Byzantine Generals Problem

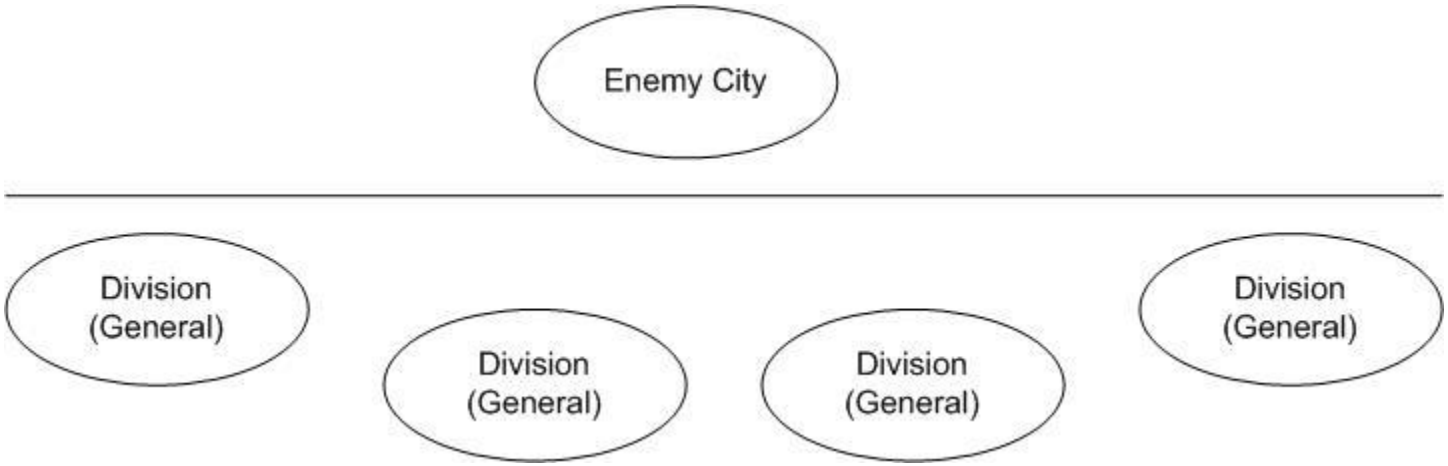
Overview

- The Problem
- Two Solutions
- Oral Messages
- Signed Messages

The Problem

- Important to have reliable computer systems
- Two solutions to ensuring a reliable system
  - Having components that never fail
  - Ensure proper handling of cases where components fail
- Byzantine Generals Problem

The Problem



- Divisions of the Byzantine army camped outside the walls of an enemy city.
- Each division is led by a general.
- Generals decide on a common plan of action

The Problem

There are two types of generals

- Loyal Generals
- Traitor Generals

Problem – Conditions

Two conditions must be met:

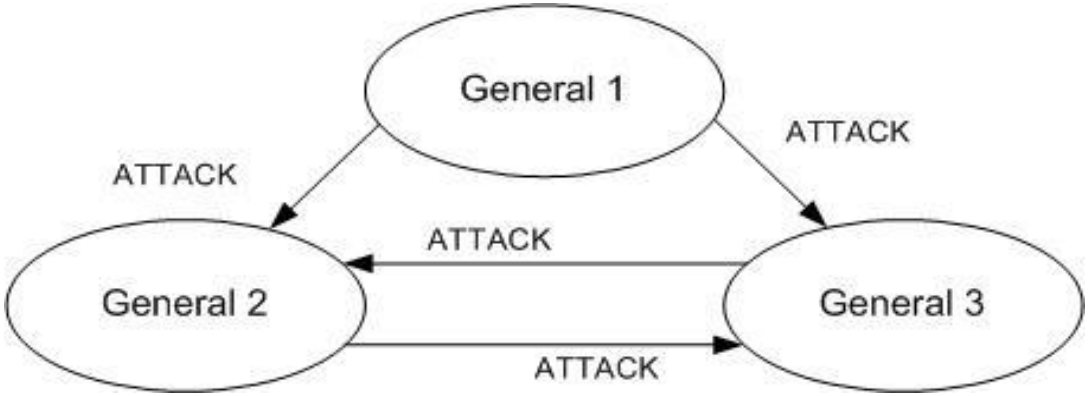
- All loyal generals decide upon the same plan of action.
- A small number of traitors cannot cause the loyal generals to adopt a bad plan.

