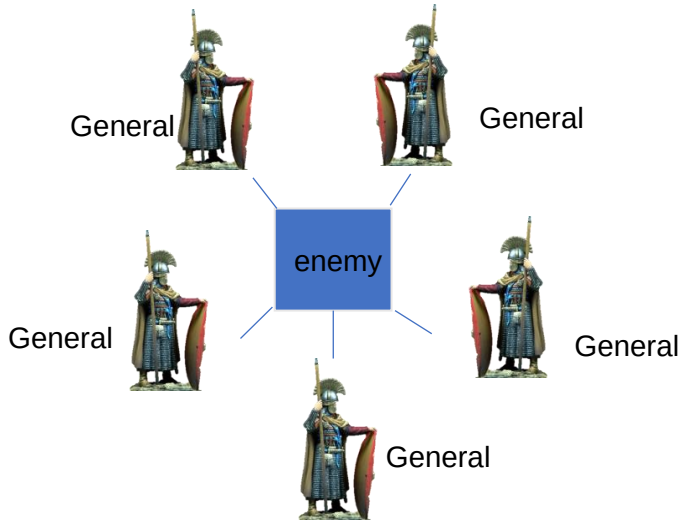


Generals must agree on a decision: attack /retrait

Each general i sends its opinion , v(i), to the other generals

Default vale: retrait

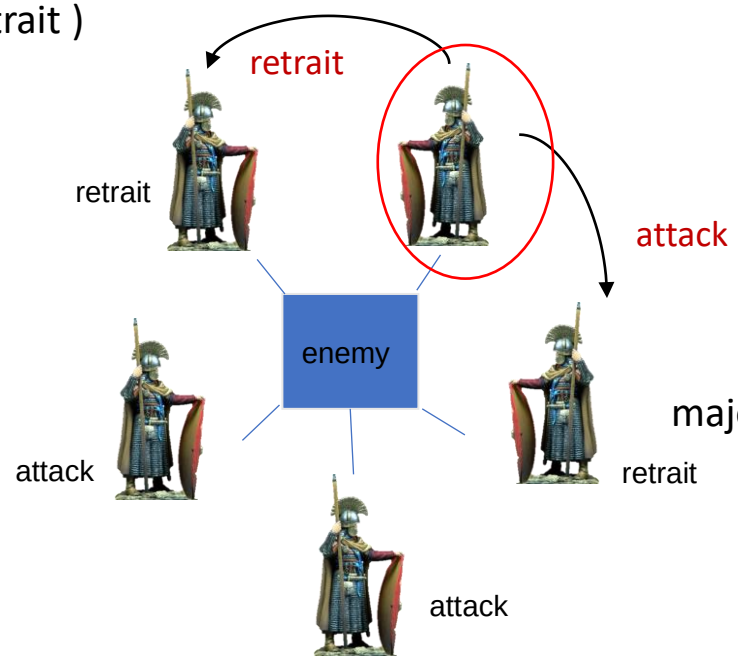
Eah general obtains the final decision by majority function:

majority(v(1), …., v(n))

If no majority: default value

In case of traitors: a general can lie and sends different opinions

majority(retrait, attack, attack, retrait, retrait)
==> retrait



majority(retrait, attack, attack, retrait, attack)
==> attack

Loyal generals can take different decisions!

Majority vote is applied to different sets of value !!!!!

Generals should agree on the value sent by the traitor before applying majority

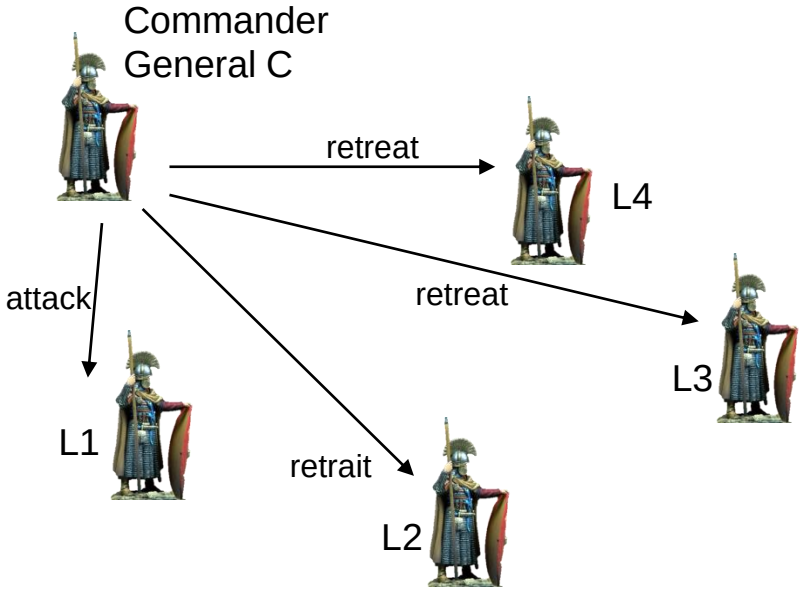
Problem: Find the consensus on the value sent by a general

