一、拜占庭将军问题的提出

拜占庭将军问题(The Byzantine Generals Problem)提供了对**分布式共识问题**的一种情景化描述, 由Leslie Lamport等人在1982年首次发表. 论文同时提供了两种解决拜占庭将军问题的算法:

- 口信消息型解决方案(A solution with oral message);
- 签名消息型解决方案(A solution with signed message).

> 拜占庭将军问题是分布式系统领域最复杂的**容错模型**, 它描述了如何在存在恶意行为(如消息篡改或伪造)的情况下使分布式系统达成一致

二、拜占庭将军问题的描述

拜占庭将军问题描述了这样一个场景:

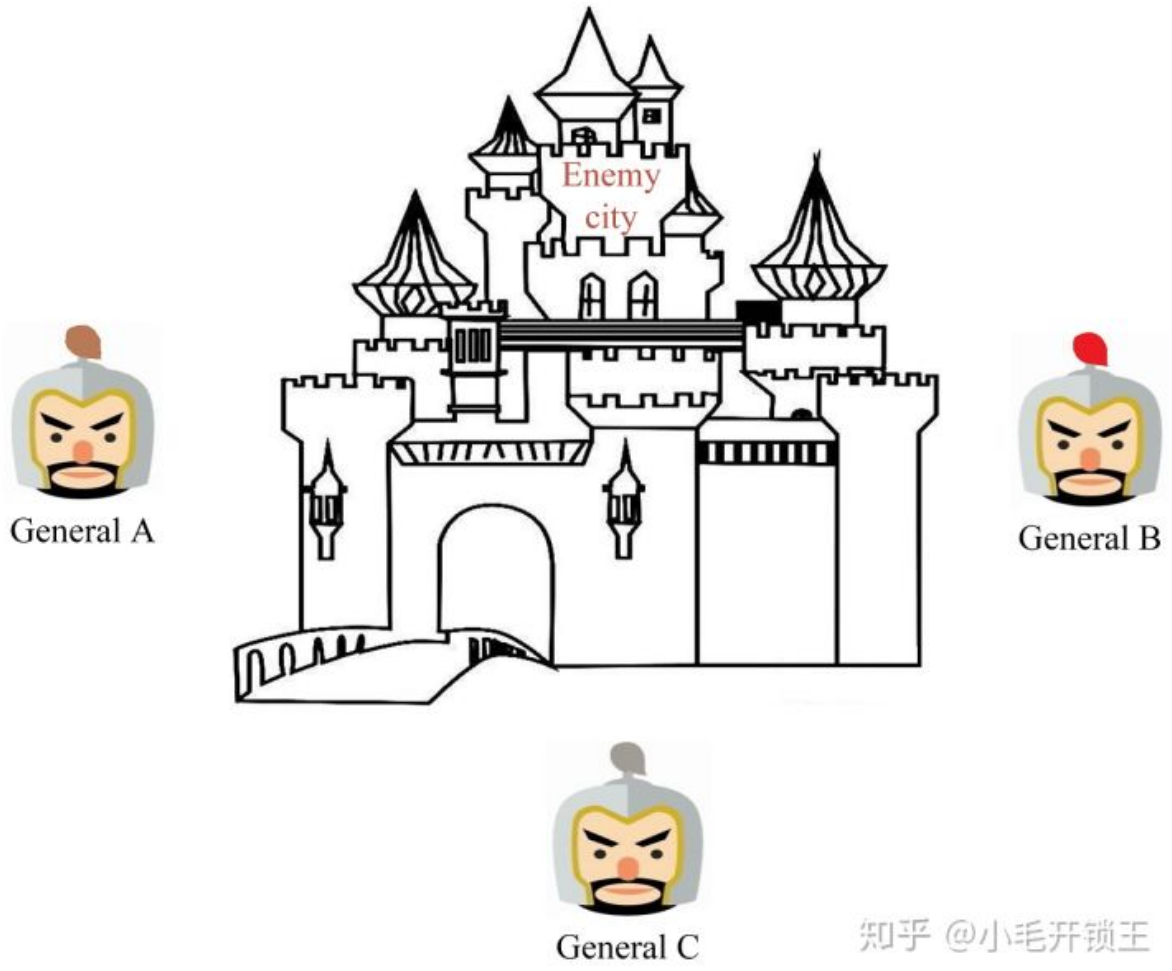

图1. 拜占庭将军问题

拜占庭帝国(Byzantine Empire)军队的几个师驻扎在敌城外, 每个师都由各自的将军指挥. 将军们只能通过信使相互沟通. 在观察敌情之后, 他们必须制定一个共同的行动计划, 如**进攻(Attack)**或者**撤退(Retreat)**, 且只有当**半数以上**的将军共同发起进攻时才能取得胜利. 然而, 其中一些将军可能是叛徒, 试图阻止忠诚的将军达成一致的行动计划. 更糟糕的是, 负责消息传递的信使也可能是叛徒, 他们可能篡改或伪造消息, 也可能使得消息丢失.

为了更加深入的理解拜占庭将军问题, 我们以**三将军问题**为例进行说明. 当三个将军都忠诚时, 可以通过投票确定一致的行动方案, 图2展示了一种场景, 即General A, B通过观察敌军军情并结合自身情况判断可以发起攻击, 而General C通过观察敌军军情并结合自身情况判断应当撤退. 最终三个将军经过投票表决得到结果为进攻:撤退=2:1, 所以将一同发起进攻取得胜利. 对于三个将军, 每个将军都能执行两种决策(进

攻或撤退)的情况下, 共存在6中不同的场景, 图2是其中一种, 对于其他5中场景可简单地推得, 通过投票三个将军都将达成一致的行动计划.

