CS 5594: BLOCKCHAIN TECHNOLOGIES

Spring 2024

THANG HOANG, PhD

CONSENSUS IN SYNCRHONOUS NETWORK

Public Blockchain (Recap)

So far, we have considered distributed consensus in public blockchain

- Repeated consensus **over time**
- **Asynchronous** network: there is no time clock. Every node can only be invoked upon receiving some message from the network
- Tolerate $f < n/2$ corruptions via randomized and asynchronous consensus
- Probabilistic

In this lecture, we will consider (classical) consensus a simpler distributed setting with synchronous network

- Suitable for private blockchain

Overview

Byzantine Generals Problem

Dolev-Strong Protocol

Muddy Children Puzzle

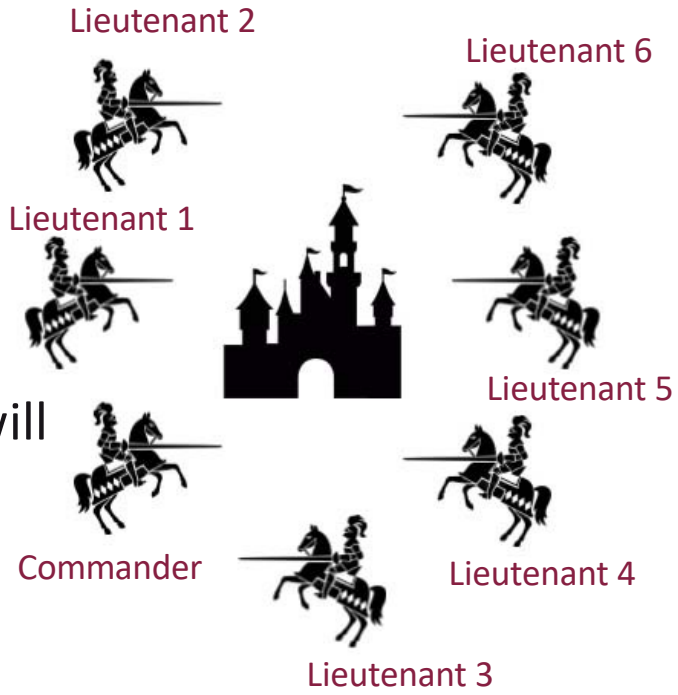
Byzantine Generals Problem

Byzantine Generals Problem

There are n generals, one of them is the commander, others are lieutenants

Commander proposes an order to all lieutenants: **ATTACK** or **RETREAT**, such that

1. All *loyal* lieutenants reach the same decision
2. If commander is *loyal*, then all *loyal* lieutenants will obey commander's order



Formulated by Lamport et al.

Also commonly referred to as Byzantine Broadcast (BB)

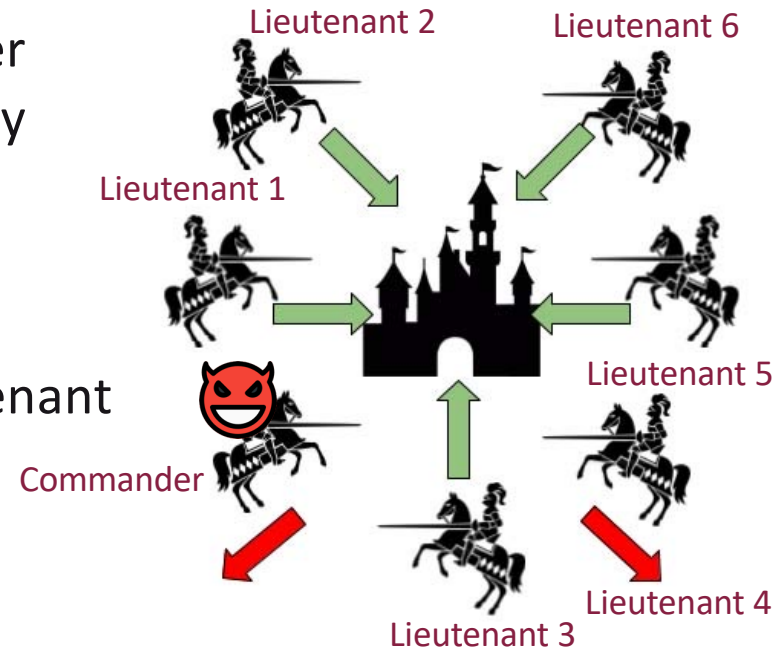
Byzantine Generals Problem

If the commander is loyal, the problem is trivial

The commander sends its order to all other lieutenants, and all lieutenants simply obey

What if the commander is a **traitor**?