Find the consensus on the value sent by a general

Oral message algorithm

1. Commander sends a message
2. each Lieutenant resends what he has received by the commander
3. Each Lieutenant apply majority function

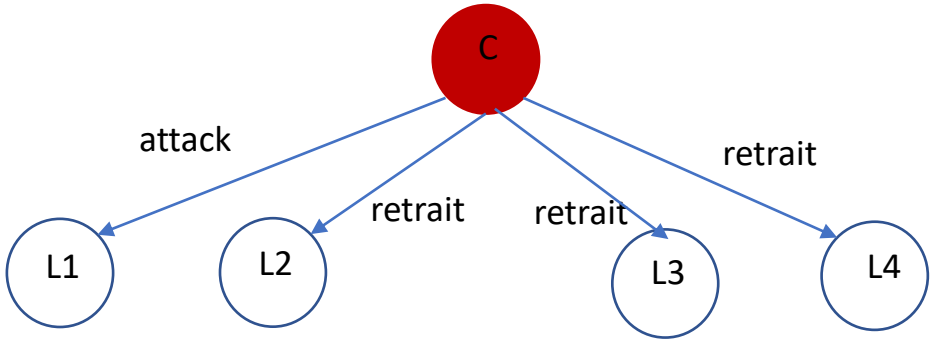
   Li: majority(v1, v2, v3, v4)



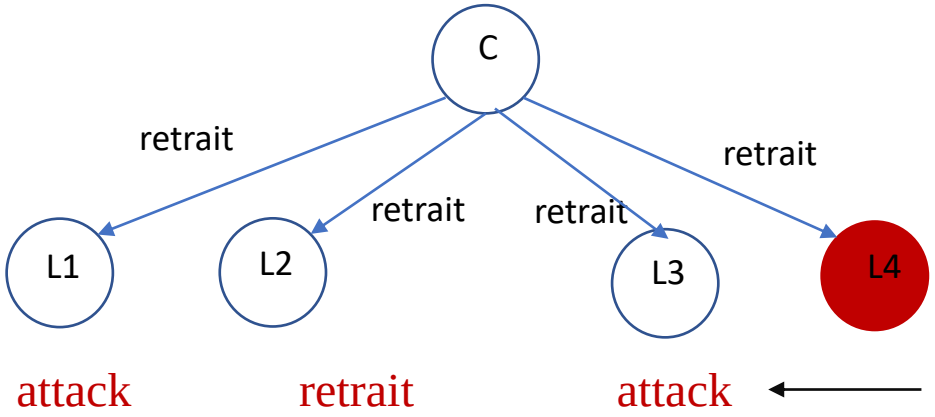
Consensus reached in case of 1 traitor and n>=4 generals