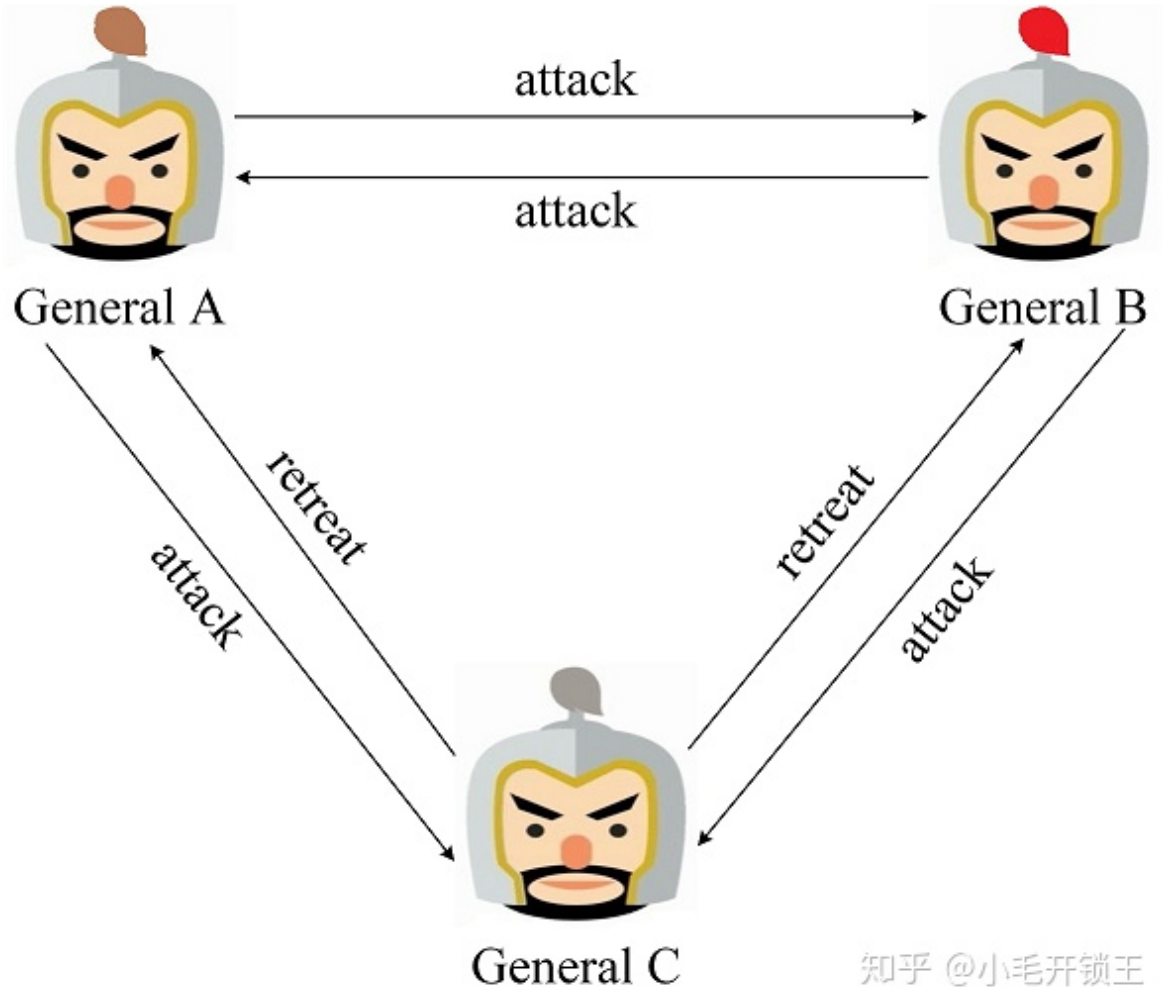

图2. 三个将军均为忠诚的场景

当三个将军中存在一个叛徒时, 将可能扰乱正常的作战计划. 图3展示了General C为叛徒的一种场景, 他给General A和General B发送了不同的消息, 在这种场景下General A通过投票得到进攻:撤退=1:2, 最终将作出撤退的行动计划; General B通过投票得到进攻:撤退=2:1, 最终将作出进攻的行动计划. 结果只有General B发起了进攻并战败.

