

Distributed Algorithms

Solution for Project 3

Group 8

1. Alexandre Georges Rémi Martin, 406294
2. Benyamin Shafabakhsh, 406305
3. Yared Dejene Dessalk, 406228
4. Anubhav Guha, 406244
5. Jiaqiao Peng, 406038

January 25, 2019

Exercise 3.1

i.

The Byzantine Generals agreement algorithm must ensure that the loyal generals shouldn't be prohibited from reaching to an agreement by the plot created by the traitors. So, the agreement algorithm should guarantee the following conditions:

- All loyal generals should decide upon the same plan of action
- Traitors shouldn't cause the loyal generals to adopt a bad plan

It is proved that the Byzantine Generals problem, there is not solution for 3 generals in which one of them is a traitor. The general rule to have solution for Byzantine Generals problem is that for m traitors, there must be at least $3m + 1$ generals or more.

One way to get solution for the problem is using oral messages. Oral messages are general forms of message which fulfill the following conditions:

- Every sent message should deliver correctly
- Receiver is aware of who sent the message
- Message absence can be detected

Oral Message algorithms $OM(n,m)$

Variable

- m : number of traitors
- n : total number of generals

Assumptions and initial values:

- Majority of the values v_i is v . i.e. $majority(v_1, \dots, v_{n-1})$

$OM(n,0)$

1. The commander sends his value to every of the lieutenants
2. Each lieutenant adopt the value received from the commander, or set the default value, RETREAT, if he hasn't received any value.

$OM(n,m), m>0$

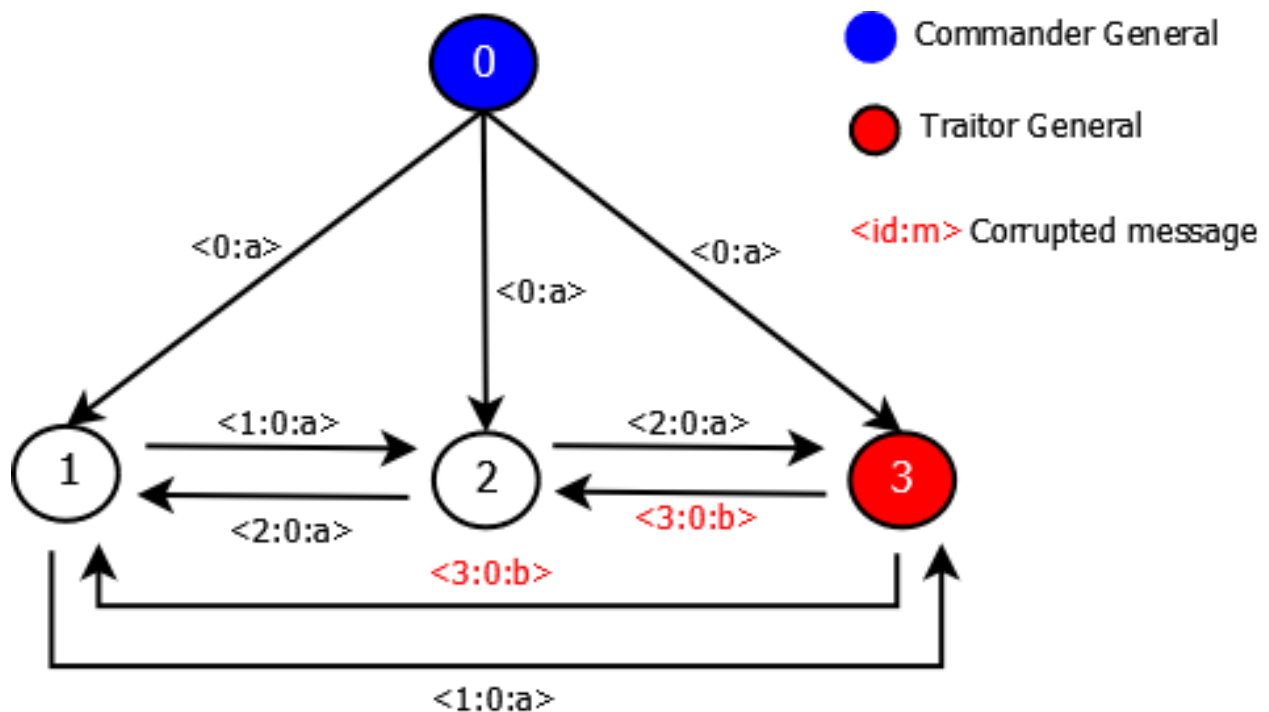
1. The commander sends his value to every of the lieutenants
 2. For each i ,
 - o Let v_i be the value that Lieutenant i receives from the command, or the default value, RETREAT, if he receives no value.
 - o Lieutenant i acts as the commander in Algorithm $OM(n - 1, m - 1)$ to send the value v_i to each of the $n - 2$ lieutenants.
 3. For each i , and each j different from i ,
 - o Let v_j be the value that Lieutenant i receives from Lieutenant j in step (2), or the default value, RETREAT, if he receives no value.
- Lieutenant i uses the value $majority(v_1, \dots, v_{n-1})$

