面向无人机集群的双层分组拜占庭容错算法

陈宇，贾连兴
（国防科技大学信息通信学院，湖北 武汉 430073）

摘 要：针对区块链技术应用于无人机集群通信时存在的通信复杂度高、稳健性差等问题，提出了一种双层分组拜占庭容错算法。根据无人机的编队结果对节点进行分组，并从每组选取一部分高信誉节点组成委员会，其他节点作为共用节点，形成双层分组共识结构。使用门限签名技术降低通信复杂度，仅通过委员会节点与其他分组节点通信，减少分组间通信次数，使平均通信时延大幅度减小。分层结构使主节点身份隐匿于委员会之中，降低了主节点被敌方自适应攻击的风险，提升了系统的稳健性。实验结果表明，所提算法相比于对比算法，共识过程的时延显著降低，同时能够有效保证系统的活性。

关键词：无人机集群；拜占庭容错；共识算法；双层分组结构
中图分类号：TN95
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022021

Two-layer grouped Byzantine fault tolerance algorithm for UAV swarm

CHEN Yu, JIA Lianxing
College of Information and Communication, National University of Defense Technology, Wuhan 430073, China

Abstract: To reduce the communication complexity and improve the robustness of blockchain network, a two-layer grouped Byzantine fault tolerance algorithm for unmanned ariel vehicle (UAV) swarm was proposed. First, nodes were divided into several groups according to the formation results of UAV swarm. A portion of high-reputation nodes were selected from each group to form a committee, and other nodes were used as shared nodes. Threshold signature techniques were employed to reduce communication complexity. In that way, nodes from other groups only needed to communicate with the committee nodes of the current group, thus greatly reducing the average communication delay. In addition, the hierarchical structure, which made the identity of the primary node hidden in the committee, reduced the risk of being adaptively attacked by the Byzantine nodes and improves the robustness of the system. Experimental results demonstrates that the proposed algorithm significantly reduces the delay of the consensus process and can effectively ensure the aliveness of the system compared with the comparison algorithm.

Keywords: UAV swarm, Byzantine fault tolerance, consensus algorithm, two-layer grouped structure

0 引言

随着人工智能技术的飞速发展，无人化设备将发挥重要作用。其中，无人机作战，尤其是无人机集群协同作战，将成为未来战争中的重要作战形式[1]。然而，近年来无人机被入侵，失去控制的案例层出不穷[2]。一方面，复杂的网络环境使无人机集群通信安全面临严峻挑战。另一方面，无人机集群具有一定自主性和灵活性，需要进行大量信息交换且高度依赖信息的真实可靠性，存在较大安全隐患。新

收稿日期：2021−09−01；**修回日期**：2021−11−01
通信作者：贾连兴，jlx@163.com
基金项目：国家自然科学基金资助项目（No.62102423）
Foundation Item: The National Natural Science Foundation of China (No.62102423)