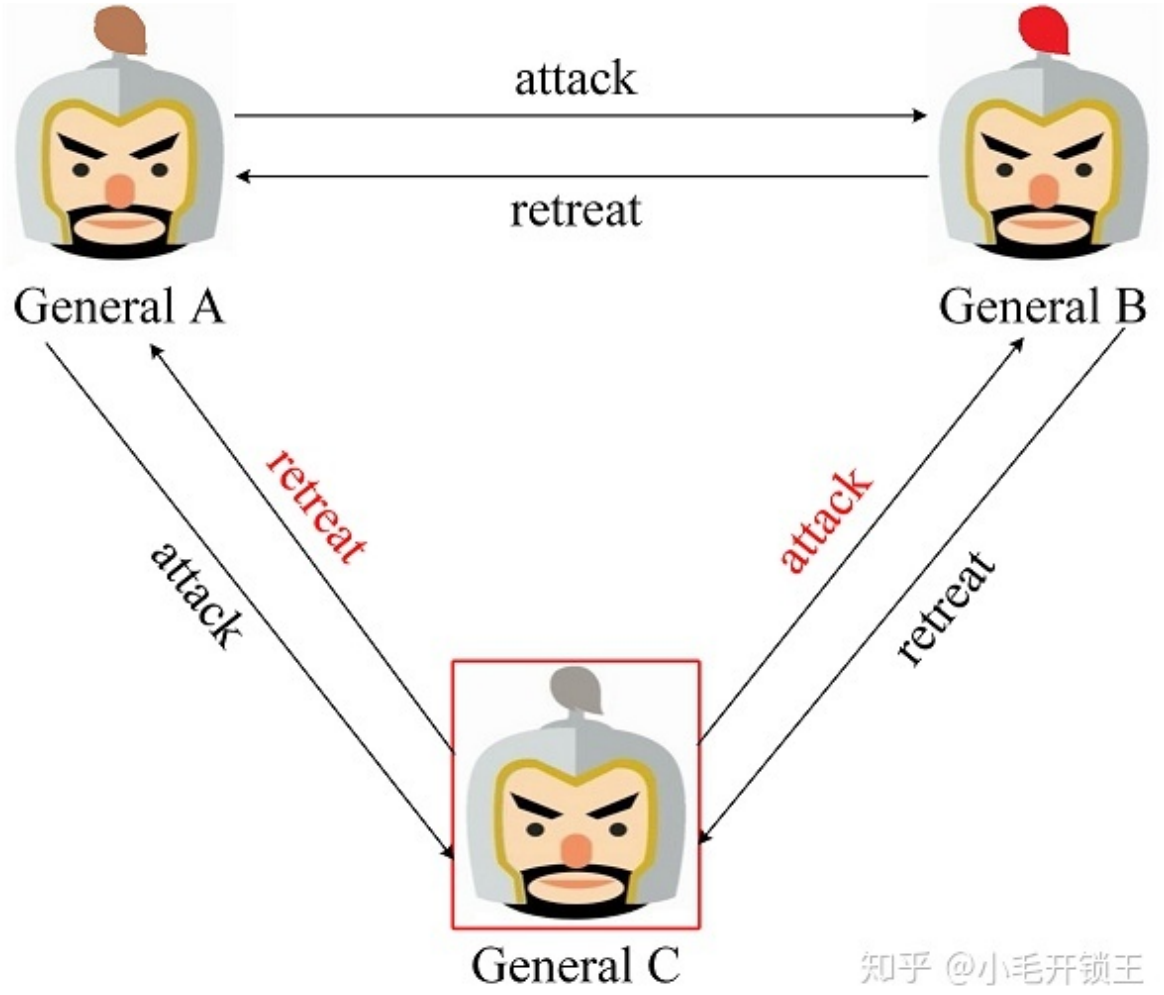

图3.二忠一叛的场景

事实上, 对于三个将军中存在一个叛徒的场景, 想要总能达到一致的行动方案是不可能的. 详细的证明可参看Leslie Lamport的论文. 此外, 论文中给出了一个更加普适的结论: 如果存在*m*个叛将, 那么至少需要*3m+1*(所有的将军数，包括叛徒节点自身)个将军, 才能最终达到一致的行动方案.

三、拜占庭将军问题的解决方案

Leslie Lamport在论文中给出了两种拜占庭将军问题的解决方案, 即口信消息型解决方案(A solution with oral message)和签名消息型解决方案(A solution with signed message).

3.1 口信消息型解决方案

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(不可篡改);
- A2. 消息的接收者知道是谁发送了消息(但是可以伪造身份进行发送);
- A3. 消息的缺席可以被检测.

基于口信消息的定义, 我们可以知道, 口信消息不能被篡改但是可以被伪造. 基于对图3场景的推导, 我们知道存在一个叛将时，必须再增加3个忠将才能达到最终的行动一致. 为加深理解, 我们将利用3个忠将1个叛将的场景对口信消息型解决方案进行推导. 在口信消息型解决方案中, 首先发送消息的将军称为指挥官, 其余将军称为副官. 对于3忠1叛的场景需要进行两轮作战信息协商，如果没有收到作战信息那么默认撤退. 图4是指挥官为忠将的场景, 在第一轮作战信息协商中, 指挥官向3位副官发送了进攻的消息; 在第二轮中，三位副官再次进行作战信息协商, 由于General A, B为忠将, 因此他们根据指挥官的消息向另外两位副官发送了进攻的消息, 而General C为叛将, 为了扰乱作战计划, 他向另外两位副官发送了撤退的消息. 最终Commanding General, General A和B达成了一致的进攻计划, 可以取得胜利.

