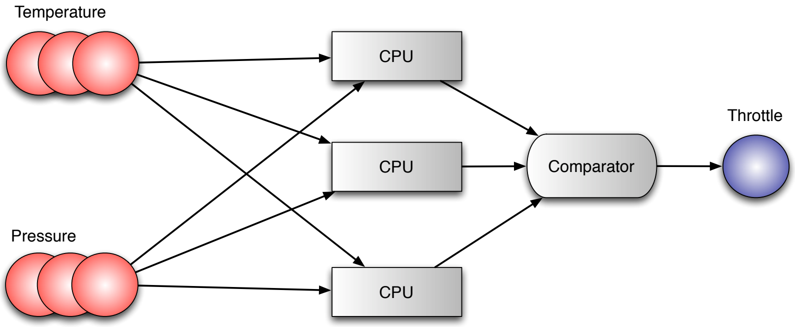
Introduction to Robust Protocols

Sébastien Tixeuil
Sebastien.Tixeuil@lip6.fr

Approach

- *Faults* and *attacks* occur in the network
- The network's user must *not* notice something wrong happened
- A *small* number of faulty components
- **Masking** approach to fault/attack tolerance

Principle



Problems

- Replicated input sensors may not give the same data
- Faulty input sensor or processor may not fail gracefully
- The system might not be tolerant to software bugs

The Island of Liers and Truth-tellers

- An island is populated by two tribes
  - Members of one tribe **consistently lie**
  - Members of the other tribe **always tell the truth**
  - Tribe members can recognize one another, but an external observer can't

Puzzle 1

- You run into a man and ask him if he is a truth-teller, but fail to hear the answer
- You inquire: "Did you say you are a truth-teller?"
- He responds: "No, I did not."
- To which tribe does the man belong ?

Puzzle II

- You meet a woman on the island.
- What single question can you ask her to determine whether she is a liar or a truth-teller?

Puzzle III

- You meet two people *A* and B on the island
- *A* says: "Both of us are from the liar tribe."
- Which tribe is *A* from ?
- What about *B* ?

Puzzle IV

- You meet two people, *C* and *D* on the island.
- *C* says: "Exactly one of us is from the liars tribe."
- Which tribe is *D* from ?

Puzzle V

- You meet two people *E* and *F* on the island
- *E* says: "It is not the case that both of us are from truth-tellers tribe."
- Which tribe is *E* from?
- What about *F*?

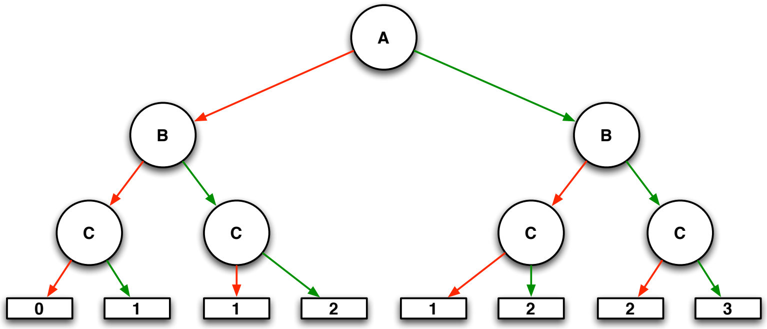
Puzzle VI

- You meet two people *G* and *H* on the island
- *G* says: "We are from different tribes."
- *H* says: "*G* is from the liars tribe."
- Which tribes are *G* and *H* from ?

Puzzle VII

- You meet three people *A*, *B*, and *C*
- You ask *A*: "how many among you are truth-tellers?", but don't hear the answer
- You ask *B*: "What did *A* say?", hear "one."
- *C* says: "*B* is a liar."
- Which tribes are *B* and *C* from?

Puzzle VII



The Island of Selective Liars

- Inhabitants lie consistently on Tuesdays, Thursdays, and Saturdays, and tell the through on the remaining days
- You ask: “What is today?” ”Tomorrow?”
- Responses: “Saturday.”, “Wednesday.”
- What is the current day ?

The Island of Random Liars

- A new Island has three tribes
  - truth-tellers
  - consistent liars
  - randomly lie or tell the truth
- How to identify three representants of each tribe with only three yes/no questions?

Byzantine Generals

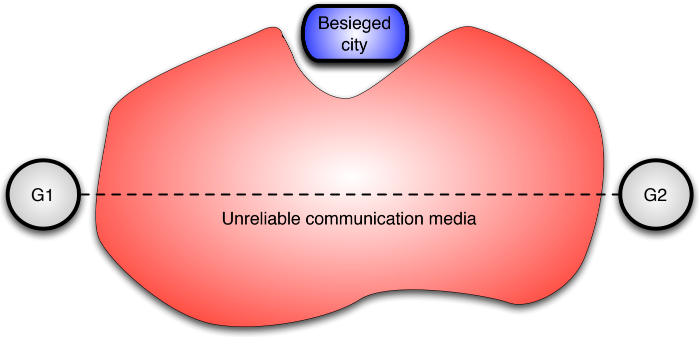
Settings

- Byzantine generals are camping outside an enemy city
- Generals can communicate by sending messengers
- Generals must decide upon common plan of action
- Some of the Generals can be traitors

