The Oral Message algorithm $OM(m)$ for the Byzantine Generals Problem

Zuyu Zhang
UW-Madison

October 4, 2013

1 Question

Imagine there are 1 loyal commander, 2 traitor lieutenants, and 3 loyal lieutenants. Please provide a concrete example where OM(2) is used among these soldiers, yet the loyal lieutenants fail to all follow the commander's command. You need to briefly describe the process of OM(2) in your example.

2 Answer

Lamport et al. [1] presented the Oral Message algorithm $OM(m)$ to solve the Byzantine Generals Problem, where all generals are connected as a complete graph.

Algorithm $OM(0)$.

(1) The commander sends his value to every lieutenant.

(2) Each lieutenant uses the value he receives from the commander, or uses the value RETREAT if he receives no value.

Algorithm OM(m), $m > 0$.

(1) The commander sends his value to every lieutenant.

(2) For each i, let v_i be the value Lieutenant i receives from the commander, or else be RETREAT if he reeives no value. Lieutenant i acts as the commander in Algorithm $OM(m-1)$ to send the value v_i to each of the $n-2$ other lieutenants.

(3) For each i, and each $j \neq i$, let v_j be the value Lieutenant i received from Lieutenant j in step (2) (using Algorithm $OM(m-1)$), or else RETREAT if he received no such value. Lieutenant i uses the value $majority(v_1, \ldots, v_{n-1})$, whose value is the majority value among the v_i if it exists, otherwise the value RETREAT.

According to the definition of the algorithm, $OM(2)$ has three steps, shown in Figure 1, Figure 4, and Figure 5, respectively.

In Figure 1, the red ellipse represent the faulty nodes, while the blue one for the normal nodes. The commander sends the "Attack" order to all lieutenants to which it connects.

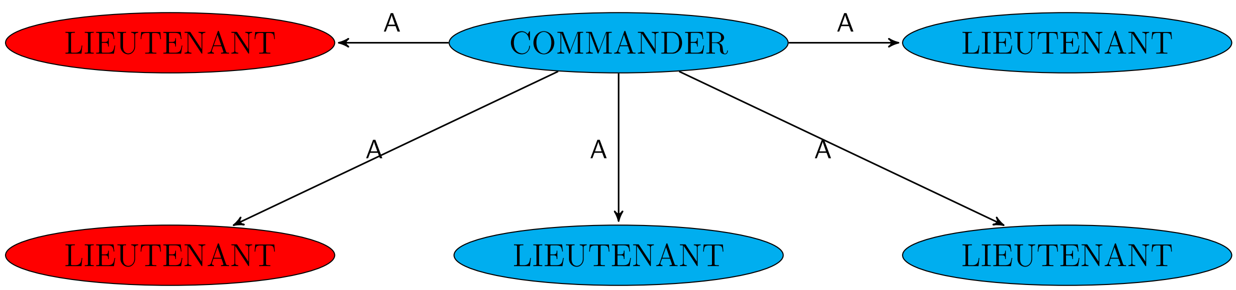
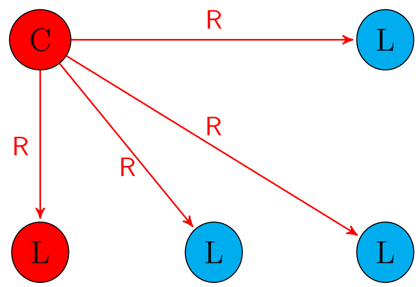
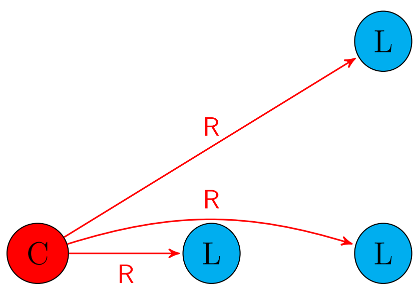


Figure 1 – OM(2) Step (1)

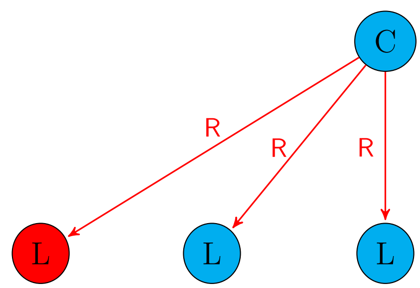
In the step (2) of $OM(2)$, each lieutenant, acting as a commander, performs $OM(1)$ to other lieutenants. Figure 2 and Figure 3, where a red line denotes a "Retreat" order, present how $OM(1)$ works over a traitor lieutenant and a loyal one. In the situation where a traitor lieutenant acts as a commander, the results of all other lieutenants should use the same order, "Retreat". On the other hand, although a loyal lieutenant sends the orignal order, "Attack", two faulty ones would have a significant impact on the results of the order that a lieutenant chooses. From the subfigures (b) to (e) in Figure 3, we found that each normal node receives four orders, two "Attack" and two "Retreat". Therefore, according to the definition of the function *majority*, every normal node chooses "Retreat" as its value, shown in subfigure (f) of Figure 3, since there is no majority value for either order.



