

基于区块链的无人机集群安全协作

王宇晨 齐文慧 徐立臻

东南大学计算机科学与工程学院 南京 211189

(wycforever@163.com)

摘要 无人机集群拓展了无人机的应用领域,也带来了更为复杂的安全性挑战。无人机收集的情报与无人机本身都易于成为黑客攻击的目标,一旦黑客截获通信信息或劫持无人机,都将对集群的作战环境产生影响,甚至造成泄露国家机密、扰乱社会秩序等严重后果。文中介绍了无人机集群所面临的安全问题与联盟链 Hyperledger Fabric 的工作原理,并基于 Hyperledger Fabric 构建了对等网络模型 UAV-Swarm Net,利用区块链账本与智能合约实现无人机的数据共享与协同决策,为无人机集群的安全协作奠定了基础。UAV-Swarm Net 网络模型具备分布式、多副本、加密通道传输与责任可追溯的特性,能有效保障数据的机密性、完整性与可用性,增强系统的鲁棒性与可扩展性,为未来无人机体系化作战环境下,无人机协同作战面临的信息安全问题提供了新的解决方案。

关键词: 无人机集群;区块链;Hyperledger Fabric;网络安全;协同作战

中图法分类号 TP319

Security Cooperation of UAV Swarm Based on Blockchain

WANG Yu-chen, QI Wen-hui and XU Li-zhen

School of Computer Science and Engineering, Southeast University, Nanjing 211189, China

Abstract Unmanned aircraft vehicle swarm not only broadens the application fields of unmanned aircraft vehicles (UAVs), but also brings more complex security issues. Both the intelligence collected by UAVs and UAV itself are vulnerable to hacker attacks. Once hackers intercept communication information or hijack UAVs, it will have an adverse effect on the combat environment, and even cause serious consequences such as leaking state secrets and disrupting social order. This article introduces the security issues faced by UAV swarm and the principle of the consortium blockchain—Hyperledger Fabric. Then it designs a peer-to-peer network model named “UAV-Swarm Net” based on Hyperledger Fabric, using distributed ledgers and smart contracts to implement the safe cooperative combat of UAV swarm. The UAV-Swarm Net model has the characteristics of distribution, multiple copies, encrypted channel transmission and responsibility traceability, which can effectively guarantee the confidentiality, integrity and availability of data, enhance the robustness and scalability of UAV system. It provides a new solution to the information security problems faced by UAV swarm in the future UAV systemized combat environment.

Keywords UAV swarm, Blockchain, Hyperledger Fabric, Network security, Cooperative combat

1 引言

无人机(Unmanned Aerial Vehicle, UAV)具有造价低、体积小、易于部署、维护成本低、机动性高的特点,现已被广泛应用于城市规划、工程监管、物流配送等民用领域。随着无人机自主能力的不断提高与战场环境日益错综复杂,无人机在原生的军事领域的应用也将更加普遍。在实际应用中,单无人机受到能量消耗与视觉范围的限制,仅能在有限的地理区域内工作。面对恶劣的作战环境和复杂的作战任务,多无人机协同作战的无人机集群(UAV swarm)通过多角度的数据感知与共享,有效克服了单无人机的视野局限问题;通过群体智能(swarm intelligence)实现协同决策,有效提高了无人机的生存能力和整体作战效能,能够完成诸如集群对抗^[1]、森林消防^[2]等高难度任务。

在无人机集群协同作战的背景下,无人机之间需要搭建信息连接通道,形成一个移动自组织(Ad hoc)的无人机网

络^[3]。与传统的移动 Ad hoc 网络相比,无人机网络具有节点移动速度快、工作环境干扰强、工作时长、实时性强等特点,这些特点为无人机集群协同作战带来了更为复杂的安全问题^[4]。无人机采集的数据及其本身都易于成为黑客攻击的目标,一旦黑客截获通信信息或劫持无人机,都将对集群作战环境产生影响,甚至造成泄露国家机密、扰乱社会秩序等严重后果。2021 年 1 月重庆朝天门发生的百台无人机坠落事件,与美国司法部对于无人机安全法的更新,都表明无人机安全在未来安全风险中占据重要地位,对无人机的安全保护势在必行。