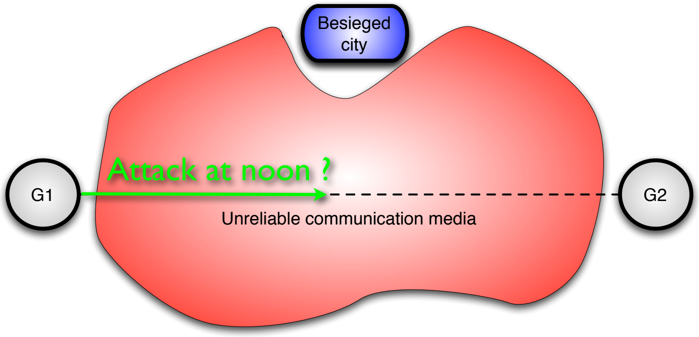
Goal

- All loyal generals decide upon the same plan of action
- A small number of traitors cannot cause the loyal generals to adopt a bad plan

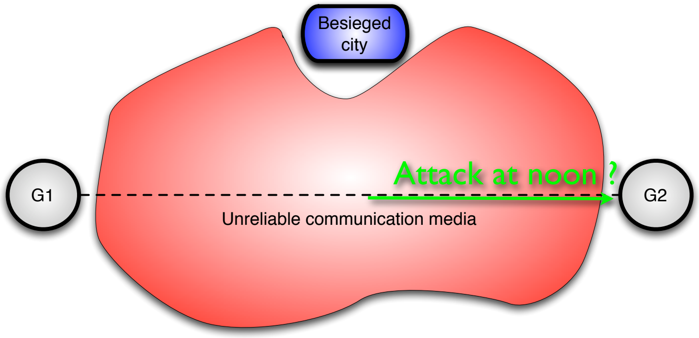
Two Generals Paradox



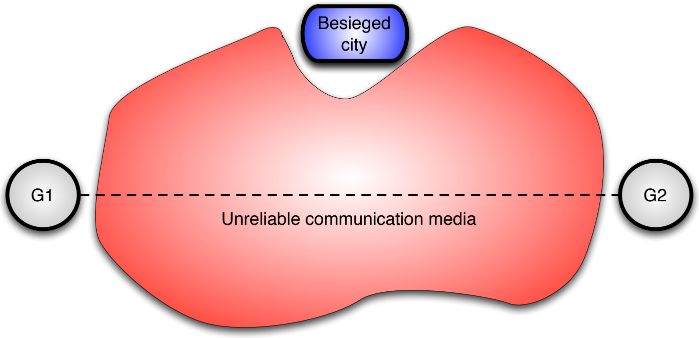
Two Generals Paradox



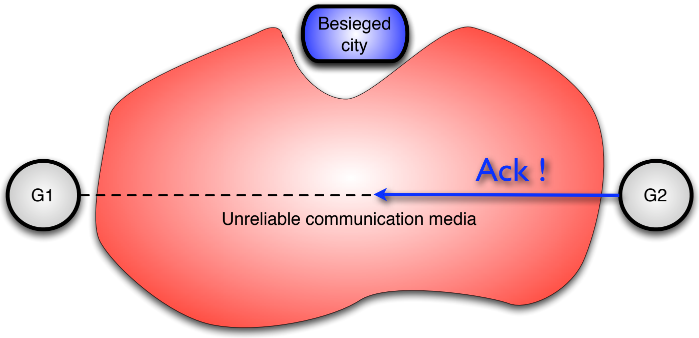
Two Generals Paradox



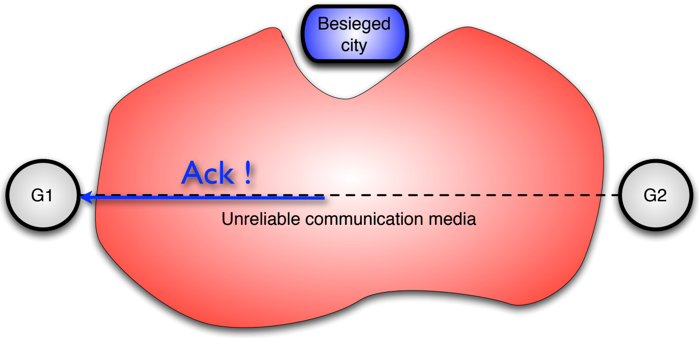
Two Generals Paradox



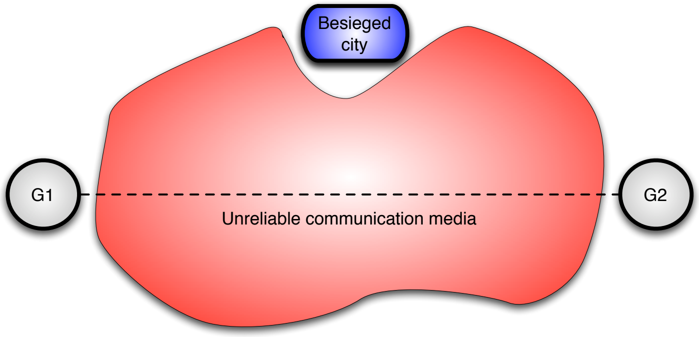
Two Generals Paradox



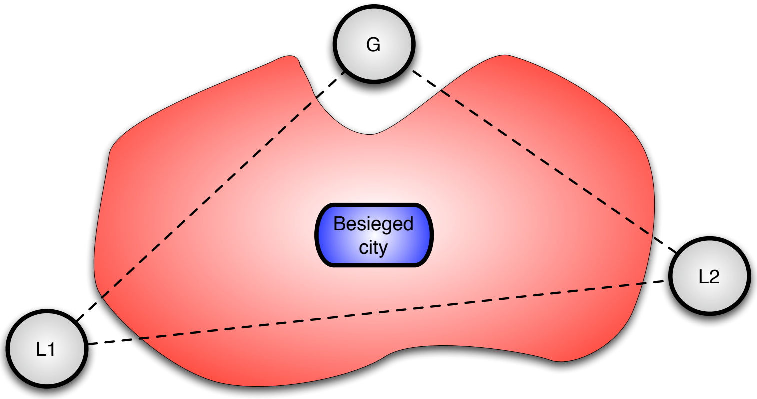
Two Generals Paradox



Two Generals Paradox



The Byzantine Generals Problem



The (simple) Byzantine Generals Problem