Propose different orders to different lieutenant



Is it still possible for the loyal generals to agree upon an attack plan by communicating with each other despite the influence of corrupted generals?

Byzantine Generals Problem Formulation

A distributed network of n nodes numbered $1,2, \ldots, n$

A subset of the nodes can be corrupt

- May not follow the protocol, may send/transmit arbitrary messages at arbitrary times, omit sending messages, stop or take an incorrect step
- Can form a coalition and share information with each other and perform a coordinated attack (controlled by a single adversary)

Byzantine Broadcast protocol must work no matter which subset of nodes are corrupt, as long as the total number of corruptions is upper bounded by $f < n$

Synchronous Network

When honest nodes send messages, the honest recipients are guaranteed to receive them within a bounded amount of time

This is considered as one round communication

Protocol proceeds in rounds

Synchrony assumption: If an honest node sends a message in round r to an honest recipient, then the recipient will receive the message at the beginning of round $r + 1$.

Byzantine Broadcast

At the beginning, the designated sender receives an input bit $b \in \{0,1\}$

All nodes execute protocol. At the end, every honest node outputs a bit

No matter how corrupt nodes behave, a Byzantine Broadcast protocol must satisfy <u>two</u> conditions:

- **Consistency**: If two honest nodes output b and b', resp., then $b = b'$
- **Validity**: If the sender is honest and receives the input bit b, then all honest nodes should output b

Oral Message Protocol

When there is no traitor

Protocol **OM(0)**, i.e., m=0, no traitor

1. Commander sends his value to every general
2. Each general outputs the value he receives from Commander, or outputs **RETREAT** if he receives no value

Oral Message Protocol

When there are some traitors

Protocol **OM(m)**, i.e., m > 0 there are m traitors

1. Commander sends his value to every general
2. For each general i:
    1. Let v_i be the value general i receives from Commander, or else be RETREAT if he receives no value. General i acts as Commander in Algorithm **OM(m-1)** to send value v_i to each of $n-2$ other generals.
3. For each i, and each $j \neq i$:
    1. Let v_j^i be the value General i received from General j in step (2) (by **Algorithm OM(m-1)**), or else **RETREAT** if he received no such value. General i outputs **majority**$(v_1^i, v_2^i, \ldots, v_{n-1}^i)$

