CSE 486/586 Distributed Systems
Byzantine Fault Tolerance

Steve Ko
Computer Sciences and Engineering
University at Buffalo

Recap

- Digital certificates
  - Binds a public key to its owner
  - Establishes a chain of trust
- TLS
  - Provides an application-transparent way of secure communication
  - Uses digital certificates to verify the origin identity
- Authentication
  - Needham-Schroeder & Kerberos

Byzantine Fault Tolerance

- Fault categories
  - Benign: failures we've been talking about
  - Byzantine: arbitrary failures
- Benign
  - Fail-stop & crash: process halted
  - Omission: msg loss, send-omission, receive-omission
  - All entities still follow the protocol
- Byzantine
  - A broader category than benign failures
  - Process or channel exhibits arbitrary behavior.
  - May deviate from the protocol
  - Processes can crash, messages can be lost, etc.
  - Can be malicious (attacks, software bugs, etc.)

Byzantine Fault Tolerance

- Result: with *f faulty nodes*, we need *$3f + 1$* nodes to tolerate their Byzantine behavior.
  - Fundamental limitation
  - Today's goal is to understand this limitation.
- How about Paxos (that tolerates benign failures)?
  - With f faulty nodes, we need $2f + 1$.
  - Having f faulty nodes means that as long as $f + 1$ nodes are reachable, Paxos can guarantee an agreement.
  - This is the known lower bound for consensus with non-Byzantine failures.

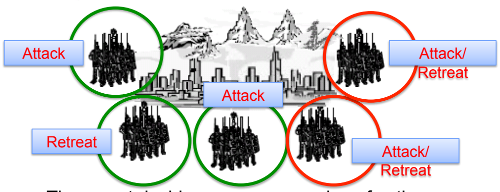
"Byzantine"

- Leslie Lamport (again!) defined the problem & presented the result.
- *"I have long felt that, because it was posed as a cute problem about philosophers seated around a table, Dijkstra's dining philosopher's problem received much more attention than it deserves."*
- *"At the time, Albania was a completely closed society, and I felt it unlikely that there would be any Albanians around to object, so the original title of this paper was The Albanian Generals Problem."*
- *"…The obviously more appropriate Byzantine generals then occurred to me."*

Introducing the Byzantine Generals

- Imagine several divisions of the Byzantine army camped outside of a city
- Each division has a general.
- The generals can only communicate by a messenger.

Introducing the Byzantine Generals



- They must decide on a common plan of action.
  – What is this problem?
- But, *some of the generals can be traitors*.

Requirements

- All loyal generals decide upon the same plan of action (e.g., attack or retreat).
- A small number of traitors cannot confuse the loyal generals nor cause the loyal generals to adopt a bad plan.
- There has to be a way to communicate one's opinion to others correctly.

The Byzantine Generals Problem

- The problem boils down to how a single general sends the general's own value to the others.
  – Thus, we can simplify it in terms of a single commanding general sending an order to lieutenant generals.
- Byzantine Generals Problem: a commanding general must send an order to *n-1* lieutenant generals such that
  – All loyal lieutenants obey the same order.
  – If the commanding general is loyal, then every loyal lieutenant obeys the order the commanding general sends.
- We'll try a simple strategy and see if it works.
  – All-to-all communication: every general sends the opinion & repeatedly sends others' opinions for reliability.
  – Majority: the final decision is the decision of the majority
  – Similar to reliable multicast

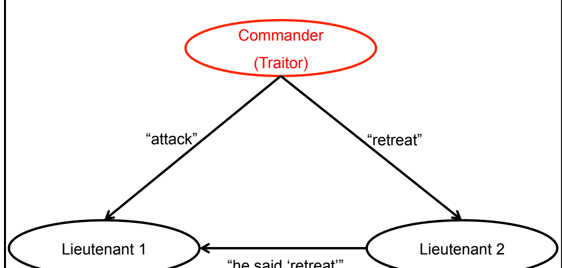
Question

- Can three generals agree on the plan of action?
  – One commander
  – Two lieutenants
  – One of them can be a traitor.
  – Want no confusion, no bad plan, but a good plan.
- This means that we have $2f + 1$ nodes.
  – Again, this is the known lower bound for consensus with non-Byzantine nodes.
  – Protocols like Paxos provides the consensus guarantee.
- The question is if we can still have this same minimum nodes to reach consensus with Byzantine nodes.