- Generals lead *n* divisions of the Byzantine army
- The divisions communicate via reliable messengers
- The generals must **agree** on a plan (“attack” or “retreat”) even if some of them are **killed** by enemy spies

Oral Model

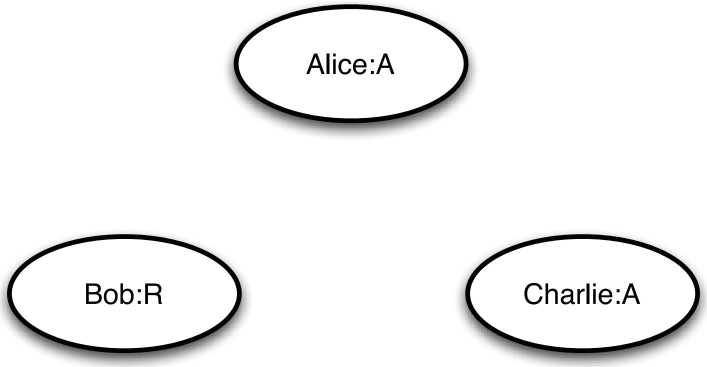
- **A1**: Every message that is sent is delivered correctly
- **A2**: The receiver of a message knows who sent it
- **A3**: The absence of a message can be detected

Solution?

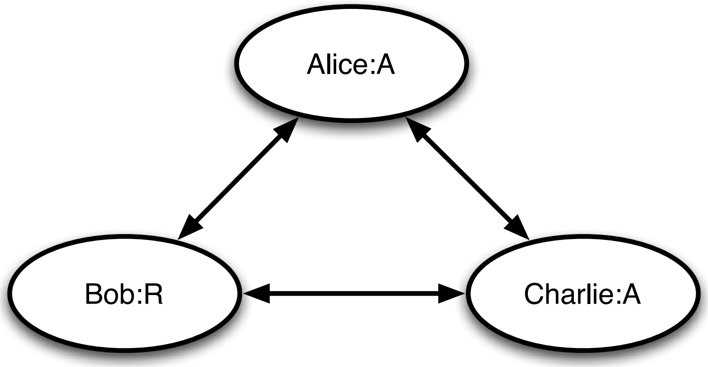
plan: **array of** {A,R}; finalPlan: {A,R}

```
1: plan[myID] := ChooseAorR()
2: for all other G send(G, myID, plan[myID])
3: for all other G receive(G, plan[G])
4: finalPlan := majority(plan)
```