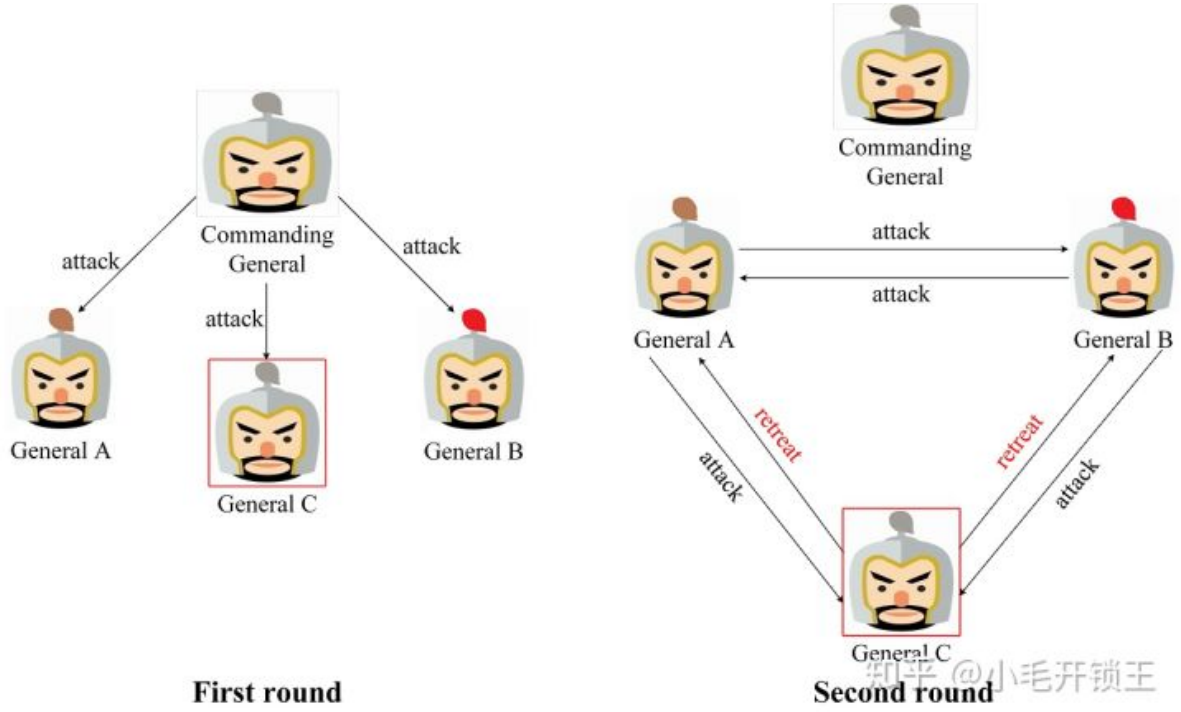

图4. 指挥官为忠将的场景

图5是指挥官为叛将的场景, 在第一轮作战信息协商中, 指挥官向General A, B发送了撤退的消息, 但是为了扰乱General C的决定向其发送了进攻的消息. 在第二轮中, 由于所有副官均为忠将, 因此都将来自指挥官的消息正确地发送给其余两位副官. 最终所有忠将都能达成一致撤退的计划.

