

11-17-2021

Access Control Mechanism of UAV Cluster Based on Blockchain Smart Contract

Ting Duan

1. *College of Systems Engineering, National University of Defense Technology, Changsha 410073, China;;*

Weiping Wang

1. *College of Systems Engineering, National University of Defense Technology, Changsha 410073, China;;*

Yifan Zhu

1. *College of Systems Engineering, National University of Defense Technology, Changsha 410073, China;;*

Wang Tao

1. *College of Systems Engineering, National University of Defense Technology, Changsha 410073, China;;*

See next page for additional authors

Follow this and additional works at: <https://dc-china-simulation.researchcommons.org/journal>



Part of the [Artificial Intelligence and Robotics Commons](#), [Computer Engineering Commons](#), [Numerical Analysis and Scientific Computing Commons](#), [Operations Research](#), [Systems Engineering and Industrial Engineering Commons](#), and the [Systems Science Commons](#)

This Paper is brought to you for free and open access by Journal of System Simulation. It has been accepted for inclusion in Journal of System Simulation by an authorized editor of Journal of System Simulation.

Access Control Mechanism of UAV Cluster Based on Blockchain Smart Contract

Abstract

Abstract: A Unmanned Aerial Vehicle (UAV) cluster access control mechanism based on Ethereum blockchain smart contract is proposed to solve the problems of the strategic stability and low security of UAV cluster access control mechanism. *The role-based access control mechanism model is improved, and the formal definition of the access control model for UAV cluster is given. The access control architecture of UAV cluster based on blockchain technology is proposed, and the corresponding basic framework and execution process is proposed, which can effectively reduce the cost of UAV cluster operation management resources, solve the problem of incomplete state information caused by the block bifurcation of unmanned cluster.*

Keywords

unmanned aerial vehicle cluster, block chain, smart contract, access control architecture

Authors

Ting Duan, Weiping Wang, Yifan Zhu, Wang Tao, and Meigen Huang

Recommended Citation

Duan Ting, Wang Weiping, Zhu Yifan, Wang Tao, Huang Meigen. Access Control Mechanism of UAV Cluster Based on Blockchain Smart Contract[J]. Journal of System Simulation, 2021, 33(11): 2656-2662.

基于区块链智能合约的 UAV 集群访问控制机制

段婷¹, 王维平^{1*}, 朱一凡¹, 王涛¹, 黄美根¹

(1. 国防科技大学 系统工程学院, 湖南 长沙 410073; 2. 湖南易维码有限公司, 湖南 长沙 410073)

摘要: 针对无人机(Unmanned Aerial Vehicle, UAV)集群访问控制机制通常稳定性策略性和安全性低等问题, 提出基于以太坊区块链智能合约的 UAV 集群访问控制机制。进行基于角色的访问控制机制模型的改进, 给出针对 UAV 集群基于访问控制模型的形式化定义。提出基于区块链技术的 UAV 集群访问控制架构, 并提出对应的基本框架与执行流程, 该机制有效降低了 UAV 集群作战管理资源成本, 解决了无人集群因区块分叉导致状态信息不完全的问题。

关键词: 无人机集群; 区块链; 智能合约; 访问控制架构

中图分类号: TP391.9 文献标志码: A 文章编号: 1004-731X (2021) 11-2656-07

DOI: 10.16182/j.issn1004731x.joss.21-FZ0712

Access Control Mechanism of UAV Cluster Based on Blockchain Smart Contract

Duan Ting¹, Wang Weiping^{1*}, Zhu Yifan¹, Wang Tao¹, Huang Meigen¹

(1. College of Systems Engineering, National University of Defense Technology, Changsha 410073, China;