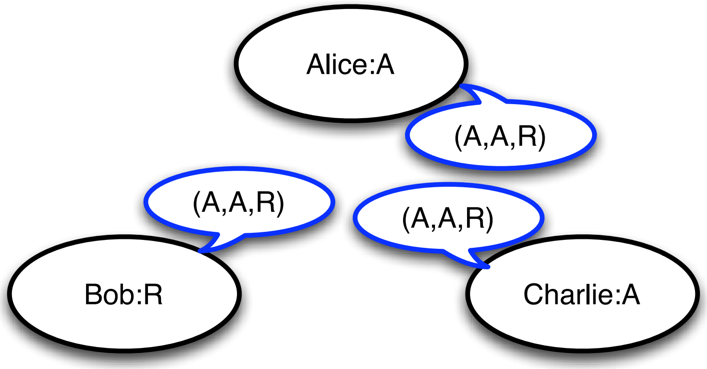
Reliable Networks



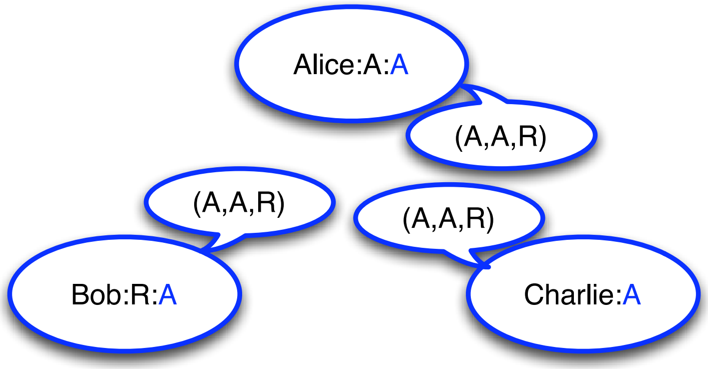
Reliable Networks



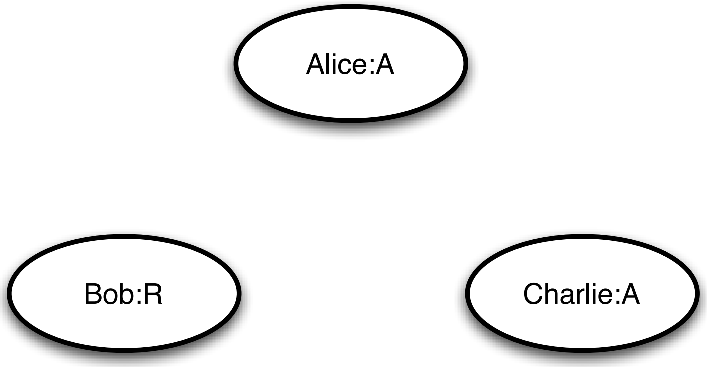
Reliable Networks



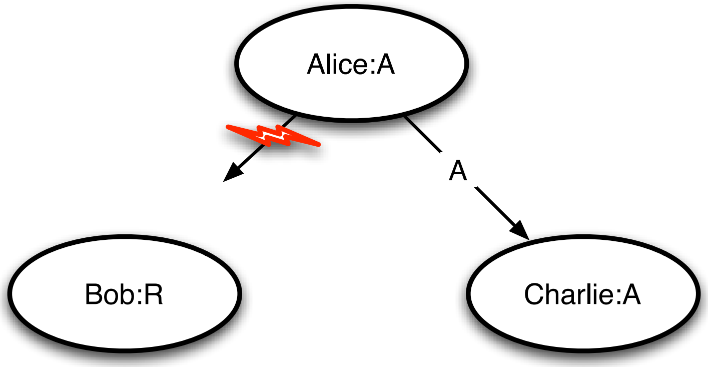
Reliable Networks



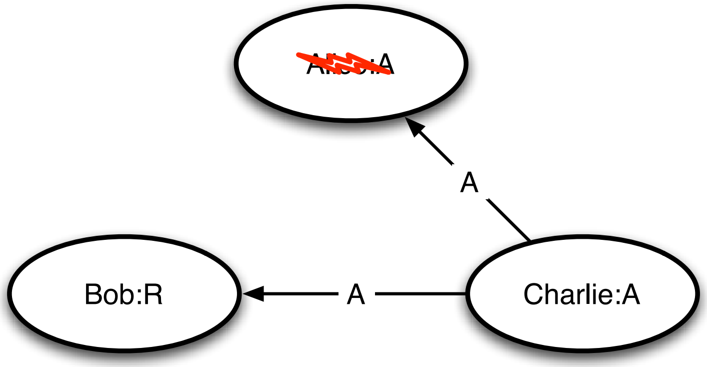
Crashing Networks



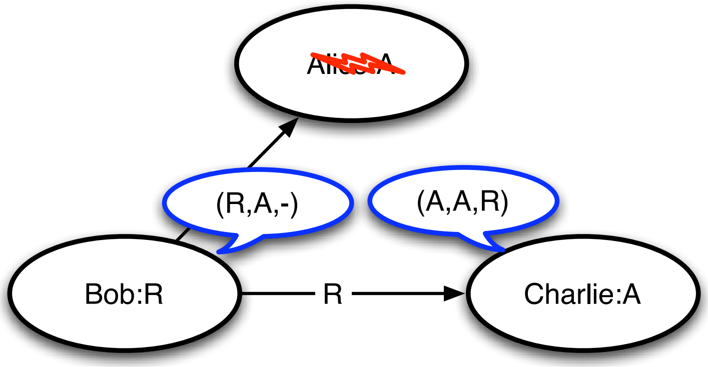
Crashing Networks



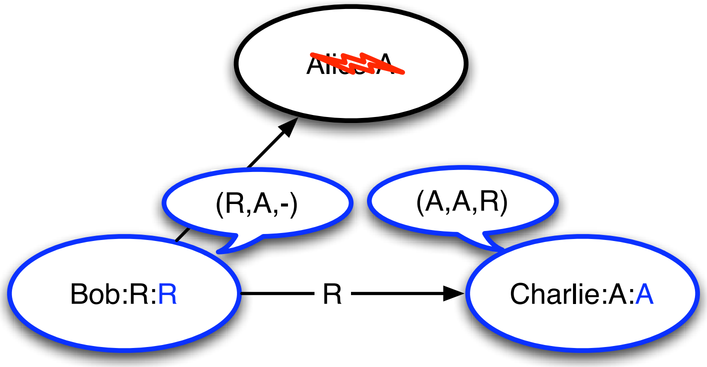
Crashing Networks



Crashing Networks



Crashing Networks



The Byzantine Generals Problem

- A general and *n-1* lieutenants lead n divisions of the Byzantine army
- The divisions communicate via messengers that can be captured or delayed
- The generals must **agree** on a plan ("attack" or "retreat") even if some of them are **traitors** that want to prevent agreement