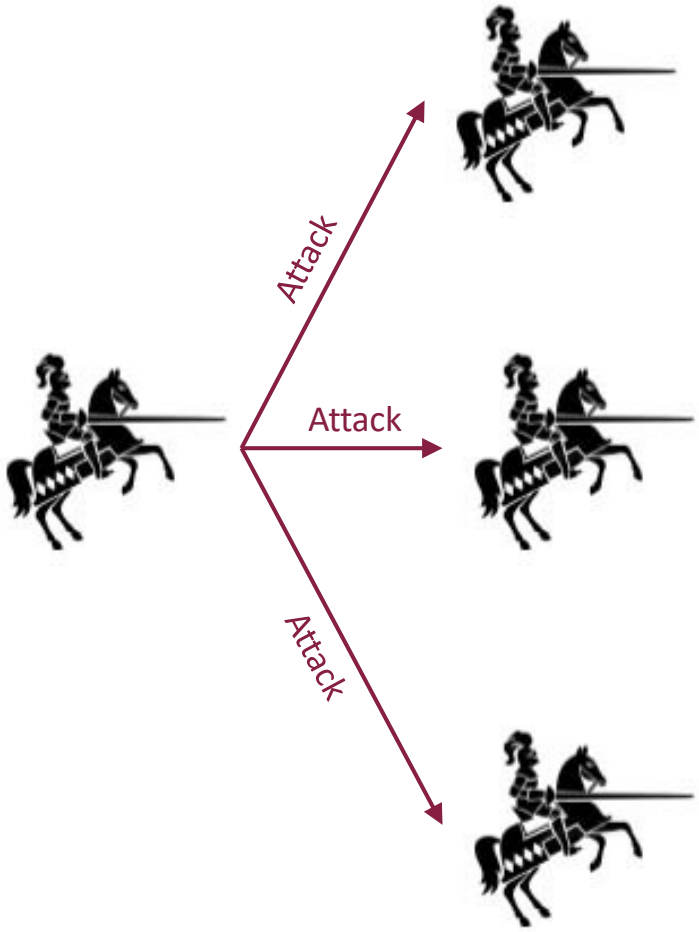
Oral Message Protocol

Example: 4 Generals

OM(m), m=0

C: Send order

L: Follow if received



Oral Message Protocol

Example: 4 Generals

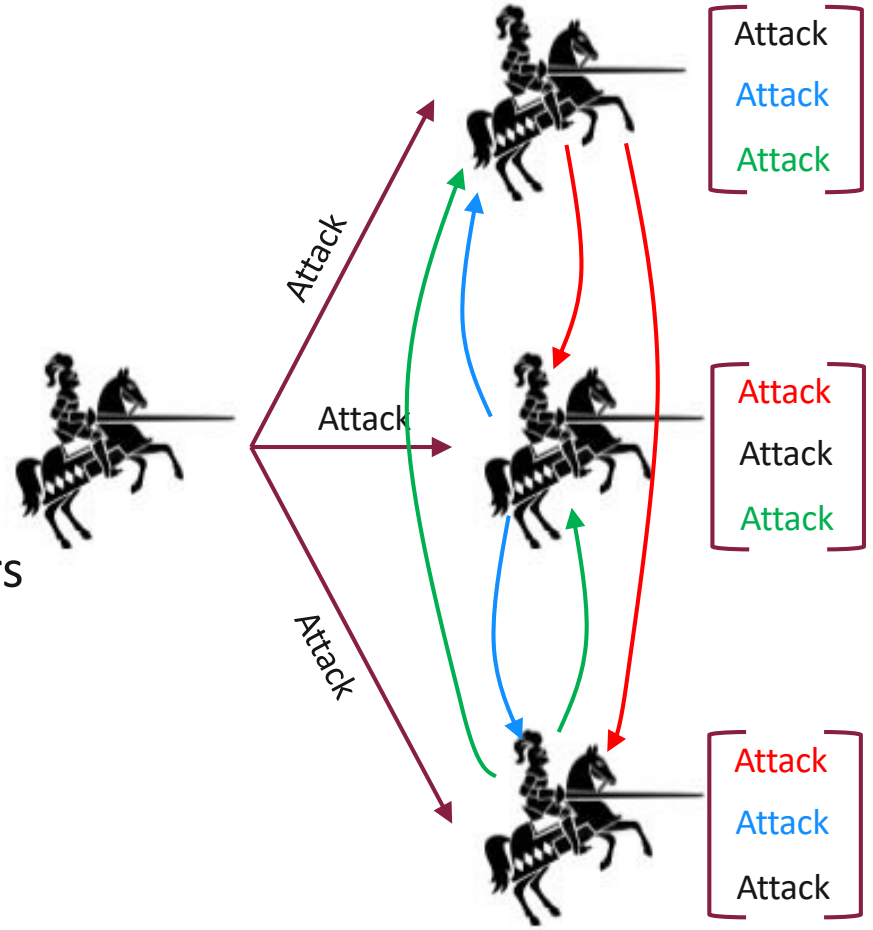
OM(m), m>0

C: Send order

L: 1. Record if received

2. Use OM(m-1) to tell others

3. Follow majority() order



Oral Message Protocol

Example: 4 Generals