为了增强无人机系统的健壮性和安全性,近年来,研究者开始尝试利用区块链技术来解决无人机协同作战的信息安全问题。区块链是一项起源于比特币的新兴技术,它将数据区块按照时间顺序相连,形成了一个不可篡改、不可伪造的分布式账本。按照开放程度分类,区块链可被分为公有链、联盟链、私有链 3 种。其中,仅限联盟成员参与的联盟链兼具较高

的交易吞吐性能与较高的去中心化程度,与公有链和私有链相比,更适于与无人机集成来创建安全可靠的通信网络。

本文以联盟链 Hyperledger Fabric^[5]为基础框架,探索将区块链的核心技术(如点对等网络、分布式账本、智能合约等)应用于无人机集群系统的方案,帮助无人机实现协同作战中的数据共享与协同决策功能,并运用区块链本身的安全特性来应对无人机协作的安全问题,使无人机集群能在对抗性空域下正常运作,增强无人机系统的安全性、鲁棒性与可扩展性。

本文第2节介绍相关工作,包括无人机系统所面临的安全问题、联盟链 Hyperledger Fabric 的工作原理以及将区块链和无人机结合的现存方案;第3节介绍本文提出的模型 UAV-Swarm Net,包括网络结构、交易流程两部分;第4节从数据的机密性、完整性和可用性3个方面说明 UAV-Swarm Net 模型如何应对无人机系统的安全性挑战;最后总结全文,探讨由于两种技术的组合而引起的局限性和未来有待深入研究的问题。

2 相关工作

2.1 无人机系统安全

典型的无人机集群系统(Unmanned Aircraft System, UAS)主要由无人机集群、地面控制基站(Ground Control Station, GCS)以及它们之间用于交换信息的通信网络组成,是一个复杂的系统。随着作战任务的日益复杂与无人机智能化水平的提高,无人机系统的控制方式逐渐由传统的无线电遥控和自动程序控制向着无人机集群自主协同控制发展^[6]。自动控制与自主控制的主要区别在于:自动控制是系统按照指令执行任务,而系统本身并没有决策与协调的能力;而自主控制则需要无人机自身在必要的时刻做出决策^[7]。相较于简单的多机协同系统,UAS在安全性、群体智能、集群复杂度等方面都面临着重大挑战。无人机系统的复杂性与实用性也引发了企业界和学术界的研究热潮,据统计,仅2020年以来以UAV为关键词发表的论文就已经接近20000篇。

安全性是UAS最主要的关注点之一。对于无人机集群来说,必须保证无人机与无人机之间、无人机与GCS之间可以实时通信和共享信息,且发送和接收的信息必须可靠,才能进一步做出实时有效的决策和进行安全的协作。美国国家标准技术所(National Institute of Standards and Technology, NIST)将数据安全政策规定为“CIA”,即系统对机密性(Confidentiality, C)、完整性(Integrity, I)与可用性(Availability, A)的要求^[8]。其中,机密性指的是对数据的保护,无人机不可向任何未经授权的个人、实体或过程披露敏感信息;完整性指的是数据的可靠性,无人机系统应具备抵御黑客修改或损坏数据的能力;可用性指的是数据和服务的可访问性,应确保无人机系统能及时可靠地访问和使用信息。

完整的无人机安全防护方案应结合主动和被动两种防护方式^[4]。主动防护是指使用各种信息加密技术消除安全威胁,提高黑客入侵的难度。例如,文献[9]将安全加密方法应用于无人机遥测盒内的WiFi 802.11接入点与整个通信路径中,以此提升数据传输的机密性。被动防护是指在检测到安全威胁后作出恰当的反应,避免持续的不良影响。例如,文献[10]运用贝叶斯博弈论检测无人机的网络入侵,在提高无人机网络性能的同时实现安全检测;文献[11]利用中间件构造

加密信道来检测匿名攻击者的DoS入侵,以中断黑客攻击的信道。

但是,上述研究都立足于物理层或链路层的底层防御,仅注重无人机的局部安全防护,缺乏对整体网络架构的考量。为此,本文将通过区块链与无人机网络的集成,将成员身份验证、加密信道、非对称加密算法等多项安全技术整合起来,为无人机协作建立安全可靠的通信网络,有效应对“CIA”安全性挑战。

