技术交底文件(发明或实用新型)

发明名称：一种决策辅助型的分布式网络共识算法

联系人电话：17631991378

联系人： 岳天一

联系人地址：

一、详细介绍技术背景，并描述已有的与本发明最相近似的实现方案

随着互联网技术的不断发展，分布式网络技术在网络通信中扮演着越来越重要的角色，逐渐成为了计算机领域研究的热点之一。分布式系统是指由多个计算机节点组成的系统，这些节点通过网络连接进行通信和协作，以完成特定的任务。分布式网络通信技术允许多个计算机之间共享资源和信息，它们可以在任何地方连接和通信，无需一个中心节点来控制整个网络。在分布式网络中，网络表决的一致性是最重要的问题之一，一致性指的是分布式系统中多个物理节点的处理结果对外呈现的状态一致性，不仅包括结果的正确性，也包括结果的状态。例如，所有节点都达成失败状态也是一种一致性。共识算法的提出就是为了解决分布式系统节点间的数据一致性问题，让各节点协同工作，看起来就像一个单独的、高可靠的状态机。依据对故障的容忍能力不同，分布式共识算法分为拜占庭容错和非拜占庭容错两类。拜占庭错误最早由 Lamport 提出，描述了最困难的分布式故障场景，除丢失消息、消息重复、伪造消息的情况外，还存在节点随机作恶，它们可能会发送错误的信息、篡改或伪造信息，导致系统产生错误的决策。

常见的 BFT 算法有 PBFT，是一种基于消息传递的一致性算法，用于分布式系统。它的核心思想是通过预准备、准备和确认三个阶段来达成一致性。在预准备阶段，主节点接收到客户端的请求后生成一个预准备信息并发送给其他节点；在准备阶段，每个节点收到预准备信息后复制请求并发送给其他节点，同时将结果打包成一个准备信息发送回主节点；在确认阶段，主节点收集到一定数量（N/2+1，假设总节点数为 N）的同意结果后，将这个信息发送给所有节点，节点执行请求并返回结果给客户端。回复阶段，所有节点将执行结果发送回主节点，主节点整合所有节点的结果并将最终结果返回给客户端。PBFT 能够容忍不超过一半的故障节点而保证系统正常运行，但需要整个系统停机并进行重启来处理故障节点。

二、上述现有技术的缺点是什么？是具体什么原因导致会有上述缺点？

现有技术的缺点：

1. 缺乏主动性。PBFT 算法依赖于外部客户端的请求来触发其流程，这导致其缺乏

自主性，并可能易受到恶意节点的攻击。

2. 大规模网络性能瓶颈。PBFT 旨在实现状态复制，其中节点转发消息以实现该消息的一致同步。然而，在处理大规模网络和动态拓扑时，PBFT 可能会遇到性能瓶颈，这主要是由于消息的广播性质。

3. 拓扑变动适应性差。PBFT 对于网络拓扑的变动（如节点加入或离开）反应较慢，这可能导致在动态环境中的一致性问题。

4. 节点作恶行为难以检测。在 PBFT 中，节点作恶行为可能体现为对接收到消息的不诚实转发。然而，在决策过程中，节点作恶行为（故障节点）可能更为复杂，表现为对真实判断结果的静默或歪曲，这使得检测和应对这种行为更为困难。

综上所述，当前的分布式网络共识方法技术虽然在解决分布式网络中的问题方面具有很大的优势，但是仍然存在一些局限性和不足，需要进一步改进和完善。

三、针对上述现有技术的缺点，说明本发明的目的（客观评价）：

❖ **发明目的：**

本发明的目的是设计一种决策辅助型的分布式网络共识算法，提高算法的主动性和安全性，有效降低恶意节点对分布式网络表决过程的影响，提高网络的安全性和稳定性。

本发明引入自主触发状态更新的机制，以提高算法的主动性，该机制允许节点在无需外部请求的情况下自主触发状态更新，保证网络状态及时更新，提高网络可用性。本发明引入新的消息广播策略，以降低网络负载，缓解大规模网络性能瓶颈问题。该策略采用去中心化的广播方式，减轻网络负担的同时增强网络鲁棒性。本发明引入新的主节点确认机制，以提高对网络拓扑变动的适应性，该机制采用独特的选举方式，保证在节点快速发现拓扑变动并相应地调整其状态的情况下，确保网络一致性并增强对节点作恶行为的检测和应对能力。本发明的技术方案不仅适用于特定领域，还可以广泛应用于各种需要分布式网络表决的场景。例如，区块链技术、P2P 网络、分布式计算等领域都可以从本发明中受益。

综上所述，该分布式网络共识算法的发明目的是为了提供更为有效且安全的网络决策辅助，从而提高分布式系统的可用性和可靠性，通过自主触发状态更新的机制、独有的消息广播策略和主节点选举放方式来实现该目标。