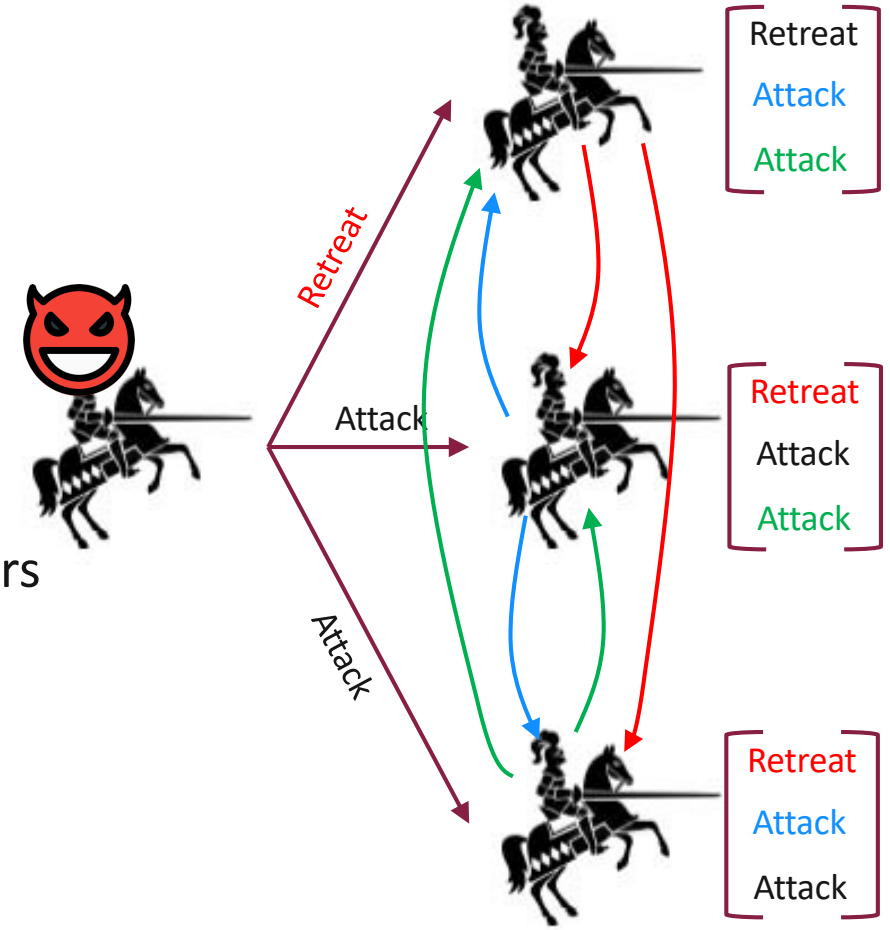
OM(m), m>0

C: Send order

L: 1. Record if received

2. Use OM(m-1) to tell others

3. Follow majority() order



Oral Message Protocol

Example: 4 Generals

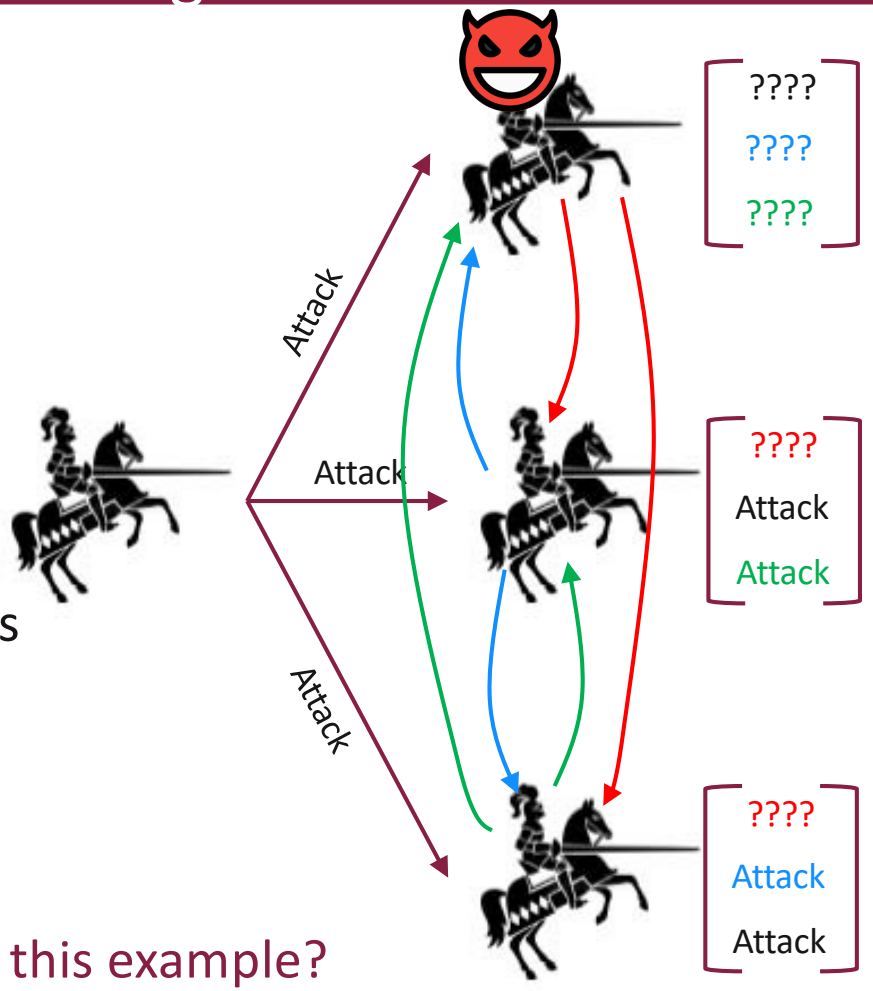
OM(m), m>0

C: Send order

L: 1. Record if received

2. Use OM(m-1) to tell others

3. Follow majority() order



What if there are 2 traitors in this example?