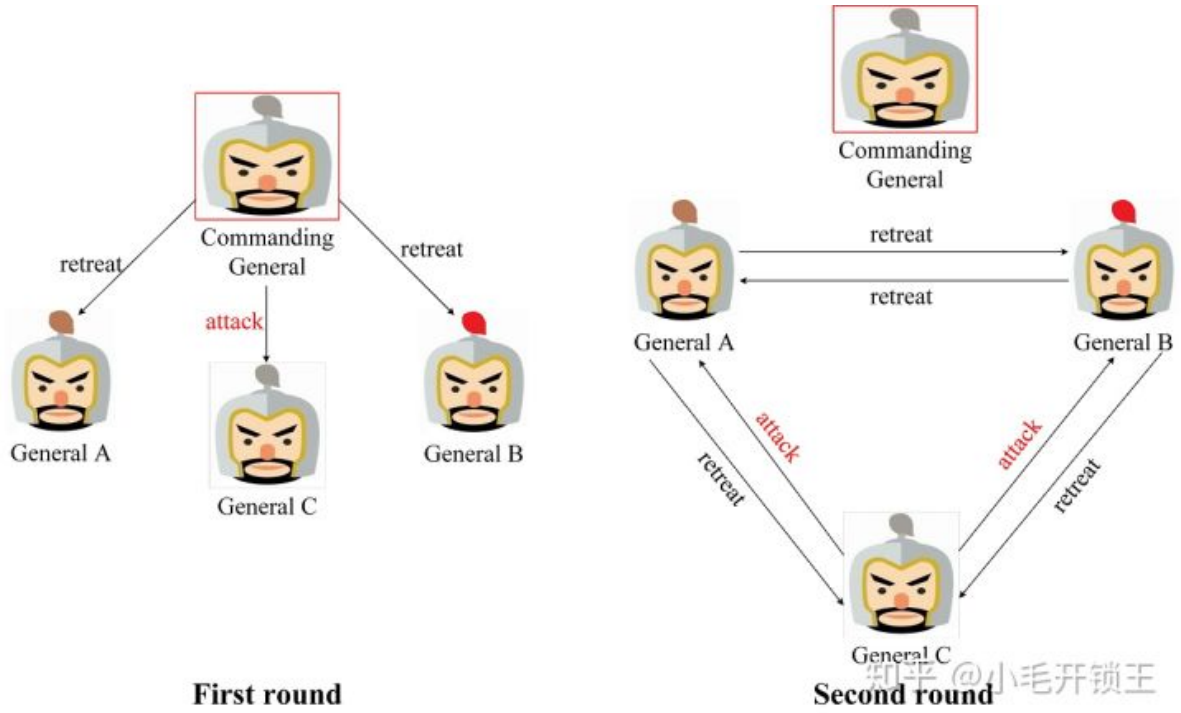

图5. 指挥官为叛将的场景

如上所述, 对于口信消息型拜占庭将军问题, 如果叛将人数为m, 将军人数不少于$3m+1$, 那么最终能达成一致的行动计划. **值的注意的是**, 在这个算法中, 叛将人数m必须是已知的, 且叛将人数m决定了递归的次数, 即叛将数m决定了进行作战信息协商的轮数, 如果存在m个叛将, 则需要进行$m+1$轮作战信息协商. 这也是上述存在1个叛将时需要进行两轮作战信息协商的原因.

3.2 签名消息型解决方案

同样, 对签名消息的定义是在口信消息定义的基础上增加了如下两条规则:

- A4. 忠诚将军的签名无法伪造，而且对他签名消息的内容进行任何更改都会被发现;
- A5. 任何人都能验证将军签名的真伪.

基于签名消息的定义, 我们可以知道, 签名消息无法被伪造或者篡改. 为了深入理解签名消息型解决方案, 我们同样以3三将军问题为例进行推导. 图6是忠将率先发起作战协商的场景, General A率先向General B, C发送了进攻消息, 一旦叛将General C篡改了来自General A的消息, 那么General B将将发现作战信息被General C篡改, General B将执行General A发送的消息.

