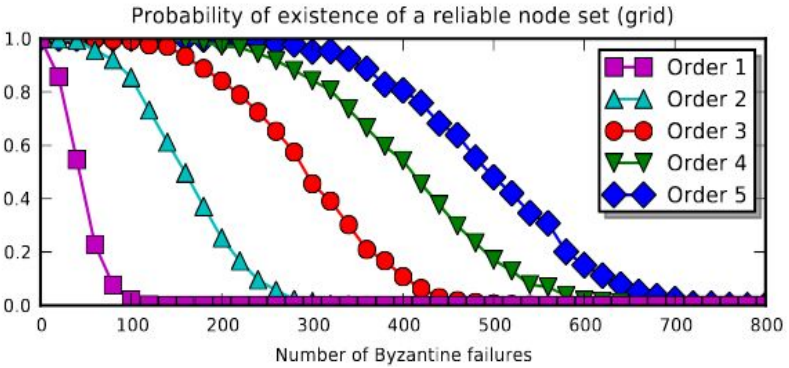
Evaluation - Testing topology

For testing purposes, they chose to run simulations on a **grid/torus** structure.

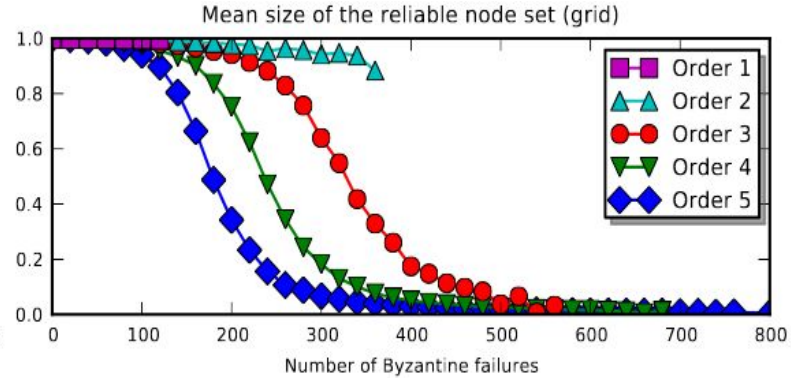
- Grid network ?
- Order of the protocol ?



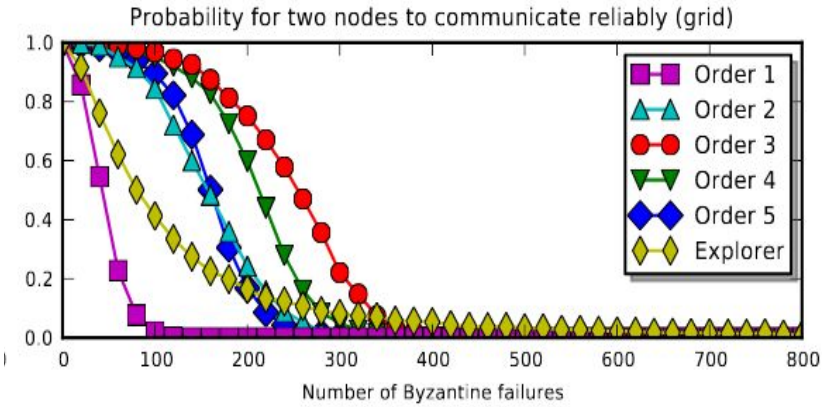
Evaluation - Results



Evaluation - Results



Evaluation - Results



Conclusion and perspectives

The protocol tolerates **reliable communication** between **most correct nodes** in the presence of Byzantine nodes in **low-connectivity** networks.

Open questions:

- Designing optimal sets of control zones

Thank you very much.