2.2 Hyperledger Fabric

Hyperledger Fabric 是 IBM 公司于 2017 年发布的区块链平台,其本质是一个开源的企业级许可分布式账本平台。它由以下模块化的组件组成:1)排序服务,由排序节点形成,负责在交易顺序上达成共识,并将交易打包到区块中;2)成员资格服务(Membership Service Provider, MSP),负责将网络中的实体与加密证书相关联;3)gossip 数据传播服务,负责将账本和通道数据传播给其他对等节点,使新节点以最快速度连接到网络并同步账本数据;4)智能合约(Fabric 中称作“链码”),负责定义区块链的业务逻辑与规则;5)数据库管理系统(Database management system, DBMS),负责存储和管理账本信息;6)可插拔的背书和验证策略,负责验证交易,确保交易的有效性。

对等节点(peer node)是区块链网络的基本组成单元,负责区块数据的校验和保存,维护着账本和链码实例。对等节点与排序节点都由组织(Organization)管理,通过证书颁发机构(Certificate Authority, CA)颁发的加密证书来标识身份。根据实际业务需要,组织被添加至联盟(Consortium)之中。Fabric 为联盟设置了通道架构,为通道内的成员组建子网,唯有参与到通道的节点才有权访问链码和账本,有效解决了用户隐私与数据机密性问题。

Hyperledger Fabric 将交易流分为“执行-排序-验证”3步:1)执行一个交易并检查它的正确性,为交易背书;2)通过可插拔的共识协议给交易排序;3)根据应用程序指定的背书策略来验证交易,将交易结果写入账本。特定应用程序的背书策略指定了需要哪些节点来为智能合约的正确执行做担保,Fabric 通过这种方式实现了应用的并行执行,从而提高了系统的整体性能和规模。

与比特币、以太坊等非许可的区块链网络不同,Hyperledger Fabric 是一个许可平台,参与者为一组已知的、已识别的且经常审查的对等节点,区块链在具有一定信任基础的治理模型下运作。正因如此,Fabric 采用确定性的共识算法(如 RAFT)为交易排序,账本不会像其他非许可链那样产生分叉,同时大大提升了共识效率。文献[12]重建的 Fast-Fabric 架构已将 Fabric 的交易吞吐量提升至 20000TPS。

Hyperledger Fabric 的上述功能特性使其成为一个高性能可扩展的系统,支持灵活的信任假设,有效地保障了交易和数据的隐私和机密性。成员资格服务为无人机的通信环境提供了良好的信任基础;智能合约能实现无人机集群协作所需的功能;背书策略使得应用程序能在不同的可信度要求下并行执行。本文将充分利用这些功能,基于 Hyperledger Fabric 建立对等网络 UAV-Swarm Net,满足无人机系统对数据机密性、完整性和可用性的安全性需求。

2.3 现存方案

2020 年 4 月,美国交通部发布的“无人机系统区块链”^[13]

断失误,UAV-Swarm Net 将根据背书节点的签名追溯责任,并依据情报等级采用不同的惩罚措施。如果情报等级较高,上传该信息的从无人机、所属的主无人机和其他为交易背书的对等节点都将被认为是间谍节点,从 UAV-Swarm Net 的信任列表中剔除,交由 GCS 审查和回收。若某无人机集群的主无人机因受牵连而停用身份或因被入侵而暂停工作,将选用以下两种方式之一来维持系统的正常工作:其一,由 GCS 分派新的主无人机来掌控接管从无人机;其二,以选举的方式选出集群中得票最多的从无人机晋升成主无人机,成为 UAV-Swarm Net 新的对等节点,接管控制集群的任务。

决策阶段和执行阶段的交易流程与侦察阶段大致相同,其区别主要在于携带决策的交易提案由主无人机发起,并由从无人机执行。发现任务目标后,主无人机根据当前的情报信息做效能评估^[20],并产生一个作战方案。为了避免因主无人机决策失误而引发的恶性事故,UAS 将为作战方案评定安全等级,不同的安全等级对应着不同的背书策略。例如,申请武器打击的方案采用最高的安全等级,需要通道内的所有主无人机和 GCS 对其背书。当决策被确定时,主无人机向从无人机发布链码事件。从无人机事先注册这些事件类型,当收到事件发生的通知时,便会立即执行对应的命令。