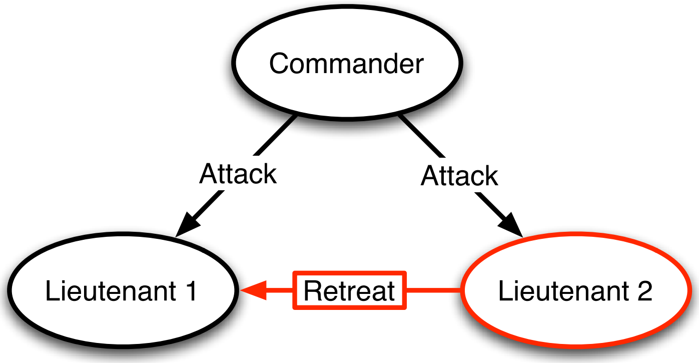
The Byzantine Generals Problem

- A commanding general must sent an order to his n-1 lieutenants generals such that
  - **IC1**: all loyal lieutenants obey the same order
  - **IC2**: if the commanding general is loyal, then every loyal lieutenant obeys the order he sends

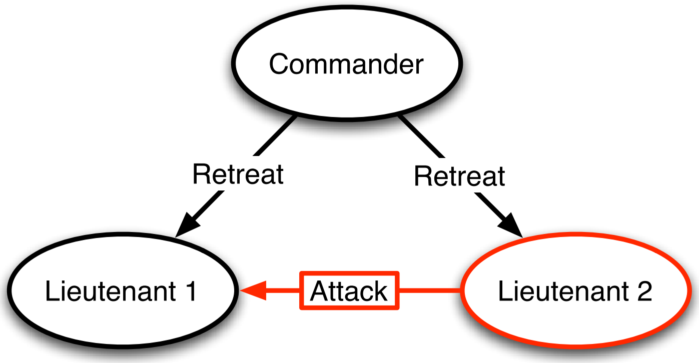
Oral Model

- **A1**: Every message that is sent is delivered correctly
- **A2**:The receiver of a message knows who sent it
- **A3**:The absence of a message can be detected

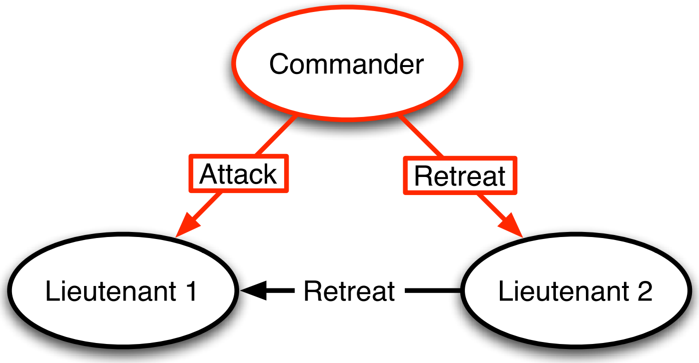
3k+1 nodes are necessary (oral model)



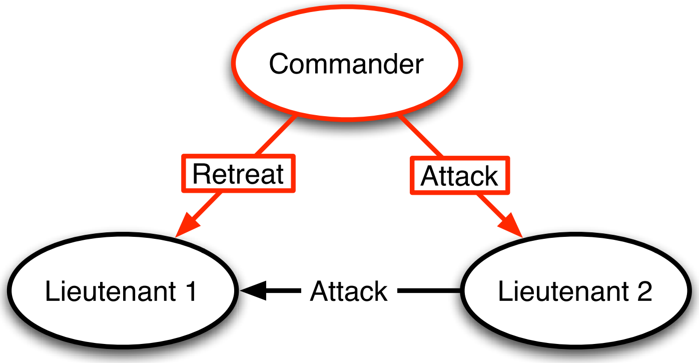
3k+1 nodes are necessary (oral model)



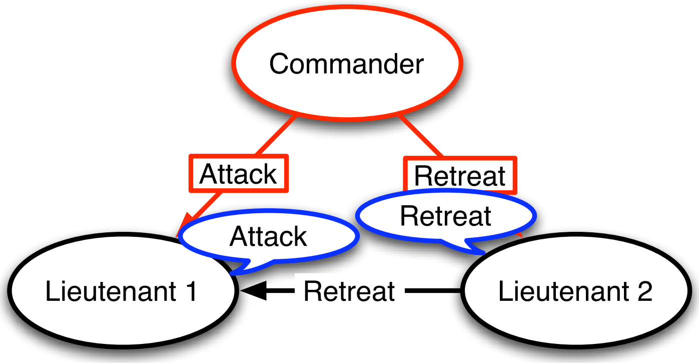
3k+1 nodes are necessary (oral model)



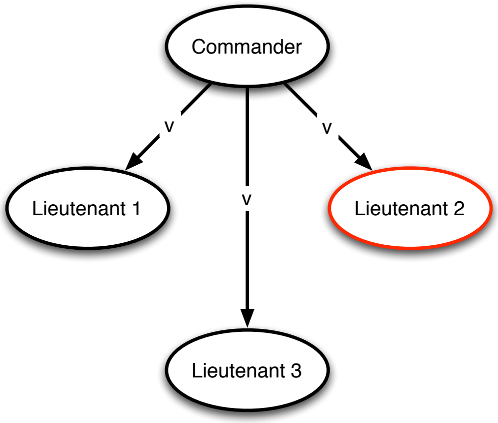
3k+1 nodes are necessary (oral model)