- $n = 4$ (4 generals), $m = 1$ (one randomly chosen general is faulty).

Let us consider different scenarios to demonstrate the above algorithm.

a. $n = 4$ (4 generals), $m = 1$ (one randomly chosen general is faulty)

Assume that one of the lieutenant generals i.e. ID=3 is traitor and ID=0 is the commander general. The image below shows how the algorithm works for this scenario.



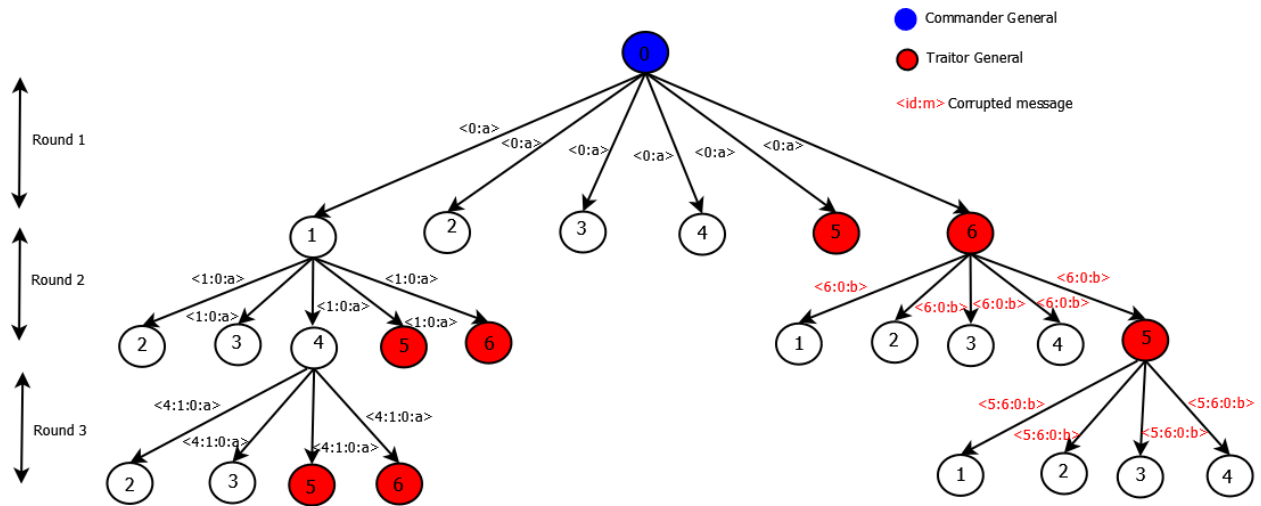
After two round of message exchange, the loyal lieutenant generals will have the following set of messages received:

- 1: $\{a, a, b\}$
- 2: $\{a, a, b\}$

Therefore, by using majority function, each of them decides that **a** as the correct message. And the algorithm terminates in **2 rounds** in which **9 messages** are exchanged among the generals.

b. $n = 7$ (7 generals), $m = 2$ (two randomly chosen generals are faulty)

Assume that two of the lieutenant generals i.e. ID=5 and ID=6 are traitors and ID=0 is the commander general. The image below shows how the algorithm works for this scenario. The image shows details of ID=1 and ID=6 up to the final round.