4 模型安全性讨论

首先,UAV-Swarm Net 对于数据的机密性作了很好的保证。UAV-Swarm Net 基于公钥基础结构(Public Key Infrastructure,PKI)设置了网络访问的限制。唯有获取由特定组织 CA 颁发的 X.509 证书的用户,才能通过 MSP 组件的验证,获得访问通道的权限,为无人机的通信环境奠定了良好的基础。此外,UAV-Swarm Net 在通信节点之间采用 TLS 传输层进行安全通信,通过双向验证保证通信双方的身份并建立一个双向的加密信道。情报数据在上链时运用加密功能转换成密文,唯有拥有密钥的节点才能解读情报信息,有效避免了对敏感数据的非法侵入。

其次,区块链账本的不变性与多副本性确保了数据的完整性,使无人机系统能够抵御外界对数据不当的修改和破坏。UAV-Swarm Net 中的每个主无人机和 GCS 都部署着一份所属通道的情报账本,即使某个主无人机被黑客入侵,数据也能通过下载其他节点的账本进行恢复。从无人机的情报上传与主无人机的决策制定都需要多个 GCS 站点与其他主无人机的背书,而大型的 GCS 通常很难被黑客入侵,大大提高了情报和决策的可靠性和可信度。账本的不变性意味着无法通过修改某个区块的情报信息来改变当前状态数据库。区块链上的每个区块都保存着上链数据和上一个区块的哈希值,如果区块的数据被黑客篡改,会导致当前区块的哈希值与下一区块记录的哈希值不匹配,从而能够检测出安全威胁并触发警报。区块链的可追溯性还为无人机系统建立起监察机制,通过区块交易信息和背书签名,能够很快定位被入侵的节点,将其剔除出信任列表,避免发生更大的损失。

最后,UAV-Swarm Net 网络去中心化的特质保证了无人机系统的可用性,使得无人机能及时可靠地访问数据信息。只要网络中大部分节点未遭遇黑客攻击,就能确保整个系统的正常运行。此外,UAV-Swarm Net 网络还具有高扩展性。

通过修改网络配置和添加通道,就能灵活实现小型无人机集群的建立与大型无人机集群的形成,背书策略的运用能满足实际的作战任务中不同程度的安全性需求。

结束语 本文基于联盟链 Hyperledger Fabric 定义了 UAV-Swarm Net 网络结构,探索了将区块链技术 with 无人机集成的方法,为无人机集群的协同作战建立了完整的安全防护方案。区块链技术在为无人机系统提高健壮性、安全性、可扩展性的同时,也存在着众多局限,如主无人机要维护链码和账本,会占用很多内存;主无人机承担着决策、背书、控制从无人机等多项任务,会对本身的作战性能造成影响;GCS 对从无人机的控制权较弱,无法及时传达命令等。未来,我们将针对现存问题做进一步探索,为区块链技术与无人机集群的结合做更深入的研究。

参考文献

[1] LIU H F,SU J M,FU Y J. Summary of Research on Unmanned System Cluster and Its Countermeasure Technology[J]. Flying Missile,2018(11):35-40,91.

[2] GHAMRY K A,KAMEL M A,ZHANG Y. Multiple UAVs in forest fire fighting mission using particle swarm optimization [C]//2017 International Conference on Unmanned Aircraft Systems (ICUAS). IEEE,2017:1404-1409.

[3] CHEN S J,ZHANG K,HE Y. High dynamic self-organizing drone network architecture design and model research[J]. Computer Science,2015,42(2):50-54.

[4] JAVAID A Y,SUN W,DEVABHAKTUNI V K, et al. Cyber security threat analysis and modeling of an unmanned aerial vehicle system[C]//2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE,2012:585-590.

[5] ANDROULAKI E,BARGER A,BORTNIKOV V, et al. Hyperledger fabric:a distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. 2018:1-15.

[6] DUAN H B,SHEN Y K,WANG Y, et al. Hot reviews in the field of drones in 2018[J]. Science & Technology Review,2019,37(3):82-90.

[7] DUAN H B,QIU H X,CHEN L, et al. Research Prospects of UAV Autonomous Cluster Technology[J]. Science & Technology Review,2018,36(21):90-98.

[8] JENSEN I J,SELVARAJ D F,RANGANATHAN P. Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs)[C]//2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE,2019:1-7.