Traitor: commanding general or lieutenant

Examples

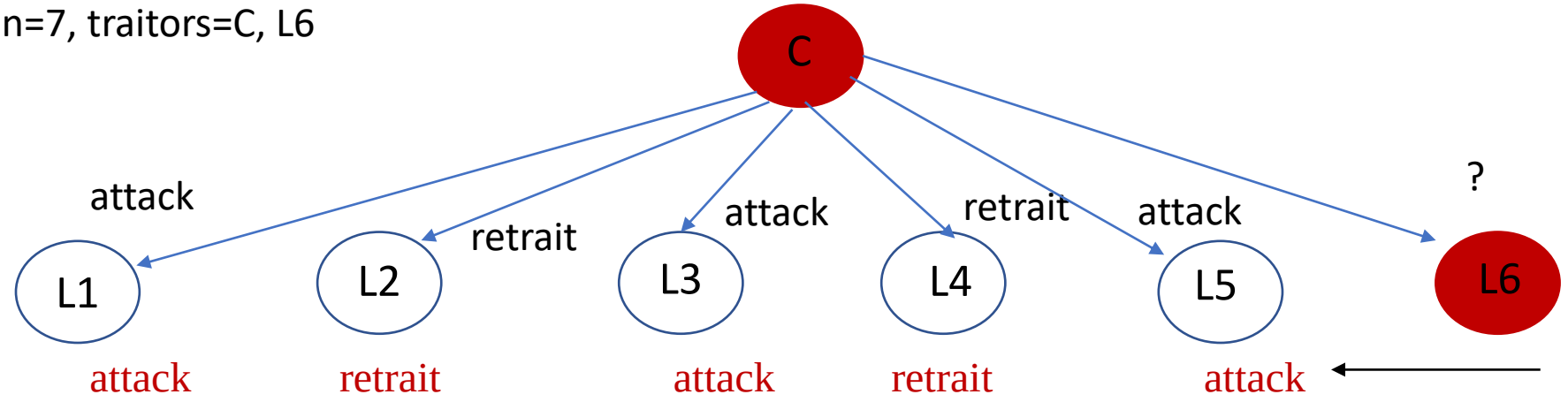


L1: majority(attack, retrait, retrait, retrait)



L1: majority(retrait, retrait, retrait, attack)

With more traitors?
2 traitors
Scenario: m=2, n=7, traitors=C, L6



1 round

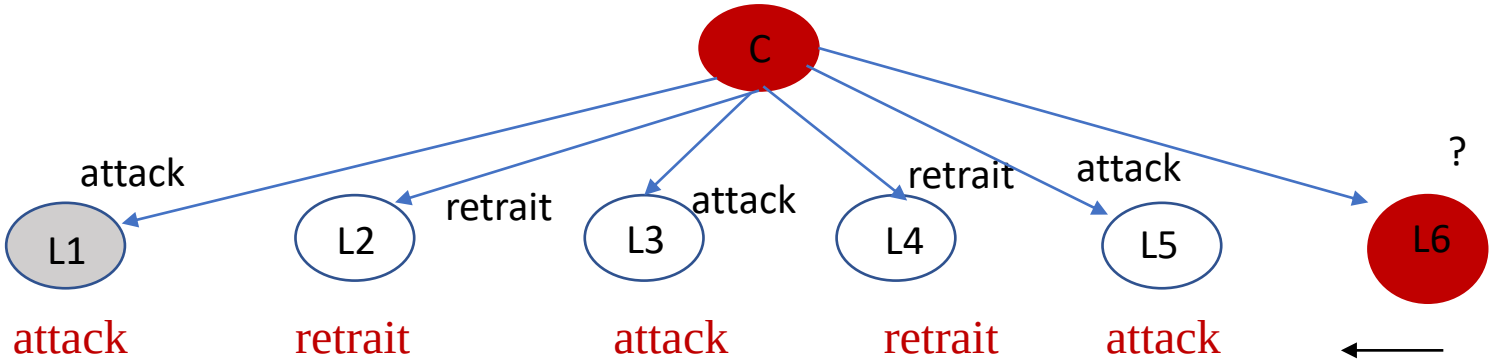
L1: majority(attack,retrait,attack,retrait,attack,attack) ==> attack
L2: majority(attack,retrait,attack,retrait,attack,retrait) ==> retreat
L3: majority(attack,retrait,attack,retrait,attack,attack) ==> attack
L4: majority(attack,retrait,attack,retrait,attack,retrait) ==> retreat
L5: majority(attack,retrait,attack,retrait,attack,attack) ==> attack

Loyal lieutenants do not choose the same action !!!

Important: what the other tell they have received by L6 !!!

Scenario: m=2, n=7, traitors=C, L6

Additional round:
Majority: what received by Li and what the other tell they have received by Li



Node Li

Round 0: C attack
Round 1: L2 retrait , L3 attack, L4 retrait, L5 attack , L6 attack (doesn't know 6 is traitor)

Round 2:

L2 { L3 attack, L4 retrait, L5 attack , L6 retrait}
L3 {L2 retrait, L4 retrait, L5 attack, L6 attack}
L4 {L2 retrait, L3 attack, L5 attack, L6 retrait}
L5 {L2 retrait, L3 attack, L4 retrait, L6 attack}
L6 {L2 ? , L3 ? , L4 ? , L5 ? }

majority majority majority majority majority

majority(attack, retrait, attack, retrait, attack, attack) ==> attack

all see same messages from L1, L2, L3, L4, and L5

L1, L2, L3, L4, L5 decide attack