拜占庭将军问题

> 👉 拜占庭将军问题描述的是最困难的，也是最复杂的一种分布式故障场景，除了存在故障行为，还存在**恶意行为**的一个场景。

问题背景：拜占庭将军问题

起源

播报 编辑

拜占庭位于如今的土耳其的伊斯坦布尔，是东罗马帝国的首都。由于当时拜占庭罗马帝国国土辽阔，为了达到防御目的，每个军队都分隔很远，将军与将军之间只能靠信差传消息。在战争的时候，拜占庭军队内所有将军和副官必须达成一致的共识，决定是否有赢的机会才去攻打敌人的阵营。但是，在军队内有可能存有叛徒和敌军的间谍，左右将军们的决定又扰乱整体军队的秩序。在进行共识时，结果并不代表大多数人的意见。这时候，在已知有成员谋反的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，拜占庭问题就此形成[2]。

简介

播报 编辑

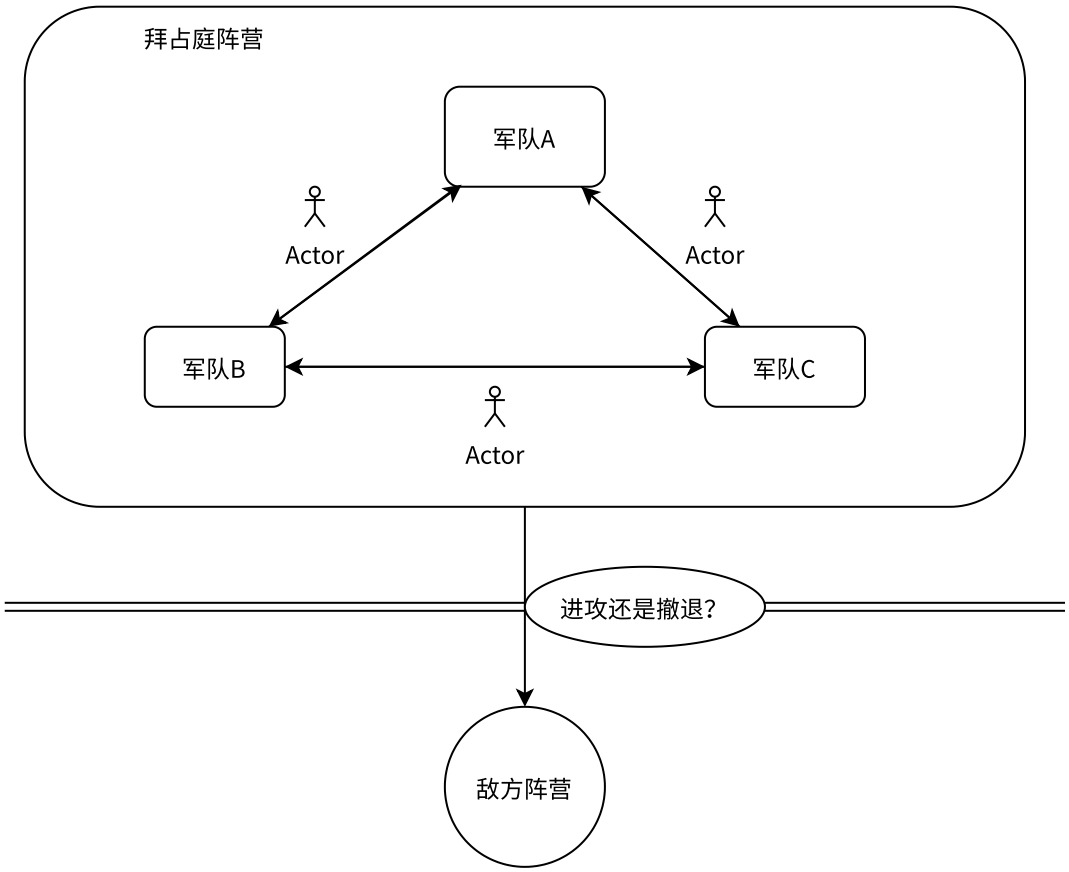
拜占庭将军问题是一个协议问题，拜占庭帝国军队的将军们必须全体一致的决定是否攻击某一支敌军。问题是这些将军在地理上是分隔开来的，并且将军中存在叛徒。叛徒可以任意行动以达到以下目标：欺骗某些将军采取进攻行动；促成一个不是所有将军都同意的决定，如当将军们不希望进攻时促成进攻行动；或者迷惑某些将军，使他们无法做出决定。如果叛徒达到了这些目的之一，则任何攻击行动的结果都是注定要失败的，只有完全达成一致的努力才能获得胜利[3]。