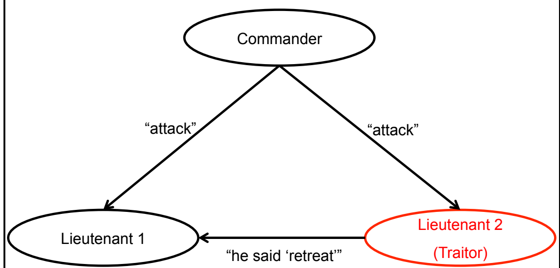
Question

- Protocol
  – Commander sends out an order ("attack"/"retreat").
  – Lieutenants relay the order to each other for reliability (to tolerate message losses).
  – Lieutenants follow the order of the commander.
  – If the commander is the traitor, we elect a new commander.
  – If one of the lieutenants is the traitor, we follow the commander.
  – We want no confusion.
- Can you come up with some scenarios where this protocol doesn't work?

Understanding the Problem



Understanding the Problem



Understanding the Problem

- One traitor makes it impossible with three generals.
- Comparison to non-Byzantine failures (e.g., Paxos)
  - With non-Byzantine failures, *f* nodes can *fail (or disappear)* from the system, but *they don't lie*.
  - E.g., Paxos works with $2f + 1$ nodes when *f* nodes are faulty (i.e., $f + 1$ nodes are reachable).
- In the Byzantine generals problem, *these f* nodes might be alive and malicious.
  - Failures are not any more about reachability.
  - Even if some nodes are reachable, they might be lying.
  - Additional concern: Is this true?
- In general, you need $3f + 1$ nodes to tolerate *f faulty nodes* in the Byzantine generals problem.
- Why?

CSE 486/586 Administrivia

- PA4 due Friday next week
- Final: 5/15 (Friday), 11:45am – 2:45pm
  - NSC 201
  - Everything
  - No restroom use (this quickly becomes chaotic)

Intuition for the Result

- Problem
  - What is the minimum number of nodes do we need to communicate to reach consensus in the presence of Byzantine (malicious) nodes?
  - Phrased differently, how many minimum votes or replies do we need from different nodes?
  - We're not talking about a protocol that makes consensus possible, but rather the minimum bound.
- For the sake of discussion, assume this setting:
  - You're interacting with replicated state machines, e.g., you're using a website that has multiple servers.
  - You send a request, all servers reply back. Some servers might be controlled by an attacker.
  - Based on the replies, you determine the actual result (e.g., yes/no).

Intuition for the Result

- With non-Byzantine failures
  - Up to *f* nodes can be unreachable, meaning, if there is *n* nodes, you might only get $n – f$ votes.
  - This means that just with $n – f$ votes, you should be able to make a decision on consensus.
  - If we set $n == 2f + 1$, we can do just that, e.g., Paxos.
- With Byzantine failures
  - One extreme: Up to *f* nodes can be unreachable (if all exhibit non-Byzantine failures), meaning, if there is *n* nodes, you might only get $n – f$ votes, i.e., you should be able to make a decision on consensus with just $n – f$ votes.
  - Another extreme: Up to *f* nodes can be lying if all exhibit Byzantine failures, i.e., you should still be able to make a decision on consensus with just $n – f$ votes, even if *f* votes out of those $n – f$ votes are in fact lies.
  - What is the minimum *n* then?

Intuition for the Result

- Let's try $n == 2f + 1$.
  - We should be able to reach consensus with $n – f$ votes, i.e., $f + 1$ votes (due to potential unreachability from last slide).
  - And, out of $f + 1$ votes, it's possible that *f* votes are in fact lies.
- Example
  - $2f + 1$ nodes, and outcome by $f + 1$ votes.
  - *f* faulty nodes say no.
  - $f + 1$ non-faulty nodes say yes
  - You get $f + 1$ votes.
  - Ideal scenario?
  - Other possibilities?
- $n == 2f + 1$ does not work.

Intuition for the Result

- Once again (reminder),
  - We should be able to reach consensus with *n – f* votes.
  - And, out of *n – f* votes, it's possible that *f* votes are lies.
- Intuition
  - If we make sure that *n – f* votes always contain more votes from honest nodes than Byzantine nodes, we're safe.
  - E.g., among *n – f* server replies, if there are more replies from honest servers, we can determine the correct result.
- How can we make sure of this?
  - We set *n == 3f + 1*.
  - We can always obtain *n – f*, i.e., *2f + 1* votes. Then we have at least *f + 1 votes from honest nodes*, one more than the number of potential faulty nodes.

Summary

- Byzantine generals problem
  - They must decide on a common plan of action.
  - But, some of the generals can be traitors.
- Requirements
  - All loyal generals decide upon the same plan of action (e.g., attack or retreat).
  - A small number of traitors cannot cause the loyal generals to adopt a bad plan.
- Impossibility results
  - With three generals, it's impossible to reach a consensus with one traitor
  - In general, with less than *3f + 1* nodes, we cannot tolerate *f* faulty nodes.

Acknowledgements

- These slides contain material developed and copyrighted by Indranil Gupta (UIUC).