

All the students (and faculty) in 15-440/640 are chosen as captains for the next Star-Trek mission. Each member will lead a Federation spaceship. Your mission is to attack and destroy the stronghold of a villain named "Beorg". However, Beorg, using his evil powers, has brainwashed some of you to betray the Federation. Suspecting this, "Captain Foy" has decided to form a practical Byzantine fault tolerant system for the mission. Captain Foy (aka "the client") sends an attack signal to all the ships. Also, the Federation has appointed "Captain Cameron" to be the organizer who then directs the other ships as per the BFT protocol (Assume that Captain Cameron properly forwards the attack request from Captain Foy to all the ships). It's given that Number of students + Number of Faculty (i.e. total number of people) = 151. To determine whether to attack, Captain Foy must count the number of photon torpedoes among the ships. If we have more than 1000 torpedoes, we should attack.

1. If all of the 151 members are participating, what is the maximum number of people who can be brainwashed by The Beorg before we can't guarantee BFT consensus?

For it to work: $151 = 3f + 1$. Solving for f , we get $f = 50$.

2. Captain Cameron wants to make the attack timing decision himself. Using PBFT, he sends the timing message, signed with a private key, to the leader among the ships (the leader is also determined using PBFT). How many matching responses from the ships does he need to wait for and why?

This asks about PBFT and for how many matching responses the PBFT client needs to wait. The answer is $f + 1$, so 51 in this case.

3. On the way to destroy Beorg, you encounter the "Asteroid Belt" and 148 ships are destroyed. You decide that even 3 ships (i.e A, B, C) are able to destroy the enemy if all of them attack simultaneously. Unfortunately, it is unknown whether any of the captains of the ships are honest or brainwashed. Describe a scenario where the captains cannot decide to attack even though they have 1000 torpedoes just among the three ships.

Here, you have to find a situation where A and C don't attack together. Assuming B (WLOG) is brainwashed it could send conflicting commands to A and C. B could tell A to attack and C to withdraw meaning that only A will attack. This is an example of byzantine failure.

4. Beorg has now been defeated (yay!) and the captains are no longer at risk of being brainwashed (yay 2!). However, they still need to come to a decision of where to return home to after their great success. Random space interference means that ships can lose connection for several minutes at a time. The ships, therefore, adopt Paxos to come to a decision. In this case, how many faults can now be tolerated?

$3 = 2f+1$. Solving for f , we get $f = 1$, only 1 fault can be tolerated.