Oral Message Protocol

Can only work with less than **one third** of generals are traitors ($n \geq 3f + 1$)

Complexity

m	Message Sent
0	O(n)
1	O(n^2)
2	O(n^3)
3	O(n^4)

For a general m, complexity is O(n^m)

Solution for n < 3f +1?

The traitor's ability to lie makes the BGP difficult

What if we can restrict this traitor's ability?

The solution: sending of the **unforgeable signed** message

Yes! n<3f +1 can be feasible with public key cryptography

Assumption: Digital signature scheme

- Each node i has a public-secret key pair $(\mathrm{pk}_i, \mathrm{sk}_i)$
- Public key pk_i is known to everybody

A node signs every message (with its secret key) before sending it

Authenticity and accountability of the received message

Attempt: Naïve Majority Voting

Let $\langle m \rangle_i$ denote the message m along with a valid signature from node i

Sender (i.e. node 1) receives the bit b as input.

Round 1: Node 1 sends $\langle b \rangle_1$ to every node (including itself).

Round 2: For every node $i \in [n]$:

If a single bit $\langle b' \rangle_1$ is received, send vote $\langle b' \rangle_i$. Else send vote $\langle 0 \rangle_i$.

Round 3: If **no** bit or **both** bits received more than $n/2$ votes from distinct nodes, output 0. Otherwise, output the bit that received more than $n/2$ votes from distinct nodes.

Does this attempt work in the presence of a single corrupt node?

Dolev-Strong Protocol

Suppose there are up to f corrupt nodes among n nodes

Initially, every node i's extracted set $\text{extr}_i = \{\emptyset\}$

Round 0: Sender sends $\langle b \rangle_1$ to every node.

For each round $r = 1$ to $f + 1$:

For every message $\langle b' \rangle_{1,j_1,j_2,\ldots,j_{r-1}}$ node i receives with r signatures from distinct nodes including the sender:

If $b' \notin \text{extr}_i$: add b' to $\notin \text{extr}_i$ and send $\langle b' \rangle_{1,j_1,j_2,\ldots,j_{r-1},i}$ to everyone

(node i added its signature to the set of r signatures it received)

At the end of round $f + 1$: If $|\text{extr}_i| = 1$: node i outputs the bit in extr_i. Otherwise, outputs 0

why is $f + 1$ rounds necessary for Dolev-Strong protocol?

Dolev-Strong Protocol

Lemma 1. Let $r \leq f$. If after round r, some honest node i has b' in ext_i, then after round $r + 1$, every honest node has b' in its extracted set.

*This implies if some honest node has included some bit b' in round $r < f + 1$, then all honest nodes will have included the same bit in the **immediate** next round*

Lemma 2. If some honest node i has b' in ext_i by the end of round $f + 1$, then every honest node has b' in its extracted set by the end of round $f + 1$.

*This implies consistency: if some honest node has included a bit b' in the final round f + 1, then all honest nodes must have included it in the **same** round*

Theorem 2. The Dolev-Strong protocol achieves Byzantine Broadcast (consistency and validity) in the presence of up to $\text{f} \leq n$ corrupt nodes.

Byzantine Broadcast without Signature

Dolev-Strong protocol [DS83] solves Byzantine Broadcast under any $f < n$ number of corruptions

Can we achieve Byzantine Broadcast without digital signatures and without a Public-Key Infrastructure (PKI)?

- There exists an Impossibility Result of Consensus with 1/3 corruptions without Digital Signatures – (*Fischer, Lynch, and Merritt's Theorem*)
- In fact, lower bound and upper bound are proven

Muddy Children Puzzle

Muddy Children Puzzle

There are n children playing in the playground, $k \leq n$ of them acquire mud on forehead

After playing, the teacher gathers the children and declares: “one or more of you have mud on your forehead”

Everyone can see if others have mud on their forehead, but they cannot tell for themselves

Problem: How do the children know that they have mud on forehead, without communicating with one another?

Muddy Children Puzzle

Teacher says to the kids: “step up if you know have mud on your forehead”.

If no one steps up, teacher repeats the request.

This goes on for multiple rounds until some children step forward.

Question: in which round will some (all) muddy children step forward?

Muddy Children Puzzle: Solution

Solved by Induction

- $k = 1$ (Muddy kid: Alice)

  Alice will step up because she sees that no other child has mud

- $k = 2$ (Muddy kids: Alice, Bob)

  Round 1: No one steps forward. Why?

  Round 2: Both Alice and Bob step forward. Why?

- In general, if k kids have mud, then all k muddy kids will step up in round exactly k

Common knowledge is reached in round k

Somewhat reminiscent of the Dolev-Strong protocol