The Byzantine Generals Problem

Siqiu Yao
Authors

● Leslie Lamport
  ○ you again!
  ○ we all know him

● Robert Shostak
  ○ PhD in Applied Math, Harvard
  ○ SRI International
  ○ Founder, Ansa Software
  ○ Founder, Mira Tech
  ○ Borland Software
  ○ Founder Portera System
  ○ Founder Vocera

● Marshall Pease
Another story from Lamport?

Time, Clocks, and the Ordering of Events in a Distributed System  
1978

The part-time parliament  
1990
Another story from Lamport?

Time, Clocks, and the Ordering of Events in a Distributed System 1978

The Byzantine Generals Problem 1982

The part-time parliament 1990
How this story came

"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.

......

The popularity of the dining philosophers problem taught me that the best way to attract attention to a problem is to present it in terms of a story."
How this story came

“
There is a problem in distributed computing that is sometimes called the Chinese Generals Problem, in which two generals have to come to a common agreement on whether to attack or retreat, but can communicate only by sending messengers who might never arrive.

“

*http://lamport.azurewebsites.net/pubs/pubs.html#byz
How this story came

"I stole the idea of the generals and posed the problem in terms of a group of generals, some of whom may be traitors, who have to reach a common decision."

*http://lamport.azurewebsites.net/pubs/pubs.html#byz
What is the Byzantine generals problem
Byzantine generals problem

“several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action.”

*castle: [http://simpleicon.com/castle.html](http://simpleicon.com/castle.html)
*lieutenant: [https://www.clipartmax.com/max/m2i8Z5i8b1H7N4H7/](https://www.clipartmax.com/max/m2i8Z5i8b1H7N4H7/)
Byzantine generals problem

- Generals should reach a consensus on the plan
- It could be ATTACK

*castle: http://simpleicon.com/castle.html
*lieutenant: https://www.clipartmax.com/max/m2i8Z5i8b1H7N41h7/
Byzantine generals problem

- Generals should reach a consensus on the plan
- Or RETREAT

*castle: [http://simpleicon.com/castle.html](http://simpleicon.com/castle.html)
*lieutenant: [https://www.clipartmax.com/max/m2i8Z5i8b1H17N4H7/](https://www.clipartmax.com/max/m2i8Z5i8b1H17N4H7/)
Byzantine generals problem

- But there might be traitors
- All loyal generals should reach a consensus

*castle: [http://simpleicon.com/castle.html](http://simpleicon.com/castle.html)
*lieutenant: [https://www.clipartmax.com/max/m2i8Z5ieb1H7N4H7/](https://www.clipartmax.com/max/m2i8Z5ieb1H7N4H7/)
*traitor: [https://thenounproject.com/term/traitor/](https://thenounproject.com/term/traitor/)
Byzantine generals problem

- But traitors can act arbitrarily
- All loyal generals should reach a consensus

*castle: http://simpleicon.com/castle.html
*lieutenant: https://www.clipartmax.com/max/mv2/8Z5i8b11H7N4H7/
*traitor: https://thenounproject.com/term/traitor/
Byzantine generals problem

- But traitors can act arbitrarily
- All loyal generals should reach a consensus

*castle: http://simpleicon.com/castle.html
*lieutenant: https://www.clipartmax.com/max/m2i8Zsi8b1H7N4H7/
*traitor: https://thenounproject.com/term/traitor/
Byzantine generals problem

- A simplified version

“A commanding general sends an order to his $n-1$ lieutenant 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.”
What is the byzantine generals problem

- IC1. All loyal lieutenants obey the same order
- IC2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.
What is the byzantine generals problem

- Consistency/Agreement
- IC2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.
What is the byzantine generals problem

- Consistency/Agreement
- Validity
What is the byzantine generals problem

- Consistency/Agreement
- IC2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.
What is the byzantine generals problem

- Consistency/Agreement
- Validity
- Liveness/Termination?
Impossibility Result
Impossibility result

“if the generals can send only oral messages, then no solution will work unless more than $\frac{2}{3}$ of the generals are loyal.”
Impossibility result

“if the generals can send only oral messages, then no solution will work unless more than $\frac{2}{3}$ of the generals are loyal.”

what are oral messages?
Impossibility result

oral messages:

- every message that is sent is delivered correctly
- the receiver of a message knows who sent it
- the absence of a message can be detected
Impossibility result

oral messages:

- every message that is sent is delivered correctly
- the receiver of a message knows who sent it
- the absence of a message can be detected
Impossibility result

oral messages:

- every message that is sent is delivered correctly
- authenticated channel
- the absence of a message can be detected
Impossibility result

oral messages:

- every message that is sent is delivered correctly
- authenticated channel
- the absence of a message can be detected
Impossibility result

oral messages:

- every message that is sent is delivered correctly
- authenticated channel
- synchronous network
Impossibility result

“if the generals can send only oral messages, then no solution will work unless more than \( \frac{2}{3} \) of the generals are loyal.”

in a synchronous network, with authenticated channel, when \( m \) generals are traitors, no solution will work unless there are more than \( 3m \) generals
impossibility result - proof

- case $m = 1$: 
impossibility result - proof

- case $m = 1$:
  - scenario 1:
    - the commander is loyal
    - one lieutenant is a traitor
impossibility result - proof

- case $m = 1$:
  - scenario 1:
    - the commander is loyal
    - one lieutenant is a traitor
    - the left lieutenant should attack

the commander said “RETREAT!”
impossibility result - proof

- case \( m = 1 \):
  - scenario 2:
    - the commander is a traitor

- the commander said “RETREAT!”
- the commander said “ATTACK!”
Three scenarios

ATTACK!

ATTACK!

ATTACK!

the commander said “RETREAT!”

I should ATTACK!

the commander said “ATTACK!”

I should ATTACK!

I should RETREAT!

the commander said “RETREAT!”

the commander said “ATTACK!”
Three scenarios

- The commander said "RETREAT!"
- The commander said "ATTACK!"
- I should ATTACK!

Consistency broken!
impossibility result

prove $m > 1$ by contradiction

- assume we have a solution protocol $f$ for $3m$ generals when $m > 1$
- we can solve $m = 1$ case by leveraging $f$
impossibility result

prove $m > 1$ by contradiction

- assume the three generals are $x$, $y$, $z$, and $x$ is the commander;
- according to protocol $f$
  - $x$ simulates one commander and $m-1$ lieutenants
  - each of $y$ and $z$ simulates $m$ lieutenants
impossibility result

prove $m > 1$ by contradiction

- assume the three generals are $x$, $y$, $z$, and $x$ is the commander;
- according to protocol $f$
  - $x$ simulates one commander and $m-1$ lieutenants
  - each of $y$ and $z$ simulates $m$ lieutenants
- at most one of $x$, $y$, $z$ is a traitor
  - at most $m$ simulated traitors
  - protocol $f$ can solve the case when there are at most $m$ traitors
impossibility result

prove $m > 1$ by contradiction

- if we can solve case $m > 1$ then we can solve $m = 1$
- we proved case $m = 1$ cannot be solved
- contradiction!
Oral messages’ fault

- With only oral messages, traitors can lie by telling the wrong command they received
Three scenarios

the commander said “RETREAT!”

I should ATTACK!

the commander said “ATTACK!”

I should ATTACK!

the commander said “ATTACK!”

I should RETREAT!
Signed message

- With only oral messages, traitors can lie by telling the wrong command they received
- Signed messages
  - cannot be forged
  - anyone can verify the authenticity
Solutions:
oral messages and signed messages
Solutions - with oral messages

- OM(k)
  - k == 0
    - commander sends the value to every one
    - everyone return the value they received
Solutions - with oral messages

- OM(k)
  - k == 0
    - commander sends the value to every one
    - everyone return the value they received
  - k > 0
    - commander sends the value to every one
    - everyone start a smaller bgp OM(k-1) containing all ones but the current commander and become the new commander
    - everyone participated n-1 OM(k-1) and get n-1 values, return the majority
OM(1)
OM(1) - 3*OM(0)
Solutions - with oral messages

- **OM(k)**
  - **k == 0**
    - Commander sends the value to every one
    - Everyone return the value they received
  - **k > 0**
    - Commander sends the value to every one
    - Everyone start a smaller bgp OM(k-1) containing all ones but the current commander and become the new commander
    - Everyone participated n-1 OM(k-1) and get n-1 values, return the majority

- Intuition: for every message M received, solve a smaller bgp containing all but the current commander to tell others you received M
Solutions - with oral messages

- **OM(k)**
  - k == 0
    - commander sends the value to every one
    - everyone return the value they received
  - k > 0
    - commander sends the value to every one
    - everyone start a smaller bgp **OM(k-1)** containing all ones but the current commander and become the new commander
    - everyone participated n-1 **OM(k-1)** and get n-1 values, return the majority

- Intuition: for every message M received, solve a smaller bgp containing all but the current commander to tell others you received M

- **OM(m)** for m traitors when 3m < n
Solutions - with oral messages

- **OM(k)** - Message complexity: \((n-1) \times MC(OM(k-1)) + n-1 = O(n^m)\)
  - \(k = 0\)
    - Commander sends the value to everyone
    - Everyone return the value they received
  - \(k > 0\)
    - Commander sends the value to everyone
    - Everyone start a smaller bgp **OM(k-1)** containing all ones but the current commander
    - Become the new commander
    - Everyone participated \(n-1\) **OM(k-1)** and get \(n-1\) values, return the majority