2. Hunan YiWei Code Co., Ltd, Changsha 410073, China)

Abstract: A Unmanned Aerial Vehicle (UAV) cluster access control mechanism based on Ethereum blockchain smart contract is proposed to solve the problems of the strategic stability and low security of UAV cluster access control mechanism. *The role-based access control mechanism model is improved, and the formal definition of the access control model for UAV cluster is given. The access control architecture of UAV cluster based on blockchain technology is proposed, and the corresponding basic framework and execution process is proposed, which can effectively reduce the cost of UAV cluster operation management resources, solve the problem of incomplete state information caused by the block bifurcation of unmanned cluster.*

Keywords: unmanned aerial vehicle cluster; block chain; smart contract; access control architecture

引言

由于无人机(Unmanned Aerial Vehicle, UAV)系统部署、维护的低成本和人类飞行员无法到达或危险的地区操作的可能性, 无人机在军事领域和民用应用方面都吸引了很多研究关注。为解决生存点搜索、多目标监控与跟踪等复杂任务, 对无人机集群的应用进行了展望。这需要更复杂的控制、沟通和协调机制^[1]。无人机集群作战是一个数目庞大且成本较低的无人平台, 能够像“蜂群”一样协同分

工作战, 并通过开放式的架构和高效的管理与控制, 实现无人系统之间的无缝集成和优化协同, 可以促使整体作战效能的提升。

为此, Jiang 等提出了一种新的基于异构角色的无人机群体分布式协调控制方案, 以实现无人机群体的编队控制。首先, 在分布式模型预测控制的基础上, 设计了分布式协调控制方案的框架^[2]。为了同时部署多个无人机加快完成任务效率, 并扩大集群覆盖区域, 文献[3-4]提出了基于任务的无人机

收稿日期: 2021-06-14 修回日期: 2021-07-19

第一作者: 段婷(1994-), 女, 博士生, 研究方向为体系工程与体系仿真、无人集群架构与优化。E-mail: duanting18@nudt.edu.cn

通讯作者: 王维平(1962-), 男, 博士, 教授, 研究方向为体系工程与体系仿真。E-mail: wpwang@nudt.edu.cn

群协调协议, 该协议允许多架无人机在执行计划任务时完美地协同飞行。在研究群体控制与网络拓扑关系的基础上, 文献[5]提出了一种主动感知网络拓扑变化的策略。为了提高无人机集群空中协同的通信传感, 文献[6]提出了一种多旋翼无人机的跟踪模型, 该模型采用接收信号强度指示器传感器组成群, 协同逼近和跟踪运动目标。同样的, 为了实现理想的协同编队飞行, 提出了一种新的分布式协同控制方案, 包括基于共识的盘旋交会、leader 无人机的路径跟踪协调控制和 leader-follower 无人机的协同控制^[7-8]。

但是在集群对抗过程中, UAV 集群内部节点因受攻击、能源耗尽等原因, 常常出现节点功能丧失等情况, 此时的集群内部会围绕集群初始任务出现访问控制紊乱。当遇到威胁群时, 一个群中的无人机作为一个单元, 一起作为一个控制对象。每个冲突群从预设的避碰策略池中选择 3 个候选避碰策略, 通过不确定性轨迹建模生成相应的规划轨迹, 然后广播并共享^[9]。但是策略的转变, 子群中某一个 UAV 节点可能遭击毁或功能丧失^[10], 都会导致集群访问控制成本提升。而当前的 UAV 集群的海量性、动态性、分布式、轻量级的特点同样使 UAV 集群访问控制机制存在稳定性不足、权限判决性能低和安全性降低。因此, 关于解决大规模下 UAV 集群协同作战的访问控制问题是一个重点也是一个难点。

1 区块链技术

区块链技术是一种将加密算法、智能合约以及共识算法等多种技术方法进行完美结合的新技术, 从根本上解决了传统的安全性问题。区块链的兴起是由于比特币的成功应用^[11], 区块链 2.0 应用了智能合约, 智能合约实质上是一种计算程序, 该程序记录节点状态, 更新状态需要多方认可, 只要满足特定的写入条件, 智能合约便可以自动响应。需要发送的数据主要被事务包含, 数据的描述信息由事件控制。由于区块链的可追溯性、安全性、公开性、