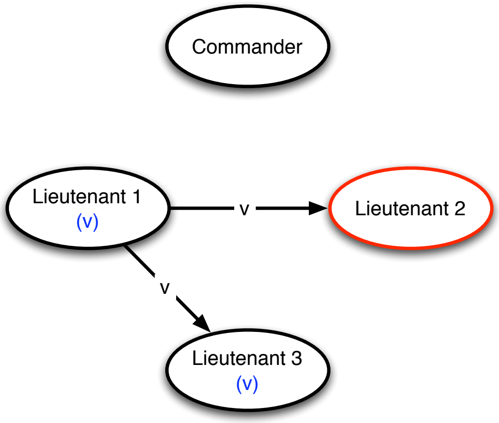
3k+1 nodes are necessary (oral model)



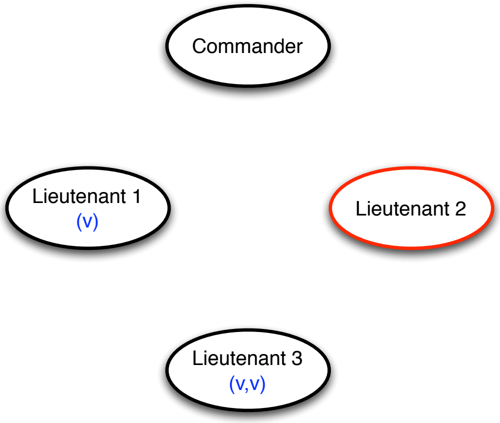
3k+1 nodes are sufficient (oral model)



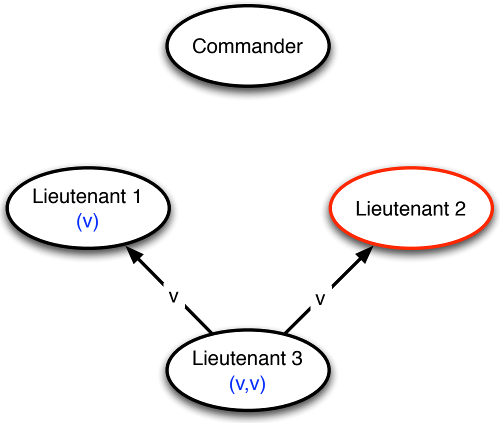
3k+1 nodes are sufficient (oral model)



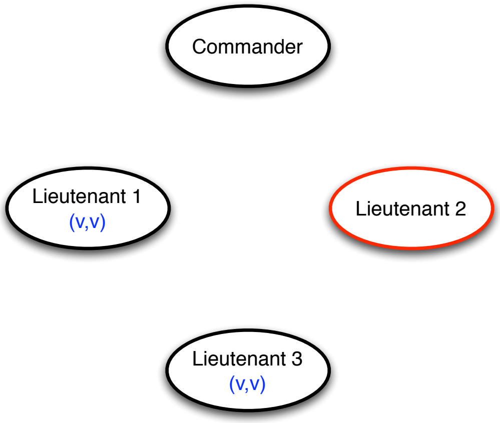
3k+1 nodes are sufficient (oral model)



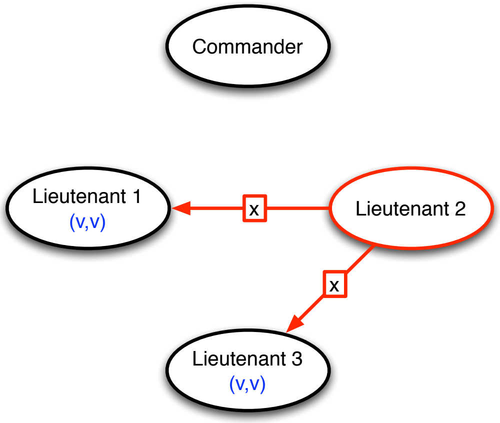
3k+1 nodes are sufficient (oral model)



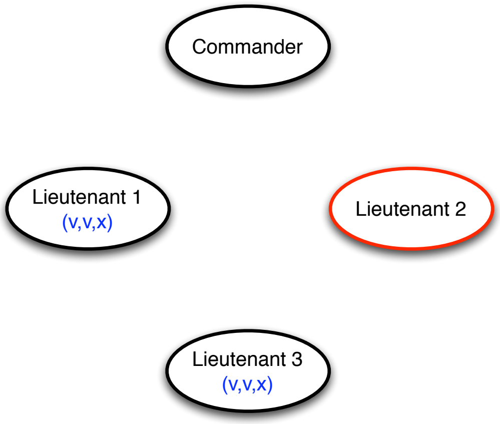
3k+1 nodes are sufficient (oral model)