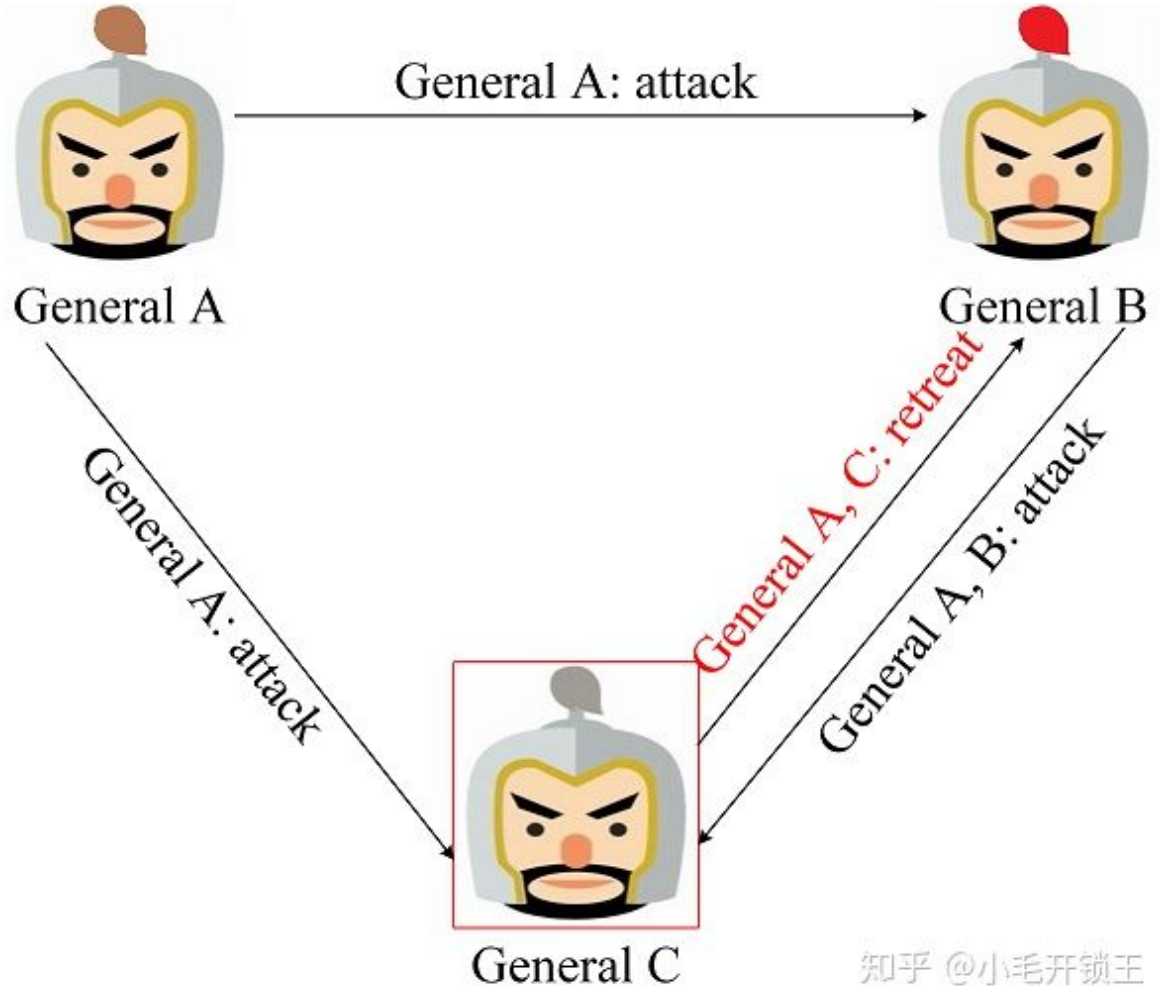

图6. 忠将率先发起作战协商

图7是叛将率先发起作战协商的场景, 叛将General C率先发送了误导的作战信息, 那么General A, B将发现General C发送的作战信息不一致, 因此判定其为叛将. 可对其进行处理后再进行作战信息协商.