兴起的区块链技术[3]具有公开透明、不可篡改、可以追溯等特点，可以防止敌方使用错误的信息或指令干扰、控制无人机集群，为提升无人机集群安全性能提供了有效途径。

共识算法[4]作为区块链的核心技术，其性能是影响区块链一致性、安全性和稳定性的重要因素。目前，区块链的共识算法可以分为非授权共识算法和授权共识算法两大类[5]。非授权共识算法是指在任意节点都可以自由加入或退出的网络中运行的分布式一致性算法，通常应用于公有链。典型算法包括基于工作量证明的共识算法（PoW, proof of work）[6]、基于权益证明的共识算法（PoS, proof of stake）[7]、基于授权股份证明的共识算法（DPoS, delegated proof of stake）[8]以及混合共识算法[9-11]。上述算法具有很好的可扩展性，且节点数量越多，攻击区块链的难度越大。但这些算法主要为加密数字货币设计，需要花费大量算力或建立虚拟资产体系。授权共识算法则是指在节点需进行身份认证后准入的网络中运行的分布式一致性算法，通常应用于联盟链和私有链。典型算法为实用拜占庭容错（PBFT, practical Byzantine fault tolerance）协议[12]，该算法通过节点间互相通信去除拜占庭节点恶意行为的影响，同时使用预准备、准备、承诺 3 个阶段保证节点的一致性。然而，节点间两两交互使 PBFT 的通信复杂度高达 $O(n^2)$，当节点数量较多时易导致网络堵塞，可扩展性较差。为了降低 PBFT 的通信复杂度，文献[13]提出了一种可扩展拜占庭容错（SBFT, scalable Byzantine fault tolerance）协议，该协议使用门限签名技术将共识过程的通信复杂度降低为 $O(n)$。文献[14]在 SBFT 的基础上提出了并行流水线处理以及线性视图转换方法，将 SBFT 视图转换过程的通信复杂度从 $O(n^2)$降低到 $O(n)$，进一步提升了共识效率。但在上述方法中，区块链主节点的身份是公开的，极易受到敌方发起的分布式拒绝服务攻击，且门限签名的合成与转发高度依赖主节点的可靠性，若主节点为拜占庭节点或被敌方控制将危害系统安全性。针对这一问题，文献[15]采用环签名技术隐匿提案生成过程中主节点的身份，模糊敌方攻击目标。同时，通过在多轮投票中合成代表法定人数投票意愿的门限签名，提升共识算法的稳健性。但该方法为了防止主节点作恶，必须选择至少 f+1 个最小共识单元，使通信复杂度提升为 $O((f+1)n)$。文献[16]提出了一种基于 Raft 集群的拜占庭容错方法，该方法首先选取少量节点组成委员会，其余节点被分为 k 组，委员会节点使用 PBFT 共识，然后将共识结果转发给各组节点，每组节点中使用 Raft 共识保持一致性。该方法引入 Raft 共识机制使通信复杂度降低为 $O(n/k+k^2)$，同时引入了监督机制实现拜占庭容错，该方法的分组思路为本文提供了借鉴，本文在此基础上结合无人机集群特点对共识算法进行了进一步优化改进。

综上，对于拜占庭容错协议的研究主要分为 2 个方向：第一个方向是降低共识过程的通信复杂度和系统开销；第二个方向是提升系统的抗攻击能力以及稳健性。但目前尚缺乏同时兼顾通信复杂度与系统稳健性的方法，且上述研究具有较高的通用性，未针对特定场景或应用进行优化，算法性能仍有较大提升空间。为此，本文根据无人机集群的特点以及需求，深度优化 PBFT，提出一种面向无人机集群的双层分组拜占庭容错（TLGBFT, two-layer grouped Byzantine fault tolerance）算法，在保障低通信复杂度的前提下提升系统稳健性。所提算法主要从以下几个方面进行了优化。

首先，无人机集群协同执行任务过程中通常会进行编队，本文采用分组思想，根据无人机编队结果对区块链节点进行分组。每组仅选取少量节点组成委员会与其他组节点进行通信，降低通信复杂度。一般地，同编队中无人机通信的质量高于不同编队无人机互相通信的质量，减少不同编队无人机之间的通信次数可以降低平均通信时延。

其次，为了避免主节点受到敌方的分布式拒绝服务攻击，导致共识过程失败，本文采用分层共识结构。每组的委员会节点作为第一层共识节点，通过第一轮共识产生初始区块。各组其他节点一起作为第二层共识节点，对初始区块进行第二轮共识。第二层共识节点不参与第一轮共识过程，主节点身份藏匿于委员会节点之中，同时采用随机轮值的方式更换每一轮发起提案的主节点，降低主节点被攻击的概率。且第二层共识节点中包含不同编队无人机对应的节点，即使某个编队中超过 1/3 以上的无人机被敌方入侵，也可以通过其他编队无人机对应的诚实节点达成共识，提升了系统的稳健性。

最后，在本文提出的双层分组共识结构下，各编队无人机可以同时发布不同的区块，进行流水线式的并行处理，进一步提升了无人机集群系统的共识效率。

1 系统模型

本文提出的面向无人机集群的双层分组共识结构如图 1 所示，其中，每个编队的无人机对应一组节点，这些节点从功能上分为 2 种类型，分别是委员会节点和普通节点。委员会节点从每组的高信誉节点列表中随机选取。各组委员会节点负责处理对应编队无人机提交的提案请求，通过第一轮共识生成初始区块。每组剩余的节点，即普通节点，作为共用节点，对所有初始区块进行确认，通过第二轮共识产生最终区块。

