

## Algorithm Overview

The Byzantine Generals Problem addresses achieving consensus in distributed systems with potential traitors. The solution requires:

1. Oral Messages: No cryptographic signatures; receivers must trust message content
2.  $T+1$  Rounds: For  $T$  traitors, need  $T+1$  communication rounds
3.  $3T+1$  Nodes: Minimum  $3T+1$  generals to tolerate  $T$  traitors (Byzantine Resilience)

## Key Properties:

1. Safety: All loyal generals decide same action
2. Liveness: Eventually reach decision
3. Fault Tolerance: Works when  $T < N/3$

## Implementation Details

1. Message Redundancy:  $T+1$  rounds ensure loyal generals receive original order through at least one honest path, multiple copies to identify inconsistencies
2. Traitor Detection: Honest nodes compare messages across rounds and identify conflicting orders from same sender. They use majority voting to filter outliers
3. Threshold Enforcement: With  $N \geq 3T+1$ , honest majority ( $2T+1$ ) can outvote traitors. This prevents traitors from creating fake majority.