Quiz 3c

- Honor Code: You must work completely independently on this assignment. Do not discuss the questions or answers with each other before the assignment is due. Any breach of the honor code will be handled per the University's policy on academic honesty.
- Follow the instructions very careful. Answers that do not conform to the instructions will not be given credit.
- Submit your answers through Blackboard as a PDF file
- You may use your BCT textbook and other course reading material only. Do not use any other resources.

1. For each of the following instances of the Byzantine General's Problem (BGP), determine whether consensus is achieved. Suppose each BGP instance consists of exactly three generals A, B, C, and suppose C is the commander.
    a. A, B, C are loyal. A, B, C all attack.
    b. A, B, C are loyal. A, B both retreat, and C attacks.
    c. A, B are loyal, but C is not. A, B both attack, and C retreats.
    d. A, B, C are not loyal. A, B both attack, and C retreats.
    e. A is loyal, but B, C are not. A, B both attack, and C retreats.
    f. A, B are not loyal, but C is loyal. A attacks, B retreats, and C attacks.

2. Consider a BGP instance with three generals A, B, and C where general C is the commander. Suppose one of the three generals is a traitor. Describe a simple consensus protocol that the generals can use to achieve consensus that satisfies agreement and validity. The protocol can only use oral messages and the generals can communicate directly with each other.

3. Consider a network consisting of six processes that use Lamport's protocol [1] to achieve consensus with at most two malicious processes and only uses oral messages. Which of the following statements are true? Select all that apply.
    a. The consensus protocol maintains a single EIG tree in the leader process that is repeatedly updated by other non-leader processes.
    b. The EIG tree of every compliant process will have the same number of vertices and levels.
    c. At the end of consensus, the labels on the EIG tree of a compliant process will be the same as the labels on the EIG tree of every other compliant process.
    d. Suppose the processes are numbered 1, 2, 3, 4, 5, 6, and that the message "13:A" means process 3 was told that process 1 was told to attack by the leader. The messages "13:A" and "31:A" have the same meaning.
    e. The EIG tree of every compliant process will have three levels, not including the root.

4. Consider a network consisting of six processes that use Lamport's protocol [1] to achieve consensus using only oral messages. How many malicious processes can the protocol handle before consensus is compromised? Select all that apply.
    a. One malicious process
    b. Two malicious processes
    c. Three malicious processes
    d. Four malicious processes

References

1. Lamport, Shostak, Pease. *The Byzantine General's Problem*. ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, Pages 382-401.