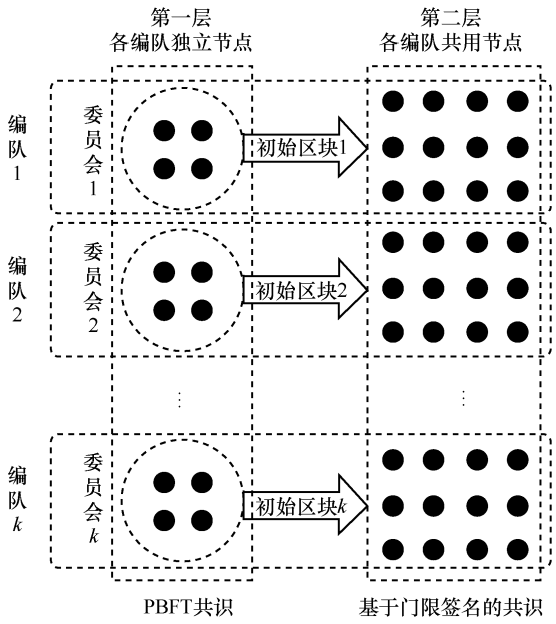

图 1 面向无人机集群的双层分组共识结构

本文使用拜占庭容错模型对系统进行建模，系统中节点总数为 n，其中，每组委员会都包含 c 个节点，第 i 组委员会节点集合表示为 $\{p_{i1}, p_{i2}, \cdots, p_{ic}\}$，共用节点集合表示为 $\{p_1, p_2, \cdots, p_m\}$。为了保障系统的安全性和活性，必须满足条件 $c+m \geqslant 3f+1$[5]。其中，f 为系统中拜占庭节点的个数。

在通信复杂度方面，系统的通信开销来自第一轮共识过程中委员会节点之间的互相通信以及第二轮共识过程中委员会节点与共用节点之间的信息交互。通常，委员会节点个数较少，远少于共用节点个数，即 $c \ll m<n$，因此系统的通信复杂度约为 $O(cm)$，相较于 PBFT，通信复杂度大幅降低。

在安全性、稳健性方面，系统采用分层共识结构，初始区块生成过程仅有委员会节点参与，主节点身份隐匿于委员会中，且委员会由信誉较高的节点组成，因此，在第一轮共识的提案阶段，主节点被敌方攻击的概率较低。在第二轮共识过程中，主节点身份对共用节点公开，此时即使敌方发动攻击也无法撤销已生成的初始区块，保障共识流程顺利进行。除此之外，分层共识结构中共用节点包含不同编队对应的节点，即使某组节点被敌方集中攻击，只要共用节点中包含 $2f+1$ 个诚实节点，仍能消除错误、恶意信息对系统的影响，确保系统的安全性。

2 面向无人机集群的共识算法

2.1 算法流程

本文根据无人机集群的特点和需求，提出了双层分组拜占庭容错算法。该算法在正常情况下的共识流程如图 2 所示。

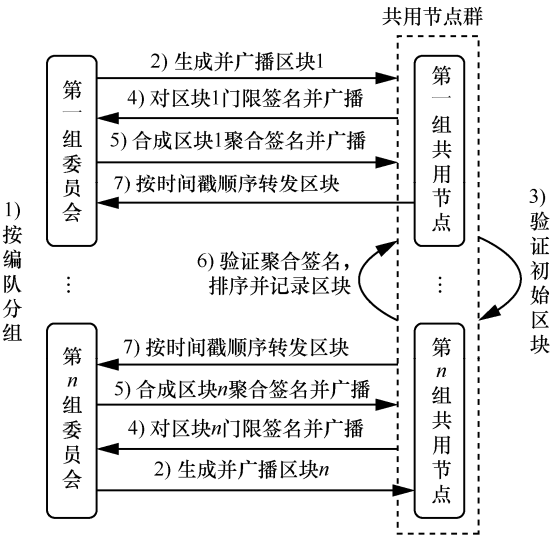

图 2 共识流程

1) 根据无人机集群编队情况进行分组，确定各组委员会节点以及共用节点。

2) 委员会节点使用 PBFT 共识生成初始区块，并向共用节点广播初始区块。

3) 共用节点验证初始区块，并检查初始区块是否包含 $2c/3+1$ 以上委员会节点的签名。

4) 初始区块验证通过后，共用节点使用门限签名私钥对其签名，并广播至委员会节点。同时，委员会节点也对初始区块签名并互相发送。

5) 委员会节点收到 $2f+1$ 个签名后合成聚合签名，并广播至共用节点。

6) 共用节点验证聚合签名，根据区块的时间戳进行排序，并将最终区块按顺序记录于账本。

7) 共用节点将该区块信息按时间戳顺序转发

至对应的委员会，委员会中的节点将该区块记录于账本。

当某个委员会在进行第一轮共识时出现拜占庭故障导致初始区块未生成或者该委员会生成的初始区块被共用节点拒绝时，将启动视图转换协议，使用预先选定的共用节点整组替换该委员会中的节点。