不可篡改性和去中心化等特点, 被成功应用于数字货币、金融、医疗^[12]、农业^[13]等领域。随着区块链的兴起, 访问控制机制也逐步融入了区块链技术。利用区块链引入完全分散和隐私保护授权管理框架, 使用户能够控制数据^[14]。Dorri 等将区块链的存储数据与物联网设备耦合, 实现访问控制技术^[15]。

越来越多的研究人员在无人机集群研究领域引入了区块链的相关技术^[16-17], 增大了无人机集群的可控性和安全性。但是, 很少有人针对无人机集群的访问控制机制策略性和安全性进行一体化研究, 如图 1 所示, 并且传统的组网和控制技术也无法满足大规模集群应对复杂动态环境下海量的访问控制^[18], 无法充分体现集群协同作战的优势。

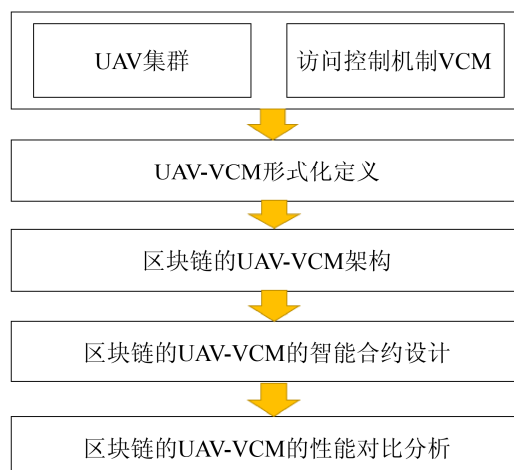


图 1 研究内容框架

Fig. 1 Research content framework

2 UAV 集群访问控制模型描述

2.1 访问控制模型

访问控制机制是指对主体访问客体的权限或能力的一种限制, 以及限制进入区域和使用的机制, 多运用于计算机存储数据的过程。访问控制机制是访问控制的判决控制所依据的规则, 一个系统可能有多种判决控制策略。UAV 发起节点的访问控制信息唯一的标识, 如图 2 所示。

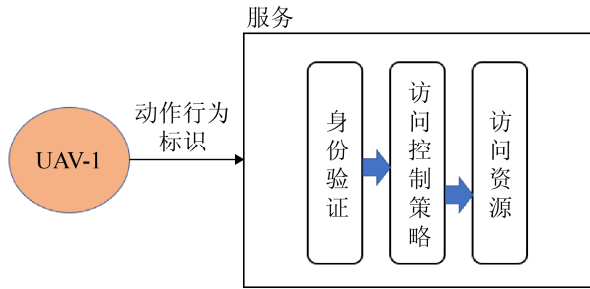


图 2 无人机访问控制模型
Fig. 2 UAV access control model

此时的无人机 UAV-1 是客体，为了地址系统资源被敌方非法入侵并占用，从根本上避免未授权用户侵占系统资源，设置主体在客体资源的访问上进行限制，设计一种访问控制机制。访问时首先进行身份验证，如图 2 所示，验证通过后允许主体进行访问策略及访问控制策略，确定客体对主体行为的约束条件，最后访问资源。

2.2 形式化定义

为了便于对控制机制进行描述，通过形式化的方式访问控制模型(Access control model, ACM)的要素进行如下定义：

访问控制模型 ACM 用函数 f 来表示，记为 $f(\text{ACM})$ 。

$$f(\text{ACM}) = \langle U, G, R, S, OJ, P, OP \rangle; UA, PA \quad (1)$$

式中： U 为用户； G 为用户组； R 为角色； S 为主体； OJ 为客体； P 为访问权限； OP 为操作。基本关系主要有 2 种：角色分配，记为 UA ；权限分配，记为 PA 。分别在下面给出定义。

定义 1. 用户是进行访问集群资源的具体某个 UAV 主体，每个用户属于任何子群，也可映射多个角色。用户有多个，可以表示为 $U = \{u_1, u_2, \dots, u_n\}$ 。