四、本发明技术方案的详细阐述（发明内容）

4.1 本发明要解决的技术问题是什么，该技术是属于哪个技术领域

技术领域：网络空间安全

本发明所要解决的技术问题：

（1）分布式网络表决方案：通过多阶段共识算法使网络中的节点能够自主触发状态更新，以确保网络状态及时更新并降低恶意节点的影响。

（2）降低恶意节点对分布式网络表决过程的影响：通过质询-拓扑更新阶段，使网络中的节点能够快速发现拓扑变动并相应地调整其状态，以确保网络的一致性并增强对恶意节点的检测和应对能力。

4.2 本发明技术实现的具体实施例

总体架构：

本发明提出一种决策辅助型的分布式网络共识方案，方案流程如图 1 所示。

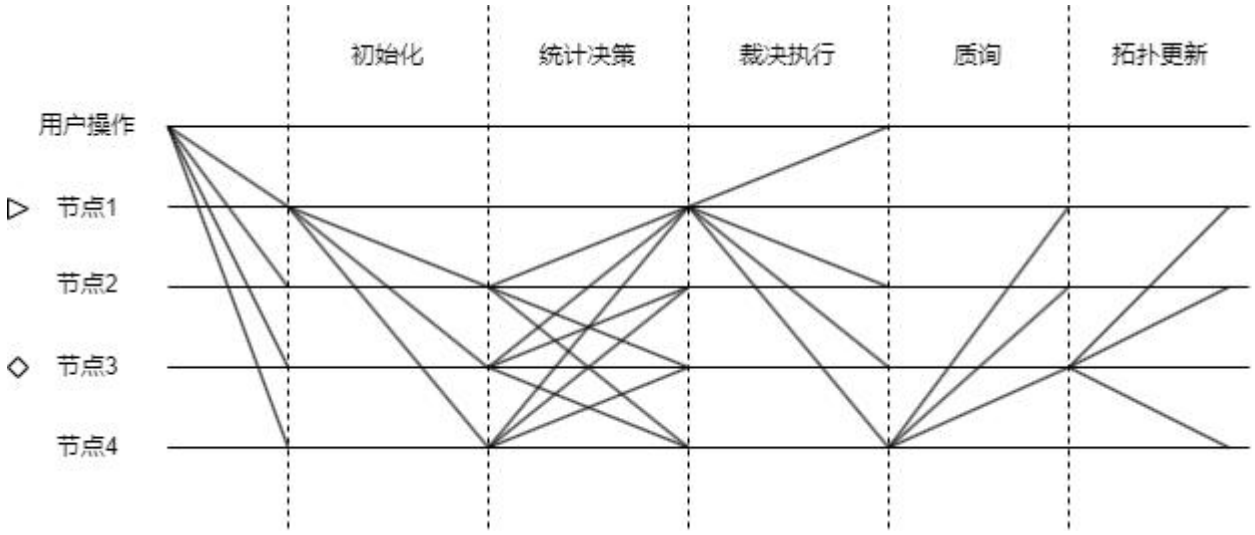

图 1 决策辅助型的分布式网络共识方案示意图

本发明装置的运行示例：

该方案将所有节点分为四种类型：主节点p_o'、普通节点、质询节点和法官节点p_o。主节点负责初始化协议并向其他节点广播；普通节点根据本地的逻辑监控用户行为，并在发现输入行为时检索相应的事件并向其他节点广播其本地的判断结果；质询节点可以为任意节点，对主节点的结果发起质询，其他节点可以参与投票；法官节点收集质询的结果并执行最终的拓扑更新输出。

主节点的选举采用随机数 random mod |n|的方式进行确保公平性、安全性，其中 random 为生成的随机数，|n|为可用节点数量。每个节点都有负责实时监控用户行为的模块，当监控模块接收到用户行为消息后，该节点会根据消息内容自主触发本机状态更新{event_id : [⟨p_i, r_i⟩]}，其中 event_id 为当前事件编号，p_i为当前本机节点编号，r_i为本机判断结果。

主节点在接收到用户行为消息后，将触发协议并将消息内容与本地判断结果进行广播。这些广播内容会通过 P2P 网络发送给其他节点。其他节点在接收到主节点的初始化消息后，会将接收到的行为消息及相应事件的本地判断结果进行广播，广播内容会通过 P2P 网络发送给其他节点。

主节点$p_o^{'}$负责收集所有节点发送的广播内容$\{\text{event_id} : [\langle p_o^{'}, \mathrm{r}_1\rangle, \langle \mathrm{p}_2, \mathrm{r}_2\rangle, \langle \mathrm{p}_3, \mathrm{r}_3\rangle, \langle \mathrm{p}_4, \mathrm{r}_4\rangle]\}$，并根据少数服从多数的原则进行决策，根据统计结果，主节点$p_o^{'}$会对用户操作执行裁决，并广播最终判断结果$\{\text{event_id} \rightarrow \text{final_res}\}$。如果某节点$\mathrm{p_o}$认为主节点$p_o^{'}$的判定结果 final_res 与本地判断$\mathrm{r_i}$不一致，可以调用质询模块，将质询内容、质询目标和质询理由（本地收集的其他节点广播内容）进行广播。