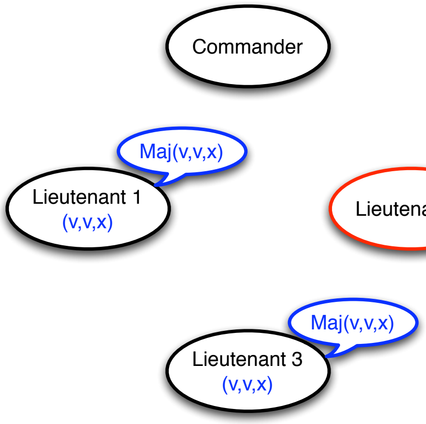
3k+1 nodes are sufficient (oral model)



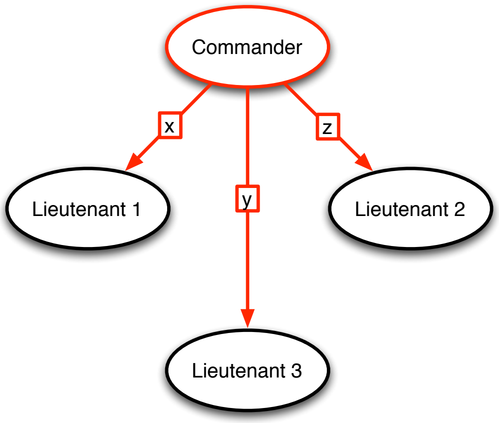
3k+1 nodes are sufficient (oral model)



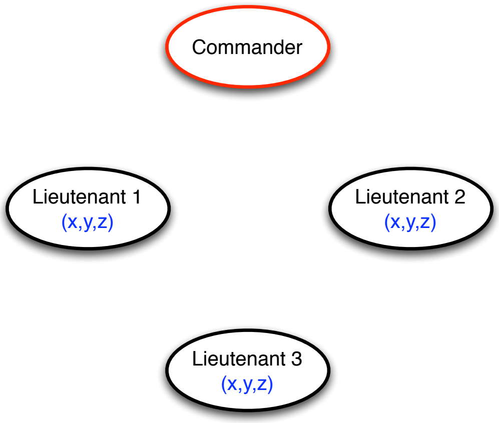
3k+1 nodes are sufficient (oral model)



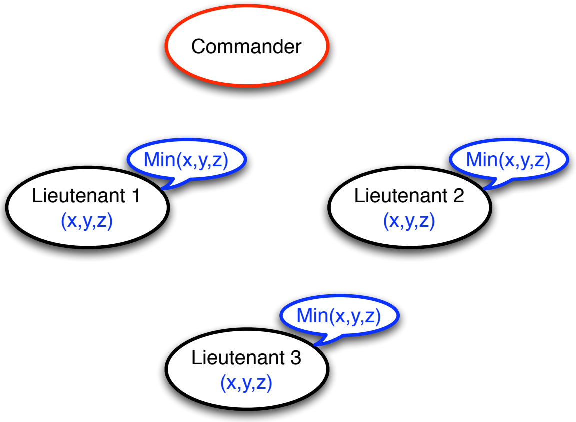
3k+1 nodes are sufficient (oral model)



3k+1 nodes are sufficient (oral model)



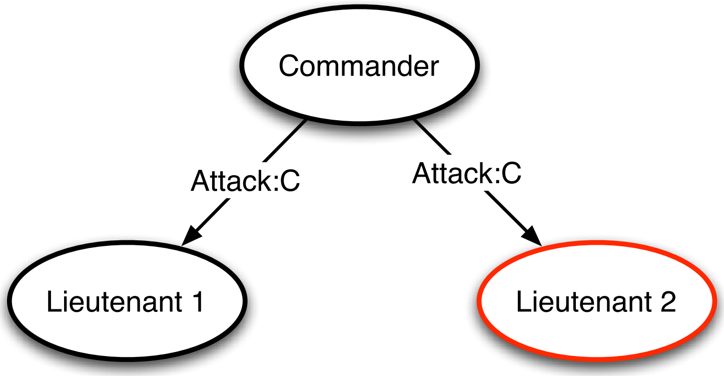
3k+1 nodes are sufficient (oral model)



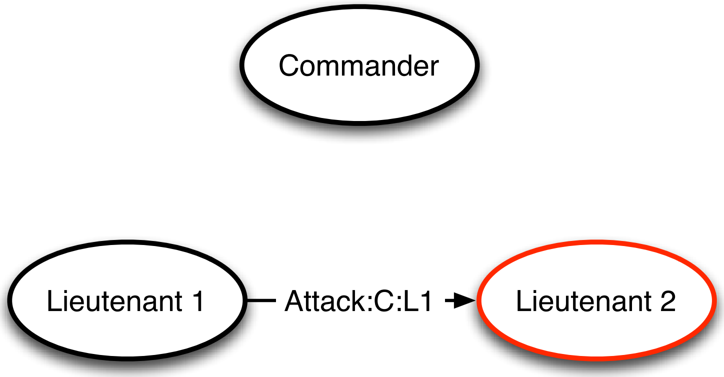
Written Model

- **A1-A3**: Same as before
- **A4**:
  - A loyal general's signature cannot be forged, and any alteration of the contents of his signed messages can be detected
  - Anyone can verify the authenticity of a general's signature