定义 2. 用户组将用户分组管理，记为用户组。

定义 3. 角色是无人机通过成为适当角色的成员而得到的角色权限。无人机依据授予它的任务来被指派响应的角色。角色有多个，可以表示为 $R = \{r_1, r_2, \dots, r_n\}$ 。

定义 4. 主体表示资源的访问者，当主体获取

了相应的角色后具备某一个权限才能进行访问。主体有多个，可以表示为 $S = \{s_1, s_2, \dots, s_n\}$ 。

定义 5. 客体是主体获取到的相应角色，并具备了某个对应的权限进行访问的对象。客体有多个，可以表示为 $OJ = \{oj_1, oj_2, \dots, oj_n\}$ 。

定义 6. 访问权限是具备访问控制能力的许可，访问权限有多个，可以表示为 $P = \{ua_i \mid ua_i \in \{\text{read, write, delete, execute}\}, i \in [1, 2, 3, 4]\}$ 。

定义 7. 角色分配用于反映机制的可执行性，能被用户主体调用并执行，并匹配对应的访问策略。UAV 集群中的角色分配有读取、写入、删除和退出等，可以表示为 $UA \subseteq U \otimes R = \{(u, r) \mid u \in U \wedge r \in R\}$ 。

定义 8. 权限分配用于表示权限许可和角色之间的关联关系映射，可以表示为 $PA \subseteq P \otimes R = \{(p, r) \mid p \in P \wedge r \in R\}$ 。

3 区块链的 UAV-VCM 控制架构

区块链的体系架构主要由应用层、智能合约层、数据层、共识层和网络层共 5 个部分组成。而 UAV 集群部分的访问控制机制主要由应用层、智能合约层、共识层和数据层 4 个部分组成，如图 3 所示。

(1) 数据层将访问控制策略发送到各个节点，并封装在各个区块中，各个区块形成区块链，实现访问控制策略的安全性、可追溯性和开放性。

(2) 共识层主要存放以太坊区块链网络中的共识算法等机制协议，抽取集群的侦控打评等信息，无人机为一个节点执行某作战任务，所有无人机共同来维护一个区块链。通过共识机制选取最后的记账者，记账者选取方式会影响整个无人集群协同架构的安全性和可靠性。