2.2　密钥生成

TLGBFT 涉及节点的身份认证、数字签名等，需要为节点生成对应的密钥。

TLGBFT 包含两轮共识过程，第一轮共识旨在生成初始区块，由于参加第一轮共识的委员会节点数量较少，因此，第一轮共识采用 PBFT 共识协议。第二轮共识主要是对初始区块进行确认，参与第二轮共识的共用节点数量较多，为了降低通信复杂度，采用基于门限签名的共识协议。系统中每个节点都有可能被选为委员会节点，而委员会节点也可能因系统拜占庭故障变为共用节点。因此，每个节点都配有 2 套密钥，分别是(pk_i , sk_i)以及(PK, SK_i)。第一套密钥(pk_i , sk_i)用于节点的身份认证，使用非对称加密算法[17]生成。第二套密钥(PK , SK_i)用于进行门限签名以及对多个门限签名合成的聚合签名进行验证，使用文献[18]提出的方案生成门限签名私钥 SK_i 以及系统公钥 PK，其中门限签名阈值为 $2f+1$[5]。同时，本文假设存在可信的证书授权中心为节点颁发相应的公钥证书。

2.3　共识过程

系统正常运行未检测到拜占庭故障时，TLGBFT 首先对节点进行分组并配置节点类型。通常，同一编队的无人机距离较近，通信环境较好，应当尽可能进行编队内通信，减少不同编队无人机之间的通信次数，从而降低平均通信时延。基于这一思路，根据无人机集群的编队结果对系统中的节点进行分组，其中，第 i 组节点对应第 i 编队的无人机。同时，从每组中选取少量委员会节点作为代表与其他组的节点进行信息交互。委员会产生的初始区块需要经过其他节点的确认，因此，所提算法的安全性与委员会中恶意节点的个数无关。系统初次运行时，委员会节点从各组节点中随机选取，各组剩余的节点即共用节点。经过分组和委员会选举后，系统中的节点形成双层分组结构。

第 i 组委员会在 t 时刻收到第 k 个客户端的提案请求〈‘request’, o, t, k〉后，主节点验证操作 o 是否合法，然后向委员会其他节点发送预准备消息〈‘pre-prepare’, v, h, $H(B)$, B〉，该消息包含当前视图编号 v、区块高度 h、区块 B 以及区块摘要 $H(B)$，区块摘要通过哈希函数 $H(\cdot)$计算得到。对于委员会中的任意节点 p_{ij}，当收到预准备消息后，检查消息签名是否正确，视图编号以及区块高度是否一致，检查通过后，向委员会广播准备消息，消息格式为〈‘prepare’, v, h, $H(B)$, j〉$_j$。当节点 p_{ij} 收到超过 $2c/3$ 个委员会节点发送的准备消息后，向委员会广播承诺消息，消息格式为〈‘commit’, v, h, $H(B)$, j〉$_j$。若节点 j 收到超过 $2c/3$ 个委员会节点发送的承诺消息，则第一轮共识完成，生成初始区块。具体流程如算法 1 所示。

算法 1　初始区块生成算法

已知　第 i 组委员会主节点 P_i，其他节点 p_{ij}，$1 \leqslant j < c$

1) P_i 将提案内容打包成区块 B
2) P_i 向委员会广播预准备消息〈 ‘pre-prepare’, v, h, $H(B)$, B〉
3) upon p_{ij} 收到合法的预准备消息 do
   向委员会广播准备消息〈‘prepare’, v, h, $H(B)$, j〉$_j$
4) end upon
5) upon p_{ij} 收到至少 $2c/3+1$ 条合法的准备消息 do
6)　向委员会广播承诺消息〈‘commit’, v, h, $H(B)$, j〉$_j$
7) end upon
8) upon p_{ij} 收到至少 $2c/3+1$ 条合法的承诺消息 do
9)　生成初始区块 $B_{\text{init}} \leftarrow B$
10) end upon
11) if p_{ij} 超时未生成 B_{init} then
12)　广播 Timeout 信息至委员会以及共用节点群
13) end if