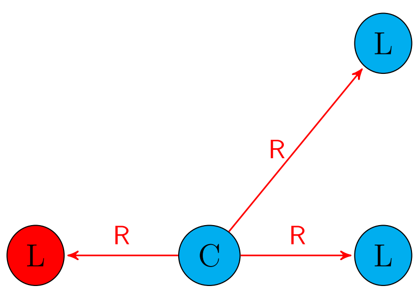
(a) OM(1) Step (1)



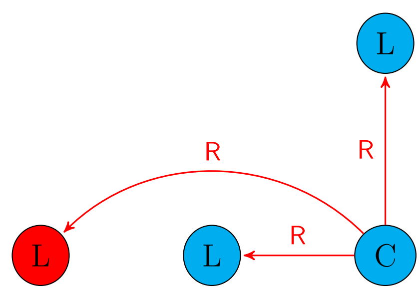
(b) OM(1) Step (2): OM(0)



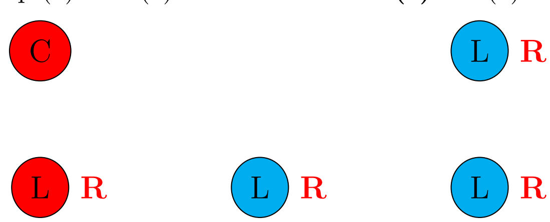
(c) OM(1) Step (2): OM(0)



(d) OM(1) Step (2): OM(0)

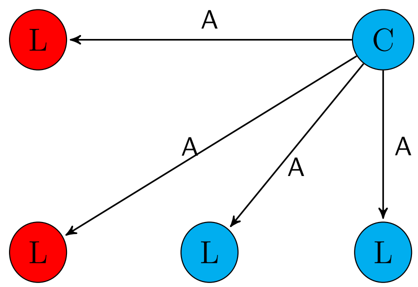


(e) OM(1) Step (2): OM(0)

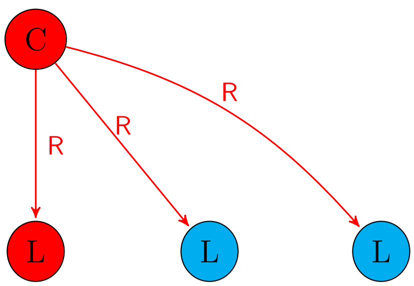


(f) OM(1) Step (3)

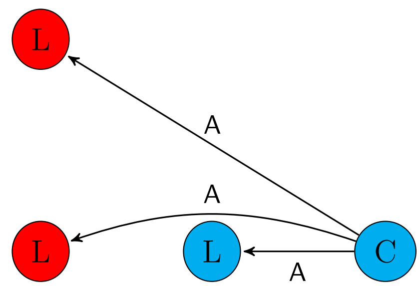
Figure 2 – OM(2) Step (2): Traitor Lieutenant's OM(1)



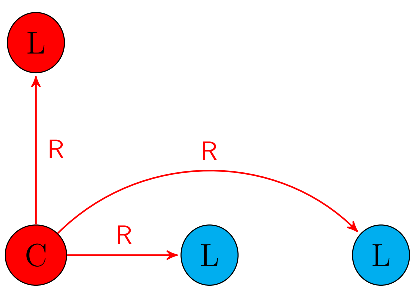
(a) OM(1) Step (1)



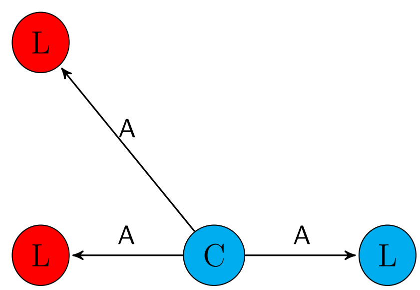
(b) OM(1) Step (2): OM(0)



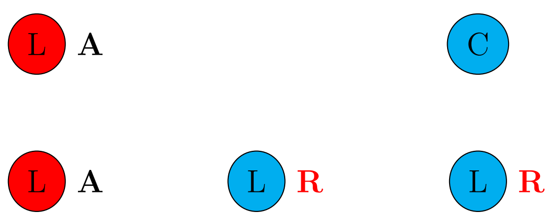
(c) OM(1) Step (2): OM(0)