(3) 合约层主要进行角色创建、角色分配及角色的权限分配等，然后将其发布在区块链上，保证无人机节点的匿名性和公开性。

(4) 应用层主要保持用户的交互。例如用户信息管理，角色管理，角色-权限管理和访问控制策略的响应等。

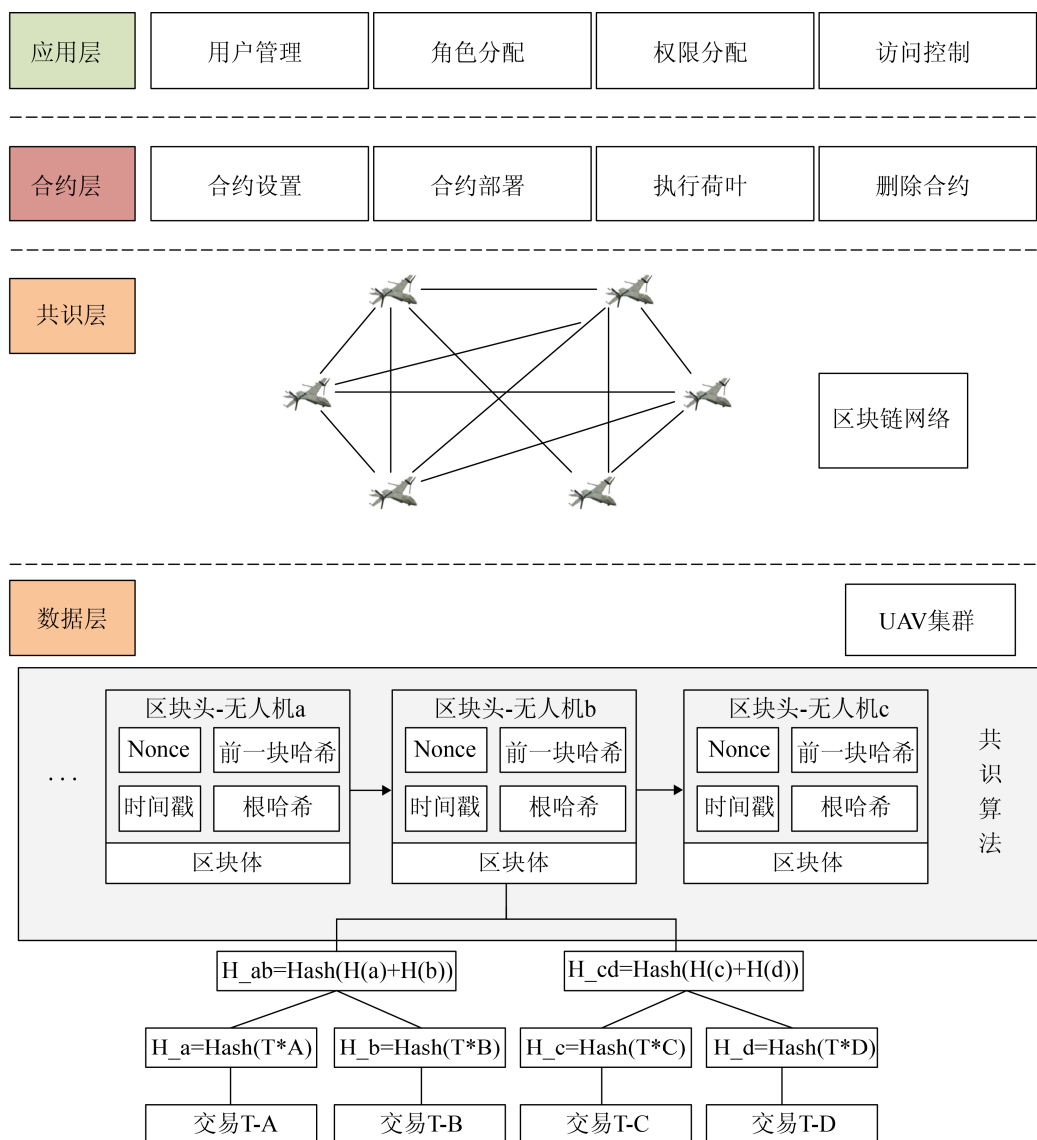


图 3 区块链 UAV-VCM 控制架构
Fig. 3 Blockchain UAV-VCM control architecture

实现各层互相协同，构成了一个完整的 UAV-VCM 架构。

4 区块链 UAV-VCM 的智能合约

本文以 UAV 集群单个无人机为节点，共同维护一个区块链，每个无人机的状态信息都可以更新和发布。

区块链技术最大的优点是不可篡改性和可追溯性，当 UAV 集群在执行任务时，集群中的子群里，有 2 架无人机同时发布一个区块，当前状态产

生分歧就会遇到分叉的情形。作战过程中，每个无人机的状态都需要实时更新。当 2 个无人机同时探测到不同的信息，或遇到不同的状况，同时发布区块时，区块链技术本身会按照分叉选取其中一个块作为链，另一个无人机的状态信息则不能更新。为了处理无人机作战遇到的这种情况，本节将对区块链 UAV-VCM 中设计一个优先级角色分配合约 (Pr-ROC) 如图 4 所示，称为区块链 UAV-VCM 的智能合约。