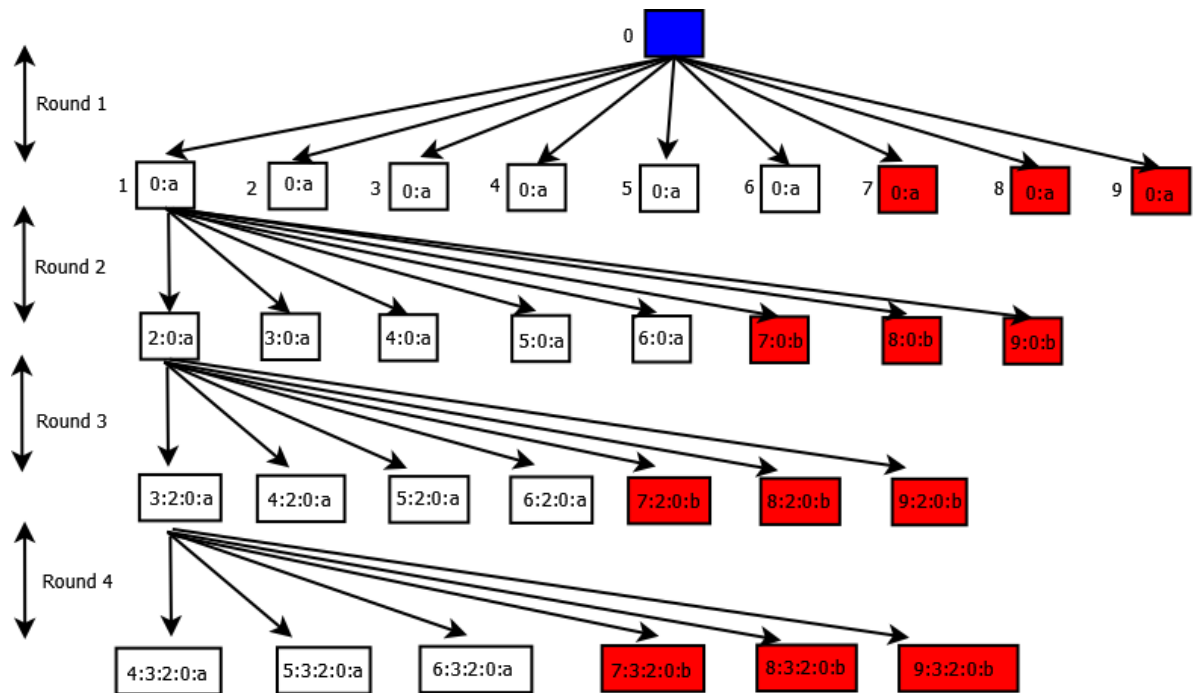


The algorithm takes **3 rounds** to finish and **156 messages** are being exchanged.

c. **$n = 10$ (10 generals), $m = 3$ (three randomly chosen generals are faulty).**

Assume that three of the lieutenant generals i.e. ID=7, ID=8 and ID=9 are traitors and ID=0 is the commander general.

Let us use the message tree here and detail is shown for only ID=1.



The algorithm finishes in **4 rounds** to finish and **3,609 messages** are being exchanged.

Exercise 3.2

I.

A: It depends.

Omission Fault - Some actions are not exercised: Data receiver flags are not set correctly and leads buffer overflows.

Crash Fault - A node suddenly fails and afterwards no actions are exercised: Data transmitter flags are not handled and leads to failure propagation.

II.

1. Byzantine faults - Faulty processes can exercise arbitrary actions and cooperate among each other: The failure was propagated to other neighbors by out-of-service message, reaching 114 switching nodes in the network.
2. Crash Fault - A node suddenly fails and afterwards no actions are exercised: Consider on board computer as a node. A crash fault results in node failure and no actions.