初始区块 B_{init} 生成后，委员会节点和共用节点的后续共识过程如算法 2 和算法 3 所示。首先，第 i 组委员会将生成的初始区块 B_{init} 广播至共用节点群，为了避免主节点可能为恶意节点，伪造初始区块的情况，第 i 组委员会中的所有节点都参与广播。当某一共用节点 p_k 收到至少 $2c/3+1$ 个有效的初始区块 B_{init} 后，使用门限签名私钥对该区块进行签名，并将签名后的区块广播至第 i 组委员会。类似地，第 i 组委员会节点也需要使用门限签名私钥对区块签名，并互相发送。当第 i 组委员会任意节点收到了至少 $2f+1$ 个有效的门限签名之后，该节点将收到

的签名合成为聚合签名，同时将其广播至共用节点群。共用节点收到聚合签名和区块后，对其进行验证并根据区块时间戳对区块进行排序，将区块按照时间顺序记录于账本。最后，共用节点将转发聚合签名和区块到各组委员会。各组委员会节点收到有效的聚合签名之后，也将区块保存于本地账本。为了降低通信时延，每个共用节点仅负责向所属分组的委员会转发聚合签名和区块。

算法 2 委员会节点后续共识流程

已知 第 i 组委员会节点 p_{ij}, $1 \leqslant j < c$，初始区块 B_{init}

1) p_{ij} 向共用节点群广播初始区块 B_{init}
2) p_{ij} 使用门限签名私钥对 B_{init} 进行签名，并广播至委员会
3) upon p_{ij} 收到至少 $2f$+1 个有效的门限签名 do
4) 合成聚合签名，并广播至委员会以及共用节点群
5) end upon
6) upon p_{ij} 收到带有错误签名的区块或收到至少 f+1 个 Timeout 信息 do
7) 启动视图转换协议
8) end upon
9) upon p_{ij} 收到共用节点发送的具有有效聚合签名的区块 do
10) 将区块记录于本地账本中
11) end upon

算法 3 共用节点后续共识流程

已知 共用节点 p_k, $1 \leqslant j \leqslant m$，初始区块 B_{init}

1) upon p_k 收到至少 $2c/3$+1 个有效的初始区块 B_{init} do
2) 使用门限签名私钥对 B_{init} 进行签名，并广播至委员会
3) end upon
4) if p_k 超时未收到初始区块 B_{init} then
5) 广播 Timeout 信息至委员会以及共用节点群
6) end if
7) upon p_k 收到有效的聚合签名 do
8) 根据区块的时间戳对区块进行排序，并将区块按顺序记录于本地账本中
9) 将区块和聚合签名广播至 p_k 所属分组的委员会
10) end upon
11) upon p_{ij} 收到带有错误签名的区块或收到至少 f+1 个 Timeout 信息 do
12) 启动视图转换协议
13) end upon

TLGBFT 在运行时可能出现的拜占庭故障如下。

1) 委员会的主节点为恶意节点，可能生成包含错误信息的区块或故意不发送消息引起超时，导致初始区块生成失败。

2) 委员会的主节点为诚实节点，但委员会包含至少 $2c/3$+1 个恶意节点，恶意节点可能故意不响应主节点引起超时，导致初始区块生成失败。

3) 委员会的主节点为恶意节点，且委员会包含至少 $2c/3$+1 个恶意节点，主节点可能与其他恶意节点共同作恶，成功生成包含错误信息的初始区块。但诚实的共用节点会检测出恶意区块，并拒绝响应委员会节点的消息引起超时，导致共识失败。

当出现上述情况时，TLGBFT 将启动视图转换协议，以免系统陷入无限等待。

2.4 视图转换

当第 i 组委员会的提案在共识过程中出现拜占庭故障时，系统中所有分组都将停止正在进行的共识提案。TLGBFT 使用预先选定的新委员会替换第 i 组委员会。虽然 TLGBFT 的安全性与委员会中恶意节点的数量无关，但为了避免频繁触发视图转换，保障系统的活性，TLGBFT 引入了信誉机制。系统会根据每个节点诚实或者恶意行为的次数进行计分并生成信誉列表[19]，该列表由所有节点共同维护，记录于区块链中，只有信誉值高于阈值的节点才能被选为委员会节点。视图转换时，从第 i 组的高信誉节点中随机抽取 c 个组成新委员会。新委员会节点向共用节点群广播视图转换消息，消息格式为〈‘view-change’, v_{old}, v_{new}, h, $H(B_c)$, B_c〉，其中，v_{old} 和 v_{new} 分别为当前视图编号和新视图编号，B_c 为节点本地账本中保存的最新区块，$H(B_c)$为 B_c 的摘要。共用节点收到视图转换消息后验证最新区块、视图编号以及区块高度是否一致。验证通过后，共用节点更新视图编号，使用门限签名私钥对视图转换确认消息〈‘view-change-confirm’, v_{new}, h, B_c〉签名，并广播至新委员会，新委员会节点收到至少 $2f$+1 条签名消息后，合成聚合签名并广播至共用节点群。最后，共用节点将聚合签名转发至所属的委员会节点，令其更新视图编号和最新区块。视图转换完成后，TLGBFT 在新的视图编号下继续运行。