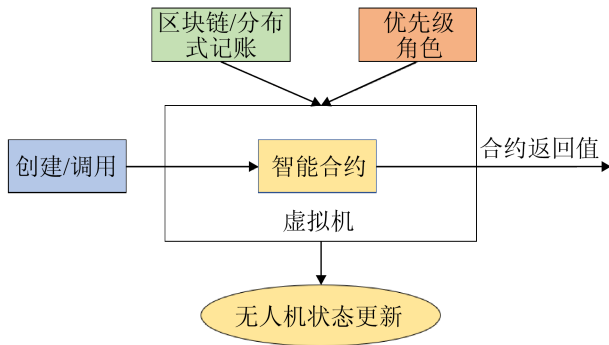


图 4 智能合约执行流程图

Fig. 4 Flow chart of smart contract execution

4.1 访问控制机制流程

为了方便后续实验分析,给出流程框架和流程伪代码如下所示:

- (1) 将当前无人机注册到集群网络中;
- (2) 获取并验证 UAV 集群网络中最长的区块链;
- (3) 发布新的状态信息。

伪代码:

Algorithm1: Pr-ROC algorithm

```

1 Input: {all_chain; nodes_sort; ax_length};
2 Output: {更新区块链 new_chain};
3   for node in all_chain:
4     if node_length== max_length;
5       list.append()
6   else:
7     continue;
8   new_chain = list(0)
9   for node in list(1:):
10    if last_node not find
11      Republish last_node;
12    else:
13      return
14 return

```

其中 all_chain 表示当前无人机集群所有区块链信息; nodes_sort 表示节点信息的权限排序; max_length 表示最长区块链长度; new_chain 表示更新区块链。

4.2 访问控制机制实验

区块链技术只保留最长的链,集群中如果同时发布了 2 个块,那么按照原本的特性,将选择最大的块作为链,那么另一块就会被舍弃。但是在无人机集群中,2 个无人机同时探索到了不同的状态,需要进行状态更新,就要同时发布 2 个区块。作战环境中,每个状态更新的块都需要保留信息,如何解决这个问题是本文的一大难点。

在本次仿真实验中本文假设:①集群作战环境通信状态保持良好;②不出现时延等意外情况;③集群节点内部存储量足够访问区块链的状态信息;④集群作战环境中未发生网络故障等意外情况。

为了解决区块链技术运用到无人集群中面对分叉从而导致信息流失的问题,我们设定了访问机制,在访问区块时,访问最大的那个块同时将原本要舍弃的区块信息读取,状态信息添加到选取块的附近,如上述伪代码所示。

仿真实验按照 2 个无人机同时发布区块,查看访问控制机制如何解决冲突导致信息不全的问题,利用区块链技术进行运行,检验对比效果如图 5~7 所示。

```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

```

```

"index": 2,
"message": "New Block Forged",
"previous_hash": "3f21c41f18b1c066726ddb497752f5e09dae8c4a7eed994b33ebef6a15722dd",
"proof": 35293,
"transactions": [
  {
    "amount": 100,
    "recipient": "find enemy",
    "sender": "e586714c6ef94896a8ba18bf9eb1d333"
  },
  {
    "amount": 103,
    "recipient": "find enemy",
    "sender": "e586714c6ef94896a8ba18bf9eb1d333"
  },
  {
    "amount": 1,
    "recipient": "d6bfa98473564034aa20f8927059097",
    "sender": "0"
  }
]

```

图 5 UAV-1 冲突图
Fig. 5 UAV-1 conflict

```

1  "index": 2,
2  "message": "New Block Forged",
3  "previous_hash": "ea8b5ccdc5c9c48abb679512d8c143e94d4ca88428d1a753886b689ee228b4ad",
4  "proof": 35293,
5  "transactions": [
6    {
7      "amount": 166,
8      "recipient": "find enemy",
9      "sender": "e586714c6ef94896a8ba10bf9eb1d333"
10   },
11   {
12     "amount": 16,
13     "recipient": "find enemy",
14     "sender": "e586714c6ef94896a8ba10bf9eb1d333"
15   },
16   {
17     "amount": 1,
18     "recipient": "c5d281aac98246ce9bb8a898b33ec9d1",
19     "sender": "0"
20   }
21 ]
22 ]
23 ]