Problem – Not a Bad Plan

A plan that is not bad is defined in the following way:

- Each general sends his observation to all other generals.
- Let v(i) be the message communicated by the i^{th} general.
- The combination of the v(i) for i = 1, …, n messages received determine a plan that is not bad.

Problem – Example Not a Bad Plan



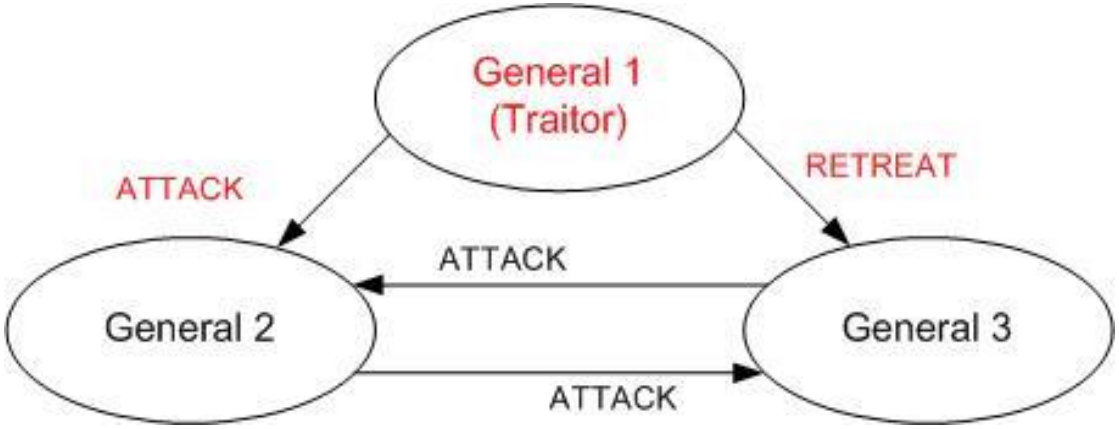
- General 2 receives ATTACK, ATTACK.
- General 3 receives ATTACK, ATTACK.

So Not a Bad Plan is to ATTACK

Problem – Example Not a Bad Plan

- Assumed that every general communicates the same v(i) to every other general.
- A traitor general can send different v(i) messages to different generals.

Problem – Example Flaw



- General 2 receives ATTACK, ATTACK.
- General 3 receives RETREAT, ATTACK.

Is Not a Bad Plan to ATTACK or RETREAT?

Problem – New Conditions

The new conditions are:

- Any two loyal generals use the same value of v(i).
- If the i^{th} general is loyal, then the value that he sends must be used by every loyal general as the value of v(i).

Byzantine Generals Problem

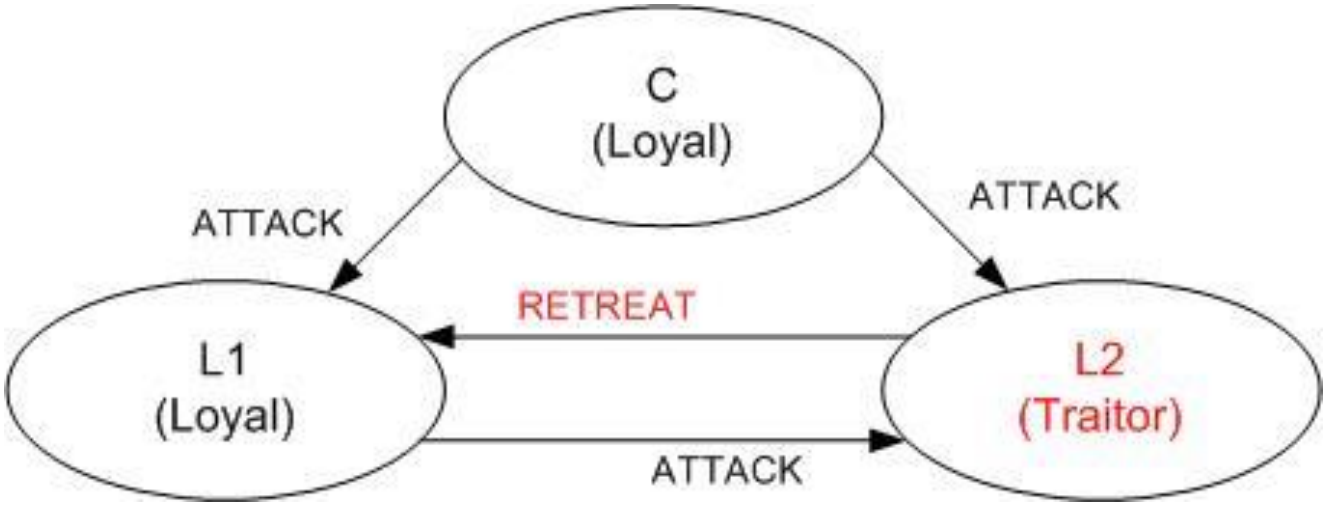
- A commander general giving orders to his lieutenant generals.
- Byzantine Generals Problem – A commanding general must send an order to his n-1 lieutenant generals such that:
  - IC1. All loyal lieutenants obey the same order.
  - IC2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.