3　实验及结果分析

3.1　实验设置

本文实验模拟无人机集群协同执行任务的场景，该集群包含多架无人机，均分为 4 个编队。对应地，本文实验采用 4 台 Intel(R) Core(TM) i7@2.2GHz 处理器，16 GB 内存的服务器模拟 4 个编队，每台服务器使用 docker 容器构建虚拟节点，服务器之间通过无线网络连接。在此基础上，基于 Hyperledger Fabric 搭建区块链网络，并实现所提算法 TLGBFT 以及对比算法 PBFT。在 Hyperledger Fabric 框架下使用组织对节点进行分组。由于 PBFT 不对节点进行分组和分层操作，区块链网络使用 PBFT 共识时仅设置一个组织，所有虚拟节点同属于该组织。当区块链网络使用 TLGBFT 共识时，将虚拟节点划分为 4 个组织，与无人机编队一一对应。每个组织中设置一定比例的委员会节点，委员会节点需要与其他组织的节点频繁通信，因此，将其设置为锚节点。本文实验的测试指标为共识时延，即算法完成整个共识过程花费的时间，实际测试中，给定一段时间，统计在该时段内完成共识的次数，计算每次共识的平均时长。

3.2　共识时延测试

本节测试中，节点数量分别设置为 60、80、120、160、200。TLGBFT 每个委员会的数量分别设置为 5、5、7、10、15。首先测试 TLGBFT 仅使用一个委员会处理提案请求时的共识时延，结果如图 3 所示。

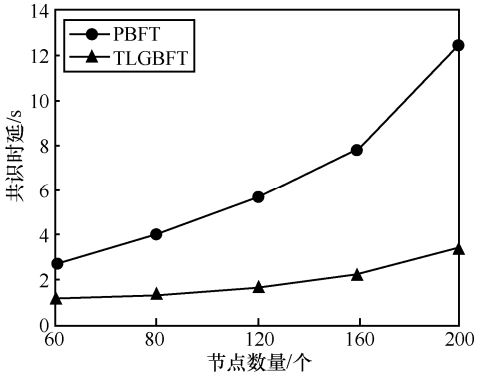

图 3　TLGBFT 仅使用一个委员会的共识时延

由图 3 可知，TLGBFT 的共识时延明显低于 PBFT，且随着节点数量的增加，PBFT 的共识时延大幅提高，而 TLGBFT 的共识时延随着节点数量趋近于线性增长。TLGBFT 的性能提升主要来自两方面。一方面，TLGBFT 使用双层分组结构，对当前委员会的提案进行共识时其他组委员会节点不参与，相比于 PBFT，共识过程参加的节点数量减少。另一方面，TLGBFT 使用门限签名技术，通信复杂度近似于 $O(cm)$，远低于 PBFT 的通信复杂度 $O(n^2)$。一般情况下，$c<<m$，因此，TLGBFT 的共识时延与共用节点数量大致呈正相关关系。

然后，测试 TLGBFT 使用所有委员会处理提案请求时的共识时延，结果如图 4 所示。

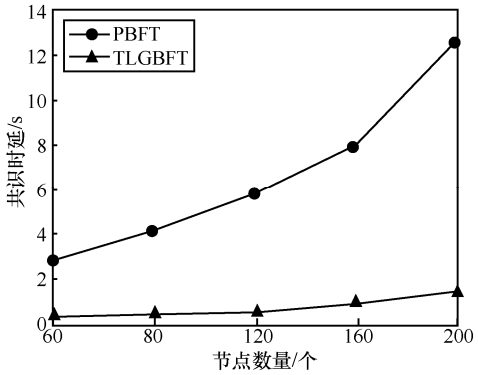

图 4　TLGBFT 使用所有委员会的共识时延

由图 4 可知，TLGBFT 使用所有委员会处理提案请求时，平均共识时延进一步降低，这得益于提出的双层分组结构带来的流水线式并行处理能力。但由于共用节点的计算能力以及负载有限，当分组过多时，共识时延降低的效果将达到瓶颈。