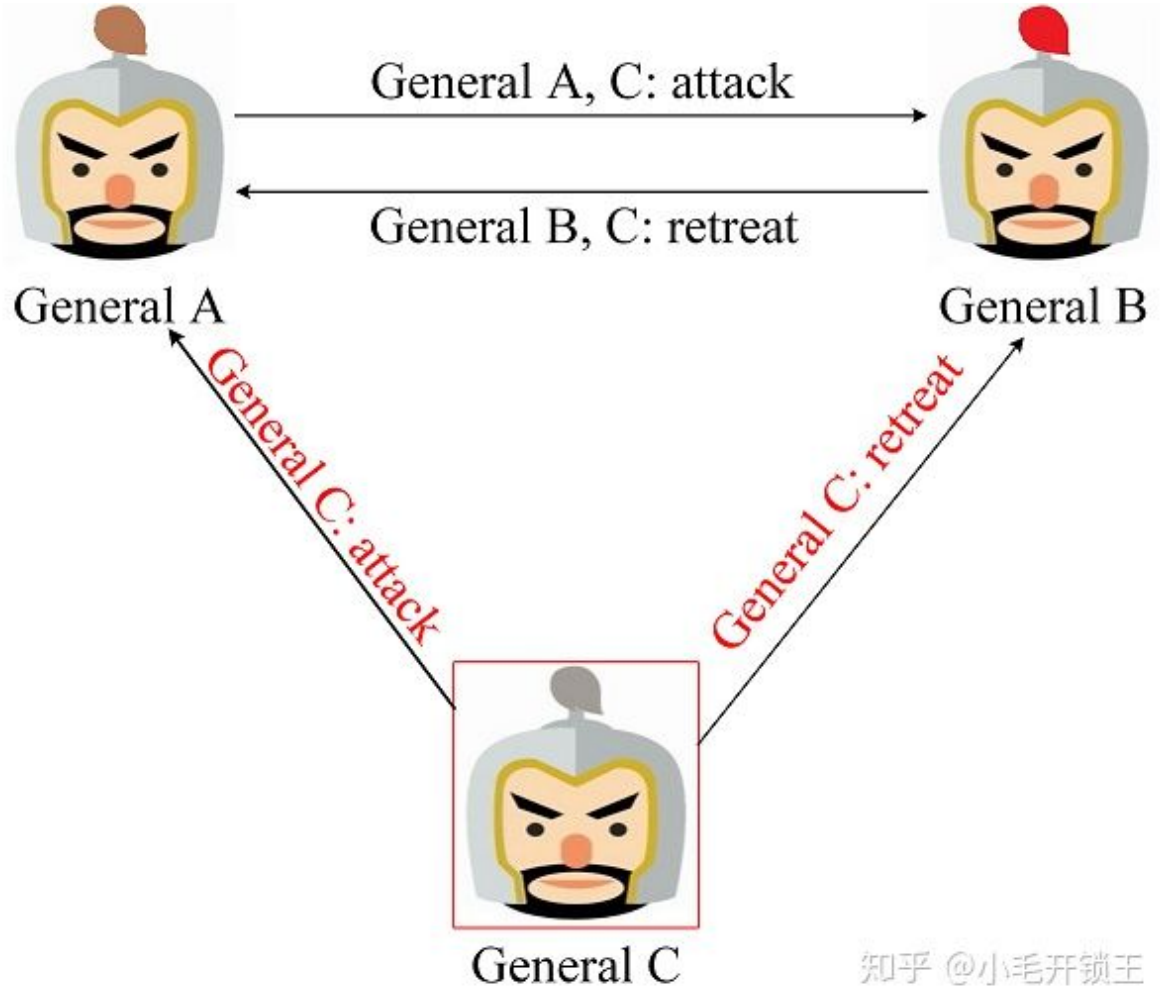

图7. 叛将率先发起作战协商

> 签名消息型解决方案可以处理任何数量叛将的场景.

四、总结

在分布式系统领域, 拜占庭将军问题中的角色与计算机世界的对应关系如下:

- 将军, 对应计算机节点;
- 忠诚的将军, 对应运行良好的计算机节点;
- 叛变的将军, 被非法控制的计算机节点;
- 信使被杀, 通信故障使得消息丢失;
- 信使被间谍替换, 通信被攻击, 攻击者篡改或伪造信息.