Impossibility Results

When will the Byzantine Generals Problem fail?

The problem will fail if 1/3 or more of the generals are traitors.

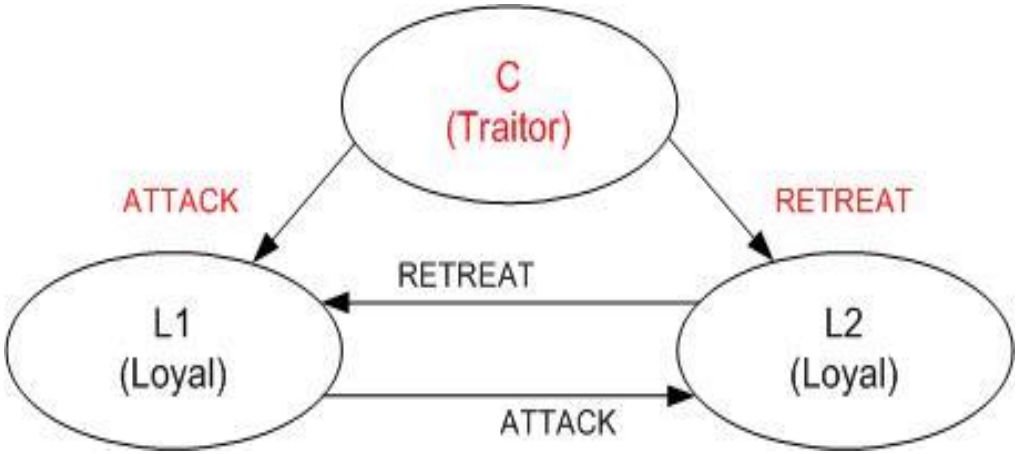
Impossibility Results – Example 1



L1 received the commands ATTACK, RETREAT

L1 doesn't know which general is a traitor.

Impossibility Results – Example 2



L1 again received the commands ATTACK, RETREAT

L1 doesn't know which general is a traitor.