(d) OM(1) Step (2): OM(0)

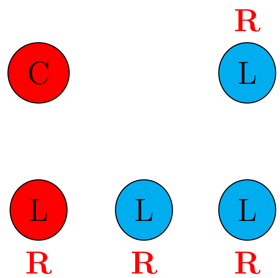


(e) OM(1) Step (2): OM(0)

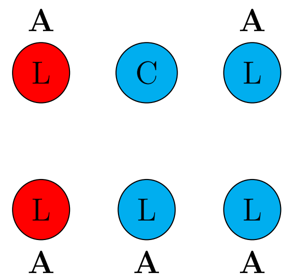


(f) OM(1) Step (3)

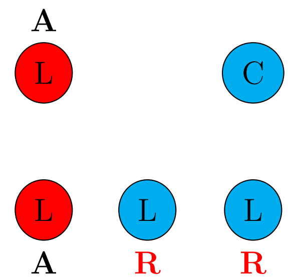
Figure 3 – OM(2) Step (2): Loyal Lieutenant's OM(1)



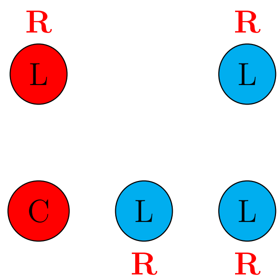
(a) OM(1) Step (3)



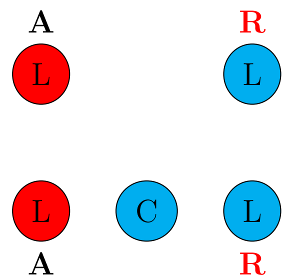
(b) OM(1) Step (3)



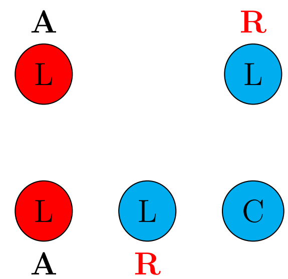
(c) OM(1) Step (3)



(d) OM(1) Step (3)



(e) OM(1) Step (3)



(f) OM(1) Step (3)

Figure 4 – OM(2) Step (2): All Lieutenants' OM(1)

Figure 4 summarizes the results of $OM(2)$'s step (2) for each lieutenant. For this question, although we have six subgraphs to present every order that each lieutenant chooses in the $OM(1)$, the subgraphs are similar to two aforementioned scenarios for both traitor and loyals, except for that different lieutenant in the subgraphs plays the role of the commander.

Finally, we present the result of $OM(2)$ in Figure 5. Every result is chosen by the *majority* function for the data in Figure 4. We could observe that, although the loyal commander sends the "Attack" order, every loyal lieutenant obeys the opposite order, "Retreat"; in other words, loyal lieutenants actually perform against the precondition, which should not happen.

To sum up, $OM(2)$ could not deal with the situation where 2 traitors exists among 5 lieutenants, along with 1 loyal commander.

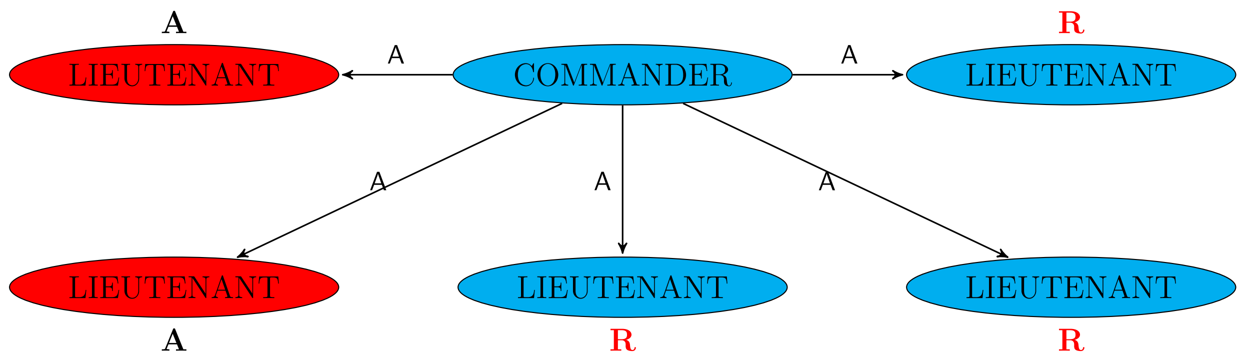


Figure 5 – OM(2) Step (3)

References

[1] Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. *The Byzantine Generals Problem*. ACM Trans. Program. Lang. Syst. 4, 3 (July 1982), 382-401. DOI=10.1145/357172.357176 http://doi.acm.org/10.1145/357172.357176