- Intuition: for every message \(M\) received, solve a smaller bgp containing all but the current commander to tell others you received \(M\)
- **OM(m)** for \(m\) traitors when \(3m < n\)
Solutions - with signed messages

- **SM(k)**
  - every lieutenant maintains a value set $V(i)$
  - the commander sends the value to every lieutenant with its signature
Solutions - with signed messages

- **SM(k)**
  - every lieutenant maintains a value set $V(i)$
  - the commander sends the value to every lieutenant with its signature
  - for every lieutenant
    - every time it receives a new value $v$
    - put it in $V(i)$
    - if $v$ is associated with less than $m$ lieutenants’ signatures, sign it and send to everyone
Solutions - with signed messages

- **SM(k)**
  - every lieutenant maintains a value set $V(i)$
  - the commander sends the value to every lieutenant with its signature
  - for every lieutenant
    - every time it receives a new value $v$
    - put it in $V(i)$
    - if $v$ is associated with less than $m$ lieutenants’ signatures, sign it and send to everyone
  - when there will be no more messages, return $\text{choice}(V(i))$
  - $\text{choice}(V)$
    - return $v$ then $V = \{v\}$
    - return RETREAT when $|V| = 0$
SM(1)

V(1) = V(2)
Solutions - with signed messages

- **SM(k)**
  - every lieutenant maintains a value set \( V(i) \)
  - the commander sends the value to every lieutenant with its signature
  - for every lieutenant
    - every time it receive a new value \( v \)
    - put it in \( V(i) \)
    - if \( v \) is associated with less than \( k \) lieutenants’ signatures, sign it and send to everyone
  - when there will be no more messages, return \( \text{choice}(V(i)) \)
  - \( \text{choice}(V) \)
    - return \( v \) then \( V = \{v\} \)
    - return RETREAT when \( |V| = 0 \)

- intuition: ensure every message received by a loyal lieutenant is sent to every loyal lieutenant
Solutions - with signed messages

- **SM(k)**
  - every lieutenant maintains a value set \( V(i) \)
  - the commander sends the value to every lieutenant with its signature
  - for every lieutenant
    - every time it receive a new value \( v \)
    - put it in \( V(i) \)
    - if \( v \) is associated with less than \( k \) lieutenants’ signatures, sign it and send to everyone
  - when there will be no more messages, return choice(\( V(i) \))
  - choice(\( V \))
    - return \( v \) then \( V = \{v\} \)
    - return RETREAT when \(|V| = 0|\)

- intuition: ensure every message received by a loyal lieutenant is sent to every loyal lieutenant

- **SM(m+1)** for \( m \) traitors
Solutions - with signed messages

- SM(k) - message complexity: O(n^2)
  - every lieutenant maintains a value set V(i)
  - the commander sends the value to every lieutenant with its signature
  - for every lieutenant
    - every time it receives a new value \( v \)
    - put it in V(i)
    - if \( v \) is associated with less than \( k \) lieutenants’ signatures, sign it and send to everyone
  - when there will be no more messages, return choice(V(i))
  - choice(V)
    - return \( v \) then \( V = \{ v \} \)
    - return RETREAT when \( |V| = 0 \)

- intuition: ensure every message received by a loyal lieutenant is sent to every loyal lieutenant
- SM(m+1) for \( m \) traitors
Solutions - with signed messages

- **SM(k)** - message complexity: $O(n^2)$
  - every lieutenant maintains a value set $V(i)$
  - the commander sends the value to every lieutenant with its signature
  - for every lieutenant
    - every time it receive a new value $v$
    - put it in $V(i)$
    - if $v$ is associated with less than $k$ lieutenants’ signatures, sign it and send to everyone
  - when there will be no more messages, return $\text{choice}(V(i))$
  - $\text{choice}(V)$
    - return $v$ then $V = \{v\}$
    - return RETREAT when $|V| = 0$

- intuition: ensure every message received by a loyal lieutenant is sent to every loyal lieutenant
- **SM(m+1)** for $m$ traitors
Minimum number required for which an $f$-resilient consensus protocol exists

<table>
<thead>
<tr>
<th></th>
<th>synchrony</th>
<th>asynchrony</th>
<th>partial synchrony</th>
</tr>
</thead>
<tbody>
<tr>
<td>fail-stop</td>
<td>$f+1$</td>
<td>inf</td>
<td>$2f+1$</td>
</tr>
<tr>
<td>crash</td>
<td>$f+1$</td>
<td>inf</td>
<td>$2f+1$ (Paxos)</td>
</tr>
<tr>
<td>byzantine with digital signature</td>
<td>$f+1 \ (SM(f+1))$</td>
<td>inf</td>
<td></td>
</tr>
<tr>
<td>byzantine with authenticated channel</td>
<td>$3f+1 \ (OM(f))$</td>
<td>inf</td>
<td></td>
</tr>
</tbody>
</table>
Minimum number required for which an $f$-resilient consensus protocol exists