拜占庭假设是对现实世界的模型化，由于硬件错误、网络拥塞或断开以及遭到恶意攻击，计算机和网络可能出现不可预料的行为[3]。

拜占庭将军问题本质上就是一个共识问题：如何让各个军队的将军都达成同一个共识！

假设现在拜占庭阵营是由三个军队A、B、C组成，但是它们是部署在不同地方的，军队之间只能通过信使来传递消息；现在他们面临着一个问题——进攻vs撤退？

他们是同属一个阵营的，要共同进退，不然有可能会被敌方逐个击败的；要共同进退的前提就是三个军队的将军都达成共识。军队与军队之间通过信使来交换信息。



如果是正常情况下，三个军队只要互相知会一声，然后根据少数服从多数的原则，就可以达成共识了（一起进攻或者一起撤退）。

> A进攻，B进攻，C进攻 -> 进攻（3:0）
>
> A进攻，B进攻，C撤退 -> 进攻（2:1）
>
> A撤退，B撤退，C撤退 -> 撤退（3:0）
>
> A撤退，B撤退，C进攻 -> 撤退（2:1）

但是总存在异常情况的，万一其中一个军队叛变了呢?

“二忠一叛”

如果有一个军队判变了的话，最终就达成了“假共识”，比如：

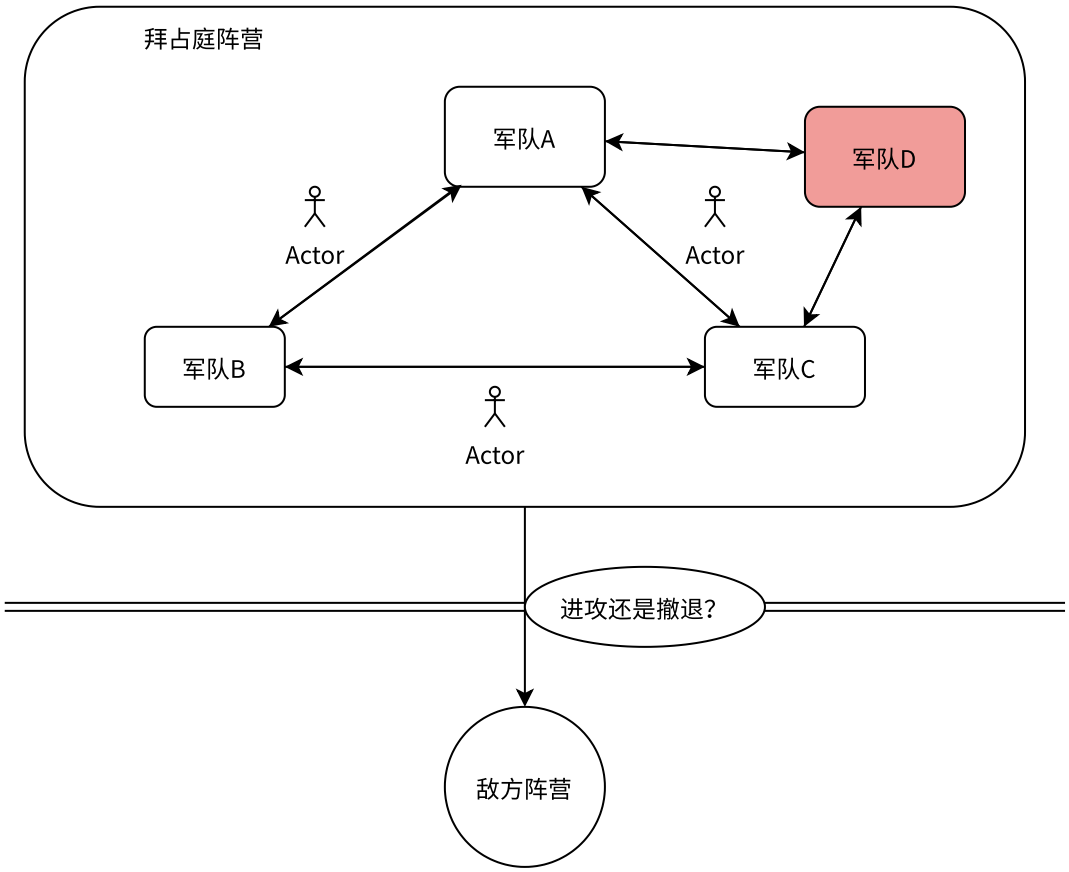
本来是AB支持进攻，C支持撤退，根据少数服从多数，最终的一致性方案是进攻的；但是假设B叛变了，将B支持进攻的消息传递成 B 支持撤退，这样就导致最后的整个作战方案的改变（有可能造成AC撤退了，但是B却傻乎乎地去进攻）