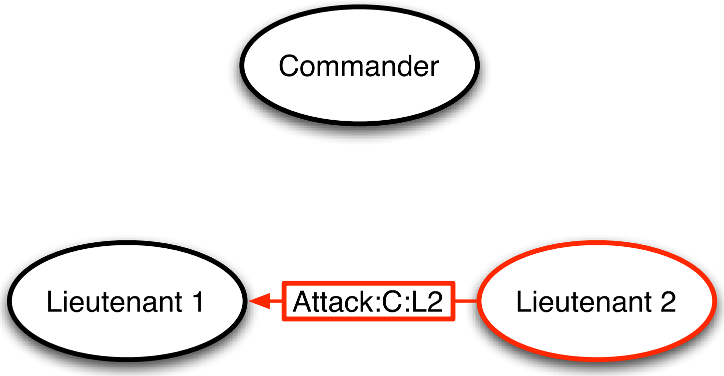
k+2 nodes are sufficient (written model)



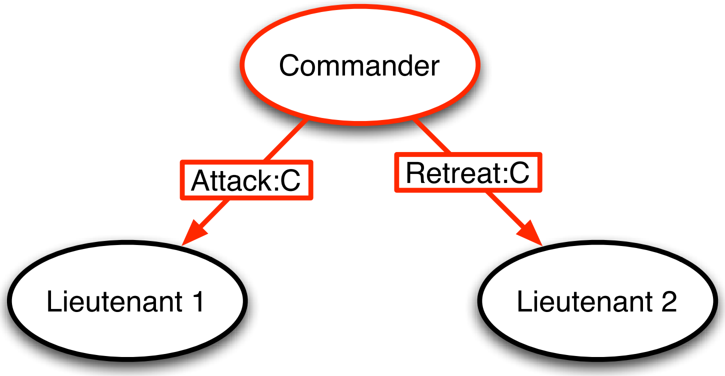
k+2 nodes are sufficient (written model)



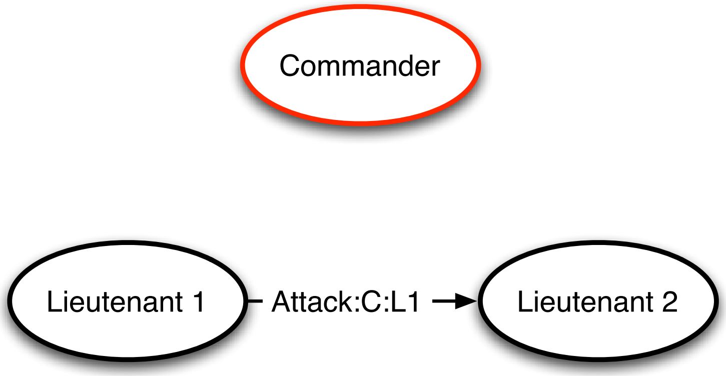
k+2 nodes are sufficient (written model)



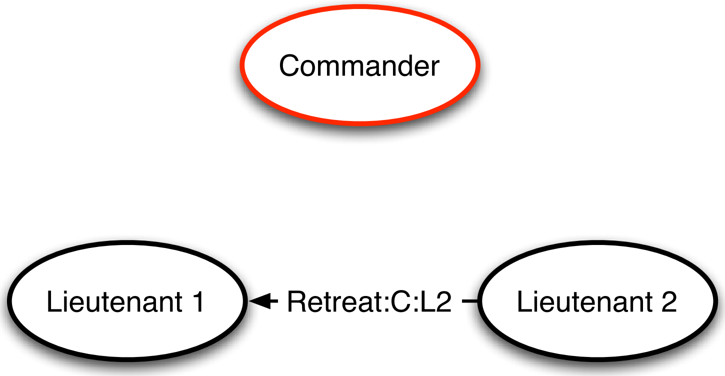
k+2 nodes are sufficient (written model)



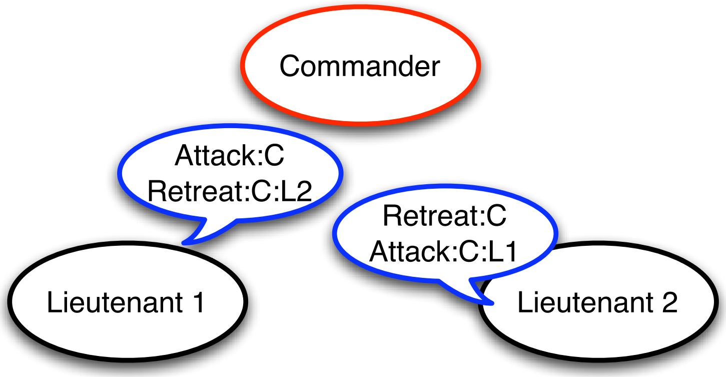
k+2 nodes are sufficient (written model)



k+2 nodes are sufficient (written model)



k+2 nodes are sufficient (written model)



Conclusion

- **Goal**: mask faults and attacks to the user
- **Basic principle**: redundancy and majority
  - not necessary to identify who misbehaves
  - most people must be reliable
  - protocols are much easier with cryptography (but how is crypto set up?)

Pros

- Masks the faults and attacks to the user
- Natural way to cope with failures
- Many protocols are available
  - Consensus, Atomic commit, Reliable Broadcast, Renaming,...

Cons

- Network must be properly initialized
- Global knowledge is assumed
  - size, names, maximum number of faults,...
- Global communication is used
- Global synchrony is assumed