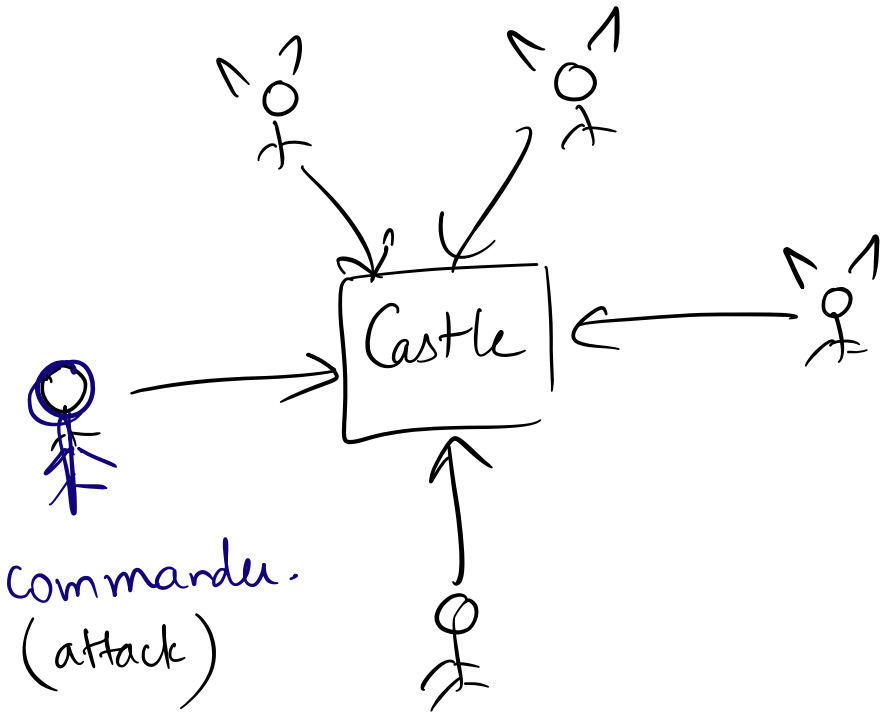
Byzantine Broadcast

n parties, t corrupt / malicious / Byzantine.



Agreement: No two honest generals take different actions.

Termination: Every honest general eventually either attacks or retreats.

Validity: If commander is honest, then output commander's order.
honest parties.

Dolev-Strong Protocol: (1983)

Intuition:

- If some honest party receives a value (txn command), share it with all honest parties.
- Eventually, one honest party learns x

$$\Downarrow$$

all honest parties learn x.

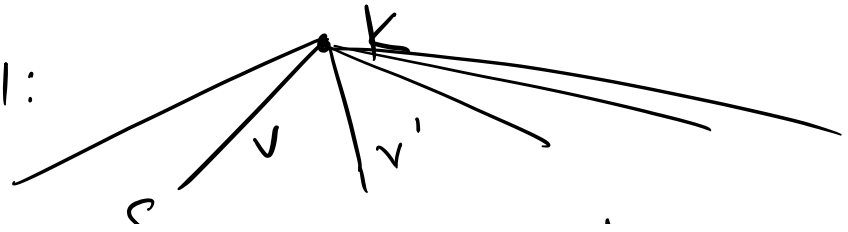
Round 1: Commander (sender) sends value v to all parties.

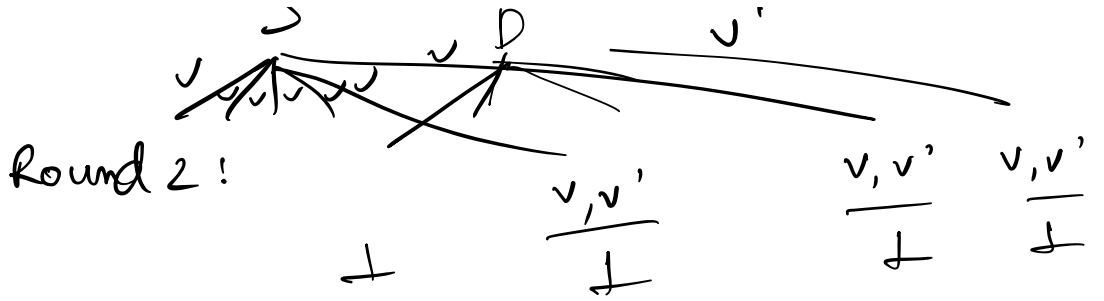
Round 2: If I receive a value from the commander, then I send it to all parties.

Commit: If I receive exactly one value v, then output v.

output $\perp$.

Round 1:

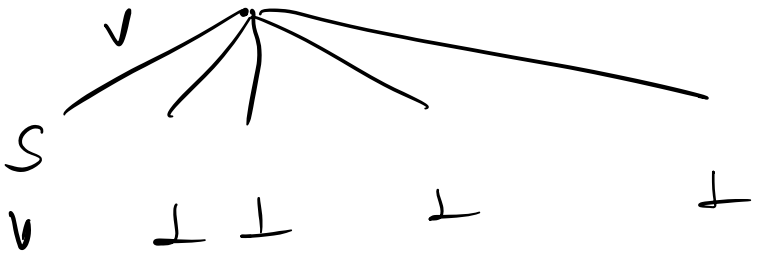




Attack 2 :

Round 1 : .K

Round 2 :

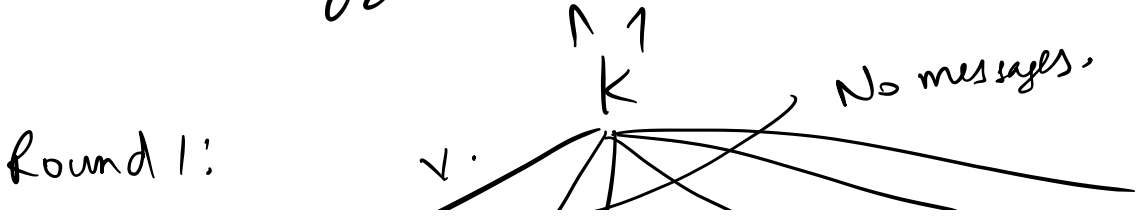


Solution :

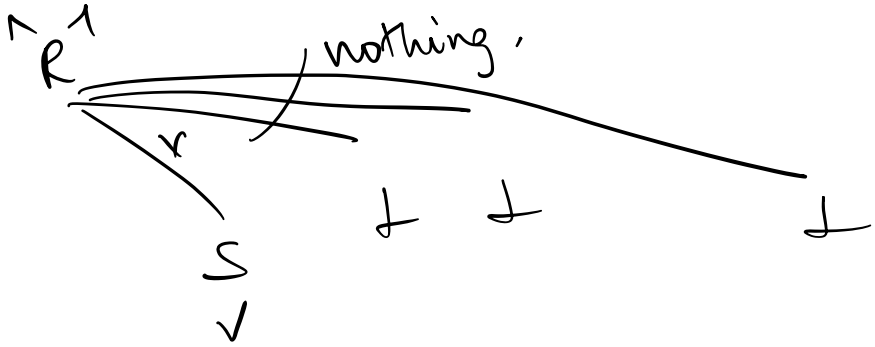
Round 2 : Do not consider commander's value.

If ≤ 1 Byzantine :

≥ 2 Byzantine parties.



Round 2:



We can tolerate Byzantine faults.