此外，为了验证提出的双层分组结构的有效性，本文实验设置了一组对照组，在该对照组中，组织的划分与无人机编队结果无关，虚拟节点被随机均分为 4 个组织，其他设置与 TLGBFT 相同。共识时延测试结果如图 5 所示。

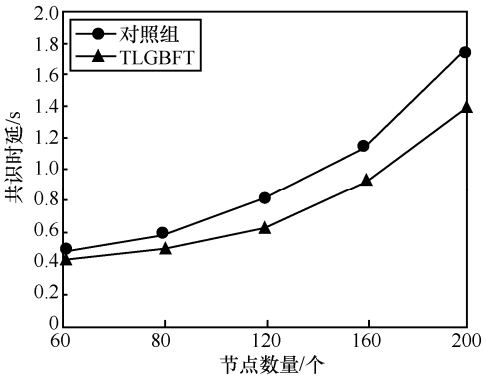

图 5　TLGBFT 与对照组的共识时延测试结果

由图 5 可知，当节点随机分组时，共识时延提高，且提高的幅度随着节点数量的增加而增加。这是因为节点随机分组使通信时延较低的节点被分

到不同组织，在共识过程中，同组织中节点通信次数远高于不同组织间节点的通信次数，导致共识时延增加。由此可知 TLGBFT 分组策略的有效性。

3.3 安全性分析

TLGBFT 采用了双层分组结构，将区块打包生成阶段限制在委员会中进行，此阶段共用节点不参与，主节点身份仅委员会节点知晓，得益于信誉机制，委员会节点为拜占庭节点的概率较低，主节点身份隐匿于委员会之中。因此，敌方对主节点发动自适应攻击的成本大幅提升，主节点被攻击的概率大幅降低，系统稳健性较高。

此外，TLGBFT 还有一个重要的特性，即系统的安全性与委员会中拜占庭节点的个数无关。即使委员会中所有节点都为拜占庭节点，故意不发送消息或生成包含错误信息的区块，共用节点群中的 $2f+1$ 个诚实节点会检测出恶意行为并启动视图转换协议选举新的委员会。一般地，考虑包含 $3f+1$ 个节点的系统，f 为拜占庭节点的数量。从中随机选取 c 个节点组成委员会，则委员会中拜占庭节点联合作恶成功的条件为数量超过 $2c/3$，概率为

$$\sum_{a=\frac{2}{3}c+1}^{c}\frac{\mathrm{C}_{2f+1}^{c-a}\mathrm{C}_{f}^{a}}{\mathrm{C}_{3f+1}^{c}} \tag{1}$$

以节点总数 $3f+1=100$ 为例，委员会中拜占庭节点联合作恶成功概率随委员会节点数量的变化曲线如图 6 所示。

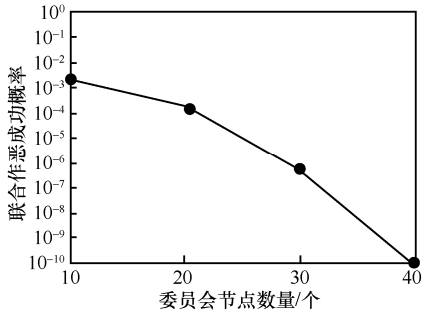

图 6 拜占庭节点联合作恶成功概率随委员会节点数量的变化曲线

由图 6 可知，在 100 个节点的区块链网络中，当委员会节点数量为 10 个时，委员会中拜占庭节点联合作恶的概率低于 0.2%，且概率随着委员会节点数量增加而降低，具有较高的安全性。此外，TLGBFT 还引入了信誉机制，委员会节点从高信誉节点中选取而非随机抽取，安全性进一步提升。

4 结束语

本文针对现有的共识算法通信复杂度高、稳健性差，难以适用于无人机集群的问题，提出了一种面向无人机集群的双层分组拜占庭容错算法 TLGBFT。该算法根据无人机的编队结果对节点进行分组，同时，从每组选取一部分高信誉节点组成委员会，其他节点作为共用节点，形成双层分组共识结构。一方面，TLGBFT 使用门限签名技术降低通信复杂度，且仅通过委员会与其他分组节点通信，减少分组间通信次数，使平均通信时延大幅度减小。另一方面，TLGBFT 的分层结构使主节点身份隐匿于委员会之中，降低了主节点被敌方自适应攻击的风险，提升了系统的稳健性，同时在委员会选举阶段引入了信誉机制，进一步确保了 TLGBFT 的安全性。分析表明，TLGBFT 能较好地契合无人机集群协同任务的需求，兼顾通信复杂度和算法稳健性、安全性。

参考文献：

[1] LI R, MA H Z. Research on UAV swarm cooperative reconnaissance and combat technology[C]//Proceedings of 2020 3rd International Conference on Unmanned Systems (ICUS). Piscataway: IEEE Press, 2020: 996-999.

