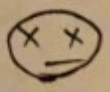
B1

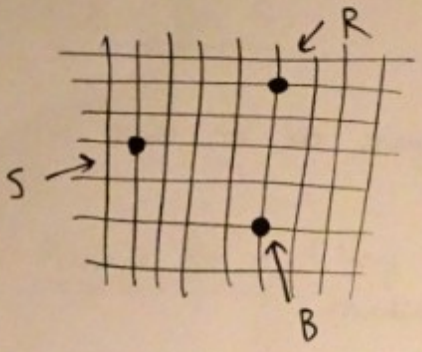
1 BYZANTINE FAILURES

CRASH failures : "dead" node



BYZANTINE failures : "evil" node

ILLUSTRATION :
BROADCAST ALGORITHM

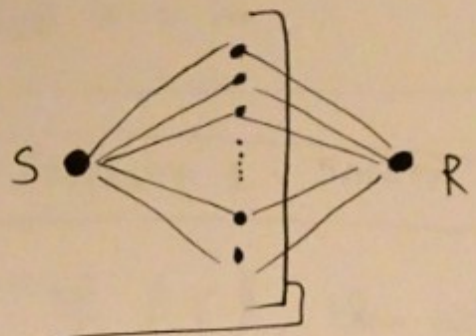


S : sender
R : receiver
B : BYZANTINE node

- S broadcasts (S, m)
- B broadcasts (S, m')
  ($m' \neq m$)
- R receives (S, m)
  AND (S, m')

→ What is the message of S ? m or m' ??

2 SIMPLE EXAMPLE : "n intermediary nodes"



↳ n intermediary nodes

- S and R are correct (non-Byzantine)
- interm. nodes can be Byzantine
  → f = ~~max~~ max. number of Byzantine nodes
- S wants to send m (m ↑ message) to R

ALGO

Preliminaries :

Define k :
- if n even : $k = n/2$
- if n odd : $k = (n-1)/2$

B2 ($k+1$ = smallest number to have a majority among n)

- R has a set Ω (memory) and a variable x (initially $x = 0$)
- GOAL : to have $x = m$

ALGO for S :

- send m to neighbors

ALGO for p (any intermediary node) :

- when receives m ~~for~~ from p : send m to R

ALGO for R :

- when receives m from p : add (p, m) to Ω ($\Omega := \Omega \cup \{(p, m)\}$)
- when there exists $k+1$ nodes $\{p_1, \dots, p_{k+1}\}$ such that ... $\forall i \in \{1, \dots, k+1\}$, $(p_i, m) \in \Omega$:

  $x := m$

PROPERTY 1 : SAFETY

"If $f \leq k$, then either $x = 0$ or $x = m$"

(f ↑ nb. of Byz. nodes)

PROOF :

proof by contradiction

[SEEK]

suppose the opposite :

$x = m'$ ($m' \neq m$)

→ ATTA, there exists $k+1$ nodes $\{p_1, \dots, p_{k+1}\}$ such that, $\forall i \in \{1, \dots, k+1\}$, $(p_i, m') \in \Omega$

B3 for each node p_i :

ATTA : 2 possibilities :
(1) p_i received m' from S
(2) p_i is Byzantine

→ case (1) impossible

→ $\{p_1, \dots, p_{k+1}\}$ are Byzantine

→ we have $k+1$ Byzantine nodes : contradiction

(→ the result)

ATTA, p_i rec. m from S

→ p_i sends m to R

→ R rec. m from p_i and adds (p_i, m) to Ω

Eventually, we have :
$\forall i \in \{1, \dots, k+1\}$, $(p_i, m) \in \Omega$

→ ATTA, $x = m$

PROP. 1+2 :
initially, $x = 0$,
and eventually, $x = m$
(we never have $x = m'$)

PROPERTY 2 : LIVENESS

"If $f \leq k$, we eventually have $x = m$"

PROOF:

Let $\{p_1, \dots, p_{k+1}\}$ be $k+1$ CORRECT (non-Byzantine) interm. nodes.

For each node p_i :

PROPERTY 3 : OPTIMALITY

"If $f \geq k+1$, it is impossible to ensure the safety property"

PROOF:

B4

let $\{p_1, \ldots, p_{k+1}\}$ be $k+1$ Byzantine interm. nodes.

possible situation:

$\forall i \in \{1, \ldots, k+1\}$,

p_i sends (p_i, m') to R

$m' \neq m$

→ ATTA, $x = m'$

(no safety)

CONCLUSION :

we can tolerate at most k Byz. failures