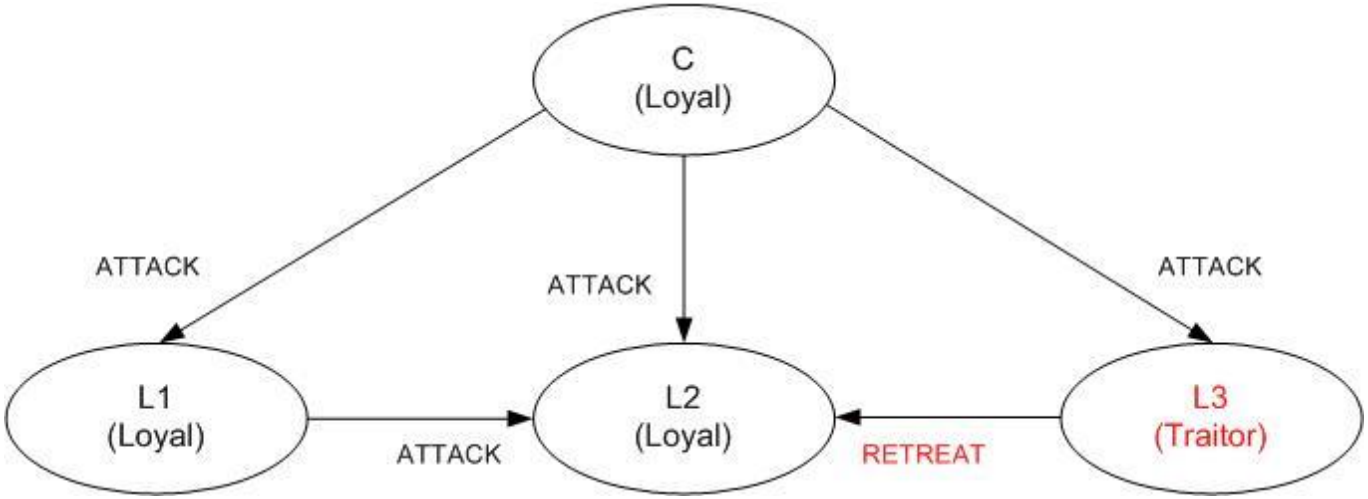
Solution with Oral Messages

Assumptions:

A1: Every message that is sent is delivered correctly.

A2: The receiver of a message knows who sent it.

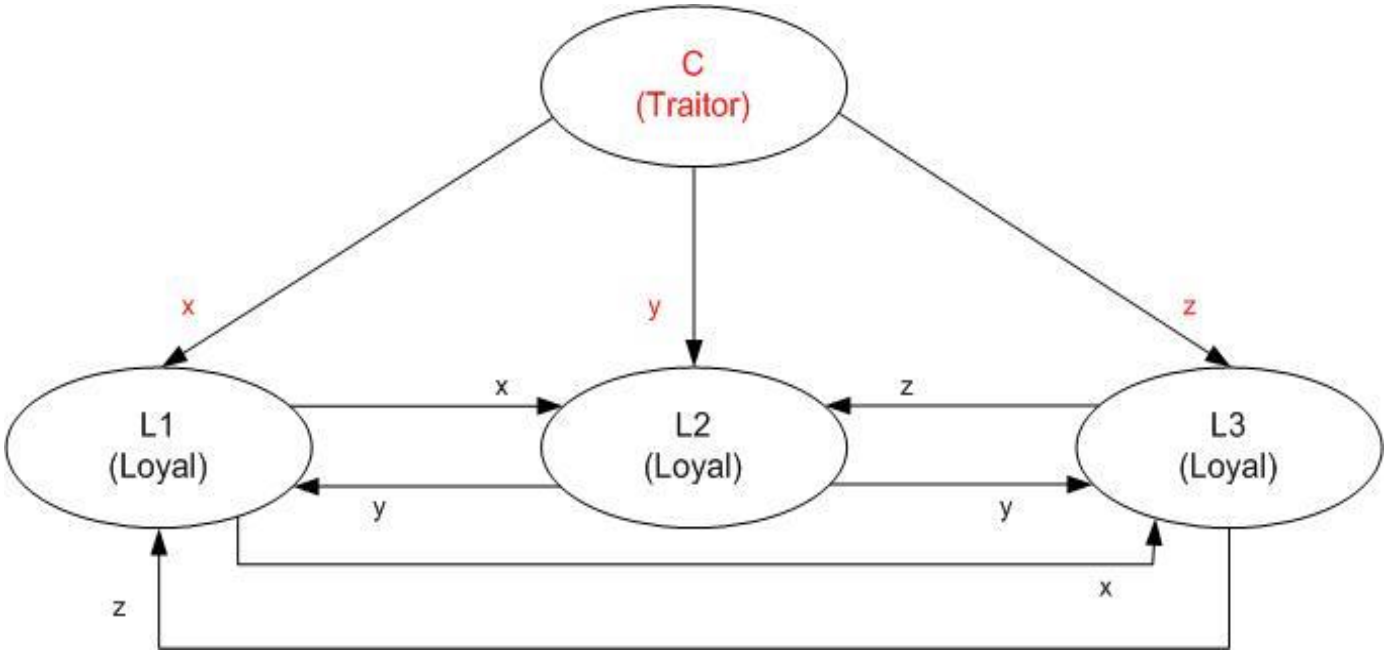
A3: The absence of a message can be detected.



n=4 generals; m=1 traitors

L2 calculates majority(ATTACK, ATTACK, RETREAT) = ATTACK

Solution with OM – Example



n=4 generals; m=1 traitors

L1, L2, L3 calculate majority(x, y, z)

Solution with Signed Messages

Simplify the problem by allowing generals to send unforgeable, signed messages

New assumption A4:

a) A loyal general's signature cannot be forged, and any alteration of the contents of his signed messages can be detected.

b) Anyone can verify the authenticity of a general's signature.

THANK YOU!!!