[2] 未央. 无人机漏洞繁多渐成黑客“帮凶”[J]. 信息安全与通信保密, 2016, 14(2): 72-73.
WEI Y. UAVs have many vulnerabilities and gradually become hackers' accomplices[J]. Information Security and Communication Secrecy, 2016, 14(2): 72-73.

[3] MERMER G B, ZEYDAN E, ARSLAN S S. An overview of blockchain technologies: Principles, opportunities and challenges[C]//Proceedings of 2018 26th Signal Processing and Communications Applications Conference (SIU). Piscataway: IEEE Press, 2018: 1-4.

[4] LUCAS B, PÁEZ R V. Consensus algorithm for a private blockchain[C]//Proceedings of 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication. Piscataway: IEEE Press, 2019: 264-271.

[5] 刘懿中, 刘建伟, 张宗洋, 等. 区块链共识机制研究综述[J]. 密码学报, 2019, 6(4): 395-432.
LIU Y Z, LIU J W, ZHANG Z Y, et al. Overview on blockchain consensus mechanisms[J]. Journal of Cryptologic Research, 2019, 6(4): 395-432.

[6] PASS R, SHI E. FruitChains: a fair blockchain[C]//Proceedings of the ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 2017: 315-324.

[7] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//Advances in Cryptology 2017. Berlin: Springer, 2017: 357-388.

[8] FAN X X, CHAI Q. Roll-DPoS: a randomized delegated proof of

stake scheme for scalable blockchain-based Internet of things systems[C]//Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. New York: ACM Press, 2018: 482-484.

[9] ABRAHAM I, MALKHI D, NAYAK K, et al. Solida: a blockchain protocol based on reconfigurable Byzantine consensus[J]. arXiv Preprint, arXiv: 1612.02916, 2016.

[10] PASS R, SHI E. Hybrid consensus: efficient consensus in the permissionless model[C]//Proceedings of 31st International Symposium on Distributed Computing. Piscataway: IEEE Press, 2017: 1-16.

[11] LUU L, NARAYANAN V, ZHENG C D, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 17-30.

[12] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[13] GOLAN G G, ABRAHAM I, GROSSMAN S, et al. SBFT: a scalable and decentralized trust infrastructure[C]//Proceedings of 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2019: 568-580.

[14] YIN M F, MALKHI D, REITER M K, et al. HotStuff: BFT consensus with linearity and responsiveness[C]//Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 2019: 347-356.

[15] 孙海锋, 张文芳, 王小敏, 等. 基于门限和环签名的抗自适应攻击拜占庭容错共识算法[J]. 自动化学报, 2021, PP(99): 1-12.
SUN H F, ZHANG W F, WANG X M, et al. A robust Byzantine fault-tolerant consensus algorithm against adaptive attack based on ring signature and threshold signature[J]. Acta Automatica Sinica, 2021, PP(99): 1-12.

[16] 黄冬艳, 李浪, 陈斌, 等. RBFT: 基于 Raft 集群的拜占庭容错共识机制[J]. 通信学报, 2021, 42(3): 209-219.
HUANG D Y, LI L, CHEN B, et al. RBFT: a new Byzantine fault-tolerant consensus mechanism based on Raft cluster[J]. Journal on Communications, 2021, 42(3): 209-219.

[17] WIENER M J. Cryptanalysis of short RSA secret exponents[J]. IEEE Transactions on Information Theory, 1990, 36(3): 553-558.

[18] SHOUP V. Practical threshold signatures[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2000: 207-220.

[19] WANG Y, SONG Z, CHENG T. Improvement research of PBFT consensus algorithm based on credit[C]//International Conference on Blockchain and Trustworthy Systems. Berlin: Springer, 2019: 47-59.

[作者简介]

陈宇（1990− ），男，湖北武汉人，博士，国防科技大学讲师，主要研究方向为区块链应用、图像视频处理等。

贾连兴（1963− ），男，河南浚县人，博士，国防科技大学教授、博士生导师，主要研究方向为区块链应用、系统建模仿真等。