> A进攻，B进攻，C撤退 -> 进攻（2:1）
>
> A进攻，B~~进攻~~撤退，C撤退-> 撤退（2:1）

口信消息型拜占庭问题之解

“二忠一叛”的问题容易导致关键一票落在了叛徒手中（如果两个忠诚的持不同的态度，那叛徒传出来的那一票就显得尤为关键了，可以决定整个战局）

一个很容易想到的方法就是增加忠诚的个数，假设有四个信使分别代表四个军队，假设信使三个忠诚，一个判变：



首先, 对于口信消息(Oral message)的定义如下:

- A1. 任何已经发送的消息都将被正确传达;
- A2. 消息的接收者知道是谁发送了消息;
- A3. 消息的缺席可以被检测.

现在假设需要进行两轮作战信息协商，每一个军队在没有收到消息的时候，默认“撤退”。

第一轮：

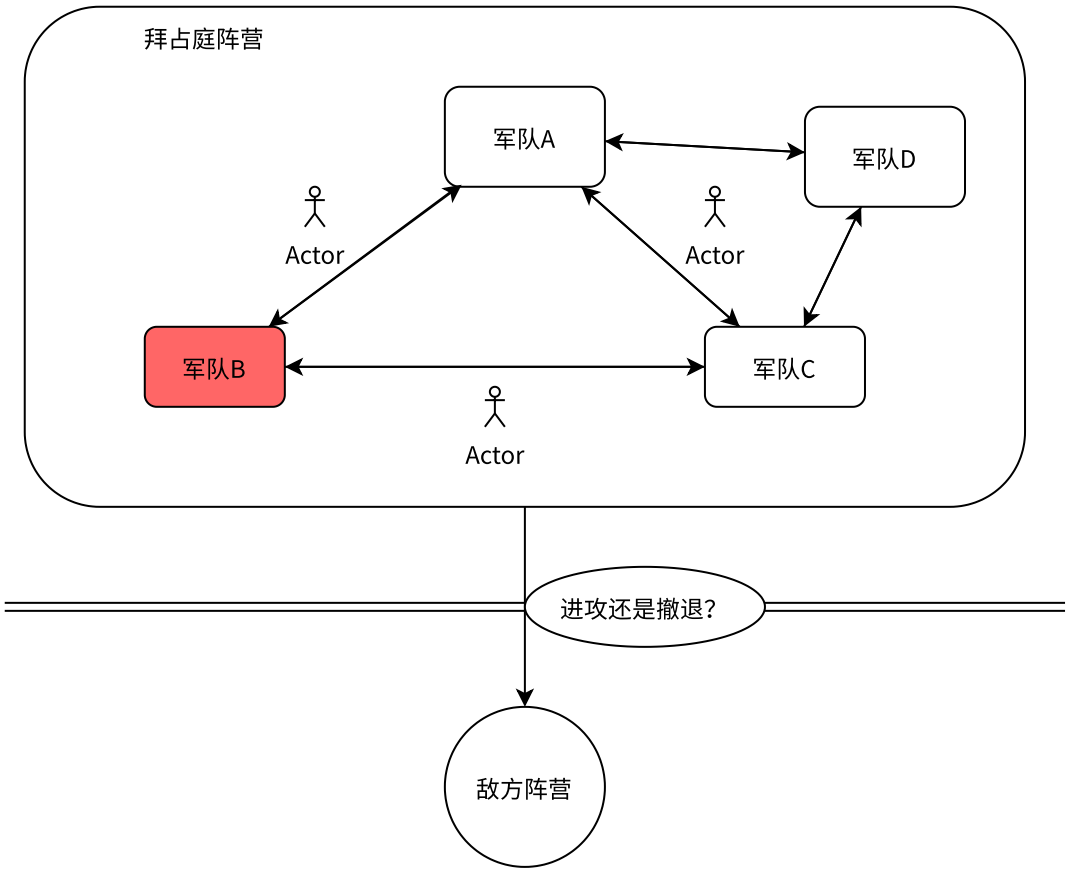
1. 先发送作战信息的将军作为指挥官，其他的将军作为副官；
2. 指挥官将他的作战信息发送给每位副官；
3. 每位副官，将从指挥官处收到的作战信息，作为他的作战指令；
4. 如果没有收到作战信息，将把默认的“撤退”作为作战指令。