[9] RODDAY N M,SCHMIDT R O,PRAS A. Exploring security vulnerabilities of unmanned aerial vehicles[C]//NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE,2016:993-994.

[10] SEDJELMACI H,SENOUCI S M,ANSARI N. Intrusiondetection Andean framework againstlethaltacksin UAV-aided Networks:A Bayesiangame-theoretic metrology[J]. IEEE Transformaton International Transportation Transportation Systems, 2016(99):1-11.

tion at Scale[C]// International Conference on Learning Representations(ICLR 2021). 2020.

[8] WU H,XIAO B,CODELLA N,et al. CvT: Introducing Convolutions to Vision Transformers[C]// Proceedings of the IEEE/ CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2021.

[9] LI Y,ZHANG K,CAO J,et al. LocalViT: Bringing Locality to Vision Transformers[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). 2021.

[10] BHOJANAPALLI S,CHAKRABARTI A,GLASNER D,et al. Understanding Robustness of Transformers for Image Classification[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2021.

[11] NAKASHIMA K,KATAOKA H,MATSUMOTO A,et al. Can Vision Transformers Learn without Natural Images? [J]. arXiv: 2103. 13023.

[12] JAMAL M A,BROWN M,YANG M H,et al. Rethinking Class-Balanced Methods for Long-Tailed Visual Recognition From a Domain Adaptation Perspective[C]// Proceedings of the IEEE/

CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020.

[13] SOHN K,BERTHELOT D,CARLINI N,et al. FixMatch: Simplifying Semi-Supervised Learning with Consistency and Confidence[C]// Advances in Neural Information Processing Systems (NeurIPS). Curran Associates, Inc. ,2020;596-608.

[14] XIE Q,LUONG M T,HOVY E,et al. Self-TrainingWith Noisy Student Improves ImageNet Classification[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020.

[15] KURNIABUDI,STIAWAN D,DARMAWIJOY O,et al. CIC-IDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection[J]. IEEE Access,2020,8:132911-132921.



YANG Yue-lin, born in 1994, master, engineer. His main research interests include network security and deep learning.

(上接第 532 页)

[11] YOON K,PARK D,YIM Y,et al. Security authentication system using encrypted channel on uav network[C]// 2017 First IEEE International Conference on Robotic Computing (IRC). IEEE,2017;393-398.

[12] GORENFLO C,LEE S,GOLAB L,et al. Fastfabric: Scaling hyperledger fabric to 20 000 transactions per second[C]// 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE,2019;455-463.

[13] H CHAO,MAHESHWARI A,SUDARSANAN V,et al. UAV traffic information exchange network[OL]. [http://dx. doi. org/ 10. 252018;14/6. 2018-3347](http://dx.doi.org/10.252018;14/6.2018-3347).

[14] 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. PerComWorkshops,2017;618-623.

[15] LIANG X,ZHAO J,SHETTY S,et al. Towards data assurance and resilience in IoT using blockchain[C]// MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE,2017;261-266.

[16] BOZIC N,PUJOLLE G,SECCI S,A tutorial on blockchain and applications to secure network control-planes[C]// 2016 3rd Smart Cloud Networks Systems. SCNS,2016;1-8.

[17] VADLAMANI S,EKSIOGLU B,NANDI H M,et al. Jamming attacks on wireless networks: A taxonomic survey[J]. Int. J. Prod. Econ. ,2016(172);76-94.

[18] ZHOU Y. Summary of UAV Ground Station Development [J]. Aviation Electronics Technology,2010,41(1):1-6.

[19] CAMPION M,RANGANATHAN P,FARUQUE S. UAV swarm communication and control architectures: a review[J]. Journal of Unmanned Vehicle Systems,2018,7(2):93-106.

[20] MCGOVERN S. Blockchain for Unmanned Aircraft Systems [R]. John A. Volpe National Transportation Systems Center (US),2020.

[21] JENSEN I J,SELVARAJ D F,RANGANATHAN P. Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs)[C]// 2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE,2019:1-7.



WANG Yu-chen, born in 1997, post-graduate. Her main research interests include blockchain and recommendation system.



XU Li-zhen, born in 1963, professor. His main research interests include database technology, software engineering and enterprise information.