```

图 6 UAV-2 冲突图
Fig. 6 UAV-2 conflict

```

"message": "Our chain was replaced",
"new_chain": [
  {
    "index": 1,
    "previous_hash": "1",
    "proof": 100,
    "timestamp": "2021-06-14-19-48-44",
    "transactions": []
  },
  {
    "index": 2,
    "previous_hash": "3f21c41f18b1c06726ddb497752f5e9dae8c4a7eead994b33ebf6a15722dd",
    "proof": 35293,
    "timestamp": "2021-06-14-19-58-30",
    "transactions": [
      {
        "amount": 100,
        "recipient": "find enemy",
        "sender": "e586714c6ef94896a8ba10bf9eb1d333"
      },
      {
        "amount": 103,
        "recipient": "find enemy",
        "sender": "e586714c6ef94896a8ba10bf9eb1d333"
      },
      {
        "amount": 1,
        "recipient": "d0bf98473564034aa020f8927059097",
        "sender": "0"
      }
    ]
  },
  {
    "index": 3,
    "previous_hash": "66411d29d30b3d25fa699025ffa7ce1913c2b102241b06b175ad98c31c79d35f",
    "proof": 35889,
    "timestamp": "2021-06-14-19-59-18",
    "transactions": [
      {
        "amount": 166,
        "recipient": "find enemy",
        "sender": "e586714c6ef94896a8ba10bf9eb1d333"
      },
      {
        "amount": 16,
        "recipient": "find enemy",
        "sender": "e586714c6ef94896a8ba10bf9eb1d333"
      },
      {
        "amount": 1,
        "recipient": "c5d281aac98246ce9bb8a898b33ec9d1",
        "sender": "0"
      }
    ]
  },
  {
    "index": 4,
    "previous_hash": "804a141ddd4b770e8a36b0ee85651290ecc5c1715fa53e3efc0498e2dfafd",
    "proof": 119678,
    "timestamp": "2021-06-14-20-02-57",
    "transactions": [
      {
        "amount": -12,
        "recipient": "find ally",
        "sender": "e586714c6ef94896a8ba10bf9eb1d333"
      },
      {
        "amount": 1,
        "recipient": "d6915361e066423ba2da8c3cb7a51393",
        "sender": "0"
      }
    ]
  }
]
]

```

图 7 Pr-ROC 执行流程结果图
Fig. 7 PR-ROC execution process result diagram

如图 5 和图 6 中 UAV-1 和 UAV-2 发生了冲突, 同时在局部发布了一个区块并发布了“find enemy”的状态信息, 并同时产生了 3 个信息, 分别发布索引号为 2, 接下来将使用 Pr-ROC 解决这个问题, 避免战场上的状态流失。

由图 7 可知, 利用第 3 部分的 UAV-VCM 控制架构, 使用 4.1 小节提出的控制机制流程图, 图 5 和图 6 遇到的区块发布冲突问题有效地被改善了。“index -2”被分别添加, 并发布了同一时间的每个无人机的状态信息。有效地解决了 UAV 集群分叉导致作战信息获取不完全问题。

5 结论

本文将提出将区块链技术应用于 UAV 集群上, 改进基于角色的访问控制机制模型, 给出针对 UAV 集群的访问控制机制模型的形式化定义。然后基于区块链技术解决应用到 UAV 集群分叉导致作战信息获取不完全问题, 基于该问题, 设计了相关的执行流程, 实验证明, 最大化保存无人机状态信息, 避免区块分叉导致的信息流失, 为无人机集群智能控制研究人员提供新的研究思路, 同时积极应对来自恶意服务者的安全性挑战。

参考文献:

- [1] Zhu X P, Liu Z C, Yang J. Model of Collaborative UAV Swarm Toward Coordination and Control Mechanisms Study[J]. Procedia Computer Science (S1877-0509), 2015, 51(1): 493-502.
- [2] Zhao J, Sun J, Cai Z, et al. Distributed Coordinated Control Scheme of UAV Swarm Based on Heterogeneous Roles[J]. Chinese Journal of Aeronautics (S1000-9361), 2021, 12(1): 1-17.
- [3] Fabra F, Zamora W, Reyes P, et al. MUSCOP: Mission-Based UAV Swarm Coordination Protocol[J]. IEEE Access (S2169-3536), 2020, 8(1): 72498-72511.
- [4] Fa Bra F, Zamora W, Reyes P, et al. An UAV Swarm Coordination Protocol Supporting Planned Missions[C]// 2019 28th International Conference on Computer Communication and Networks (ICCCN). Valencia, IEEE, 2019: 1-7.
- [5] Hong L, Guo H Z, Liu J J, et al. Toward Swarm

- Coordination: Topology-Aware Inter-UAV Routing Optimization[J]. IEEE Transactions on Vehicular Technology (S0018-9545), 2020, 9(69): 10177-10187.
- [6] Yannis S A, Thomas L B C, Panagiotis S D, et al. Modelling and Simulation of a New Cooperative Algorithm for UAV Swarm Coordination in Mobile RF Target Tracking [J]. Simulation Modelling Practice and Theory (S1569-190X), 2021, 107(1): 1-13.
- [7] Wan X K, Shen L C, Liu Z H. Coordinated Flight Control of Miniature Fixed-wing UAV Swarms: Methods and Experiments[J]. Science China (Information Sciences) (S1674-733X), 2019, 11(62): 134-150.
- [8] Wang X K, Shen L C, Liu Z H. Coordinated Flight Control of Miniature Fixed-wing UAV Swarms: Methods and Experiments[J]. Sci. China Inf. Sci (S1674-733X), 2019, 11(62): 134-150.
- [9] Wan Y, Tang J, Lao S Y. Distributed Conflict-Detection and Resolution Algorithm for UAV Swarms Based on Consensus Algorithm and Strategy Coordination[J]. IEEE Access(S2169-3536), 2019, 7(1): 100552-100566.
- [10] Ye Y, Wei W, D Geng, et al. Dynamic Coordination in UAV Swarm Assisted MEC via Decentralized Deep Reinforcement Learning[C]//2020 International Conference on Wireless Communications and Signal Processing (WCSP). Nanjing: IEEE, 2020.
- [11] Xu Y, Guan K, Lei L. Review on the Principle, Progress and Application of Block Chain Technology[J]. Journal of Physics: Conference Series (S1742-6588), 2020, 1651: 012041.
- [12] Wang M, Wu S. Research and Application of Sports Health System based on Block Chain Technology[J]. Iop Conference Series: Earth and Environmental Science (S1755-1307), 2021, 714(2): 22-25.
- [13] Liu Z, Huang W, Wang D .Functional Agricultural Monitoring data Storage based on Sustainable Block Chain Technology - ScienceDirect[J]. Journal of Cleaner Production (S0959-6526), 2020, 281: 124078.
- [14] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a New Blockchain-based Access Control Framework for the Internet of Things[J]. Security and Communication Networks (S1939-0114), 2016, 9(18): 5943-5964.
- [15] Dorri A, Kanhere S S, Jurdak R, et al. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home[C]//2017 IEEE International Conference on Pervasive Computing and Communications Workshops (Per Com Workshops). Kona, HI, USA: IEEE, 2017: 618-623.
- [16] Xu X, Zhao H, Yao H, et al. A Blockchain-enabled Energy Efficient Data Collection System for UAV-assisted IoT[J]. IEEE Internet of Things Journal S2431-2443), 2020, 4(8): 2431-2441.
- [17] Aloqaily M, Bouachir O, Boukerche A, et al. Design Guidelines for Blockchain-Assisted 5G-UAV Networks[J]. Moayad Aloqaily (S0890-8044), 2020(35): 2-9.
- [18] Shen L C, Wang X K, Zhu H Y, et al. UAVs Flocking and Reconfiguration Control based on Artificial Physics[J]. Scientia Sinica (Technologica)(S1674-7259), 2017, 3(47): 266-285.