<table>
<thead>
<tr>
<th></th>
<th>synchrony</th>
<th>asynchrony</th>
<th>partial synchrony</th>
</tr>
</thead>
<tbody>
<tr>
<td>fail-stop</td>
<td>$f+1$</td>
<td>inf</td>
<td>$2f+1$</td>
</tr>
<tr>
<td>crash</td>
<td>$f+1$</td>
<td>inf</td>
<td>$2f+1$ (Paxos)</td>
</tr>
<tr>
<td>byzantine with digital signature</td>
<td>$f+1$ (SM($f+1$))</td>
<td>inf</td>
<td>???</td>
</tr>
<tr>
<td>byzantine with authenticated channel</td>
<td>$3f+1$ (OM($f$))</td>
<td>inf</td>
<td></td>
</tr>
</tbody>
</table>
Byzantine with digital signature in partial synchrony

- No partial synchronous protocols can tolerate \( \frac{1}{3} \) faults.
- Sound familiar?
- Assume there exist a protocol that can solve it.
Byzantine with digital signature in partial synchrony

It takes less than $T_l$ to reach a consensus. I should **ATTACK**!

It takes less than $T_r$ to reach a consensus. I should **RETREAT**!

It takes more than $\max(T_l, T_r)$ for messages to be delivered.

The commander said "**RETREAT!**"
Practical Byzantine Fault Tolerance

- Commander sends the value to every lieutenant
- Every lieutenant
  - if it receives a new value $v$, broadcast (prepare, $v$)
  - if it receives $2f+1$ (prepare, $v$), broadcast (commit, $v$)
  - if it receives $2f+1$ (commit, $v$), broadcast (committed, $v$)
  - if it receives $f+1$ (committed, $v$), broadcast (committed, $v$)
Practical Byzantine Fault Tolerance

- Commander sends the value to every lieutenant
- Every lieutenant
  - if it receives a new value $v$, broadcast (prepare, $v$)
  - if it receives $2f+1$ (prepare, $v$), broadcast (commit, $v$)
  - if it receives $2f+1$ (commit, $v$), broadcast (committed, $v$)
  - if it receives $f+1$ (committed, $v$), broadcast (committed, $v$)
- Ensure agreement
- Ensure liveness under a loyal commander
Practical Byzantine Fault Tolerance

- Commander sends the value to every lieutenant
- Every lieutenant
  - if it receives a new value v, broadcast (prepare, v)
  - if it receives 2f+1 (prepare, v), broadcast (commit, v)
  - if it receives 2f+1 (commit, v), broadcast (committed, v)
  - if it receivers f+1 (committed, v), broadcast (committed, v)
- Ensure agreement
- Ensure liveness under an loyal commander
- What if the commander is faulty?
  - we need view change
Minimum number required for which an $f$-resilient consensus protocol exists

<table>
<thead>
<tr>
<th></th>
<th>synchrony</th>
<th>asynchrony</th>
<th>partial synchrony</th>
</tr>
</thead>
<tbody>
<tr>
<td>fail-stop</td>
<td>$f+1$</td>
<td>$\inf$</td>
<td>$2f+1$</td>
</tr>
<tr>
<td>crash</td>
<td>$f+1$</td>
<td>$\inf$</td>
<td>$2f+1$ (Paxos)</td>
</tr>
<tr>
<td>byzantine with digital signature</td>
<td>$f+1$ (SM($f+1$))</td>
<td>$\inf$</td>
<td>$3f+1$ (PBFT)</td>
</tr>
<tr>
<td>byzantine with authenticated channel</td>
<td>$3f+1$ (OM($f$))</td>
<td>$\inf$</td>
<td></td>
</tr>
</tbody>
</table>
Thoughts

- Defined Byzantine generals problem
- Proved lower bound in synchronous environment with authenticated channel
- Introduced solutions in synchronous environment with authenticated channel and with digital signature
- But today we usually discuss about the case when in partial synchronous/asynchronous environment with digital signature where PBFT works
Timeline

1982
- The Byzantine Generals Problem
  - OM() sync/authenticated channel
  - SM() sync/digital signature

1990
- The part-time parliament
- Paxos: async/non-byzantine(crash-failure)

1998
- Practical Byzantine Fault Tolerance
  - PBFT: partial sync/digital signature/state machine replication

2008
- Bitcoin: A peer-to-peer electronic cash system
- Blockchain: partial sync/proof of work/state machine replication