第二轮：

1. 除了第一轮的指挥官外，剩余的 3 位将军将分别作为指挥官，向另外 2 位将军发送作战信息；

2. 然后，这 3 位将军按照“少数服从多数”，执行收到的作战指令。

现在假设“三忠一叛”分别指的是：ACD忠，B叛



假设忠将先发作战信息

假设A率先进入第一轮，以最高指挥官的身份发出了作战信息，则

> B收到：进攻
>
> C收到：进攻
>
> D收到：进攻

然后进入第二轮：

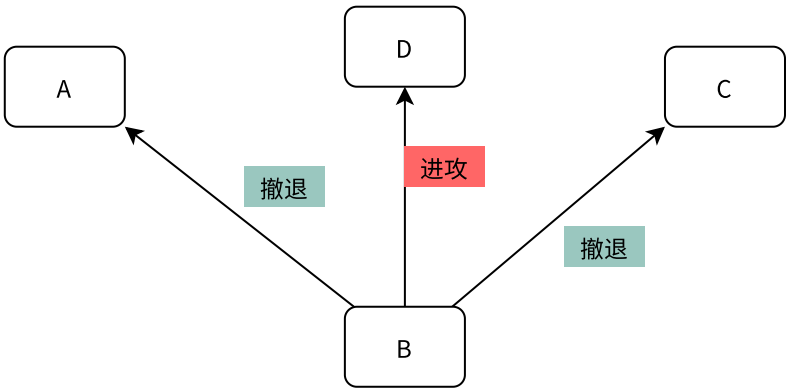
除A以外的将领，进行协商（B叛变）：

> B发出：~~进攻~~撤退，C：进攻，D：进攻 ->进攻（2：1）

最终作战方案和A提出的一致！

假设叛将先发作战信息

叛将为了扰乱作战计划，给不同的军队发出了不同的命令：



然后进入第二轮：

除B以外的将领，进行协商（B叛变）：

> A：撤退，C：撤退，D：进攻 -> 撤退（2：1）

可以看到哪怕有了叛将的捣乱，其他军队都是可以做出一致性作战方案的，而不会有的进攻，有的撤退。

签名消息型拜占庭问题之解

可以看到上述口信消息型是需要增加忠诚将领的，那么这一小节就介绍如何在不增加的前提下解决拜占庭问题！

口信消息型最大的缺点：无法单从消息本身判断消息真假！

这就引进了——签名消息型，很显然这种方法是可以通过消息本身辩证真伪的。（比如虎符）

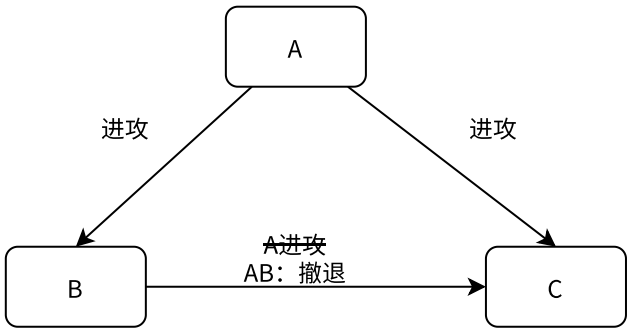
签名消息型的前提：

1. 忠诚将军的签名无法伪造，对其消息做任何更改都会被发现
2. 任何人都可以鉴别出忠诚将军的签名

假设忠将先发作战信息

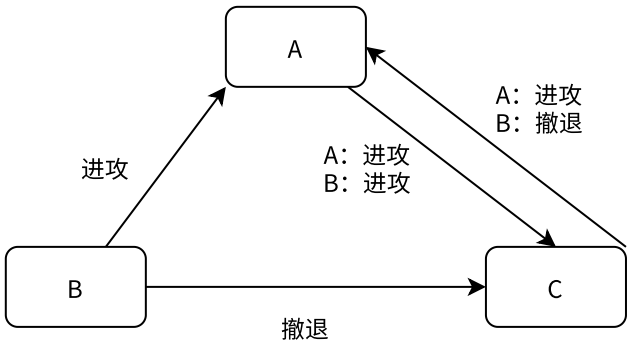
AC忠，B叛

假设A率先发出进攻的消息，B在收到消息之后，篡改了A的消息（进攻改为撤退）；但是因为是签名型的消息，所以 C 在收到 B 的消息之后就会发现 B 给他传递的消息是篡改过的。



假设叛将先发作战信息

叛将B给A发进攻，给C发撤退，最终A和C在协商过程中会发现B前后发出的指令不一致，也是会发现问题的。



总结：

拜占庭将军问题描述的是最困难的，也是最复杂的一种分布式故障场景，除了存在故障行为，还存在**恶意行为**的一个场景。

拜占庭问题到分布式领域的延伸：

1. 每一个将军都可以是一个计算机节点，忠诚的将军就是正常的节点，叛变的将军就是出现故障且会发送误导信息的节点
2. 信使失踪，消息中断，可以理解为通讯故障、信息丢失
3. 信使被替换，可以理解为通讯被中间人攻击，攻击者在恶意伪造信息和劫持通讯。