若发生质询，将采用 random mod |n|方式选举出节点$\{\mathrm{p_i} \mid \mathrm{p_i} \notin \{\mathrm{p_o}, p_o^{'}\}\}$ 为法官节点，该节点将根据本地采集的所有节点状态信息来判断恶意节点。一旦确定恶意节点的身份，法官节点将调用清洗模块完成拓扑结构的更新，进行节点替换并将结果进行广播，通过这种机制，所有节点都能够同步网络状态的状态更新变动。

本发明装置的组成：

本发明装置由（1）行为监控模块、（2）状态更新模块、（3）统计决策模块、（4）质询与清洗模块共同构成。

（1）行为监控模块：该模块负责在分布式网络中实时监控用户的行为，并能够对这些行为进行分析和处理。它可以检测和记录用户的行为模式和异常行为，如频繁的重复请求、恶意攻击等。这些监控数据不仅用于后续的决策参考，而且可以与其它模块共享，以提高网络的安全性和稳定性。

（2）状态更新模块：该模块负责确保每个节点能够根据接收到的消息自主触发状态更新并进行广播，每个节点都会接收来自其他节点的消息，并根据这些消息调整自己的状态。通过这种机制，网络中的所有节点都能够保持同步的状态更新，从而及时反映网络状态的变动。

（3）统计决策模块：该模块负责所有节点根据收集的数据，按照少数服从多数的原则进行结果统计。当收集到超过一半数量的同一类型结果时，主节点将执行最终判断输出。这种决策制定方式可以大大提高网络表决过程的安全性和主动性，同时降低恶意节点的影响。

（4）质询与清洗模块：该模块负责对节点发起质询的节点进行处理。如果存在节点对主节点的结果发起质询，其他节点可以参与投票。如果多数节点认为主节点存在问题，则进行节点清洗。通过这种机制，可以增强分布式网络表决系统的可用性和可靠性，同

时优化网络的性能和效率。

4.3 本发明技术方案带来的有益效果（与现有技术相比较，本发明有哪些优点，每项优点各是因为本发明采用了什么不同于现有技术的技术手段来实现的？可结合发明内容简单介绍）

有益效果：

（1）更高效的分布式决策方案：本发明的技术方案采用分布式网络架构、巧妙的防御机制和优化算法设计等技术手段，提供了一种高效的分布式决策方案，大大提高了信息传播的速度和效率。

（2）更强的抗攻击能力：本发明质询模块保证了节点的可靠性，有效保护了系统的安全性，可以在更短的时间内发现并限制恶意节点的影响。。

（3）更高的鲁棒性：本发明技术方案具有较高的鲁棒性，能够有效地抵御恶意攻击。在现有技术中，一旦受到恶意攻击，系统往往会出现崩溃或数据损坏的情况。而本发明通过设计巧妙的防御机制，能够在受到恶意攻击时迅速进行自我保护和修复，保证系统的正常运行。

五、本发明的关键点和欲保护点是什么？依每个关键点和欲保护点，本发明与现有技术的实施方案各是怎样，二者有哪些不同之处？（本段应简单介绍，两三个自然段即可，重点放在把本发明的关键技术与现有技术作比对，并做客观评价；该比对应是具体技术手段的比对，而不能仅仅是功能上的比对）

关键点及欲保护点：

1. 分布式决策共识算法：本发明通过将所有节点分为四种类型：主节点、普通节点、质询节点和法官节点，并设计算法流程有效降低恶意节点对分布式网络表决过程的影响。相较于现有技术，本发明的实施方案具有更高的的主动性和安全性，有效限制恶意节点对分布式网络决策过程的影响。

2. 质询和裁决拓扑更新机制：本发明中的质询与清洗模块使得任意节点的异常识别具有动态自适应能力。与现有技术相比，有助于防止恶意节点长时间逃避检测，在出现争议时提供更准确的判断。

3. 主节点、法官节点的随机选举机制：本发明通过随机选举机制完成分布式网络统计决策，增加恶意节点操纵选举结果的难度，进一步提高了安全性和稳定性。相较于现有技术，本发明的实施方案具有更强的抗攻击能力。

在本发明与现有技术的实施方案中，本发明针对分布式网络表决过程中的恶意节点问题，通过自主触发状态更新的机制、独有的消息广播策略和主节点、法官选举，实现了更为有效且安全的网络决策辅助算法。与现有技术相比，本发明在技术手段上进行了创新，实现了更高的安全性和稳定性，具有显著的优势。

六、专业术语

分布式网络，统计决策，拜占庭将军问题