面向无人机集群的认证及密钥同步协议研究

杨竞　曾玲　王小骥　刘星江
（中国电子科技集团公司第三十研究所　四川成都　611041）

摘　要：针对无人机集群的组网安全，设计了一种面向无人机集群的认证及密钥同步协议。首先利用改进的门限秘密共享方案进行预处理操作生成系统参数和秘密共享密钥并分发，然后簇首节点根据秘密共享密钥与成员节点进行双向身份认证并进行密钥同步，形成簇内群组密钥，最后给出了协议的正确性、安全性和性能分析，分析结果表明协议具有机密性、完整性、新鲜性、可认证和抗合谋攻击性，通信复杂度为 O（n）。

关键词：无人机集群；门限密码；双向认证；密钥同步

中图分类号：TP391.9　　文献标志码：A　　文章编号：

Research on Authentication and Key Synchronization Protocol for Drone Cluster

YANG Jing [1]ZENG Ling　WANG Xiaoji　　LIU Xingjiang

(1. No.30 Institute of CETC, Chengdu Sichuan 611041, China)

Abstract: In order to ensure the network security of UAV clusters, a UAV cluster-oriented authentication and key synchronization protocol is designed.Firstly, an improved threshold secret sharing scheme is used for preprocessing operations to generate system parameters and secret sharing keys and distribute them.　Then, the cluster head node performs mutual authentication with member nodes based on the secret sharing keys and performs key synchronization to form a cluster-wide group key.　Finally, the correctness, security, and performance analysis of the protocol are provided.The analysis results show that the protocol has confidentiality, integrity, freshness, authenticity, and resistance to collusion attacks, with a communication complexity of O（n）.

Key words: Drone Cluster; Threshold Cryptography; Mutual Authentication; Key Synchronization

0　引言

在军事领域中，无人机在现代战争中大量使用，但由于单个无人机功耗不足、载荷受限的情况难以满足无人机协同任务、联合作战的需求。随着无人机技术和智能协同的发展，无人机集群化概念近几年来一直是世界各国竞相发展的重点[1]。

近年来，群体智能技术成为无人机集群发展的重要方向之一，如蚁群算法[2]、粒子群算法[3]应用于无人机集群组网任务协同分配，人工鱼群算法[4]、狼群算法[5]应用于无人机集群智能寻优组网、协同控制。与传统的点对点的通信模式不同，无人机集群组网不受地面站的控制，集群中的节点组网具有自主组网、互联互通、动态变化的特点[6]。与此同时，无人机集群的组网安全问题也是国内外研究热点之一。无人机集群中各个节点之间通信使用开放的无线信道，导致无人机集群内部通信很容易遭受攻击者的侦听、篡改、伪造、重放、仿冒身份攻击。文献[6]论述针对无人机的常见攻击手段，攻击者可以使用特定工具向无人机发送错误的命令，干扰无人机正常的飞行路径。文献[7]提出一种利用 MAVlive 协议漏洞的方法，可以禁止无人机执行当前任务。文献[8]提出针对无人机集群的攻击策略，通过伪造

通过认证的节点的信息，对集群内其他节点进行诱骗，迟误无人机集群所有节点的集合时间。面对着针对无人机集群攻击手段的愈发丰富的情况，为确保无人机集群组网安全可靠，无人机集群内节点在组网时需要确保节点间的身份认证和密钥的同步。

无人机集群内节点数量不确定，组网成员需要根据作战任务随时变换，依靠传统的端端密钥协商方案显然难以满足无人机集群的需求。为满足无人机集群的特定，确保集群内节点之间的安全保密通信，建立一个集群内同步的工作密钥是一种好的解决思路。文献[9]设计了一种适用于移动自组网的同步工作密钥协商方案，该方案使用基于三叉树的密钥管理模型进行群组内密钥的同步，并支持节点的动态变换，但是该方案没有身份认证机制，同时通信开销和计算开销较大，难以满足实际使用。文献[10]提出了一种无中心群组密钥协商协议，该协议支持群组间成员的动态变换，满足多种网络拓扑结构，同时可以抵抗拒绝服务攻击，但是存在着节点数量的限制，无法支撑大量节点同时进行协商，而且无法抵挡内部攻击。结合无人机集群自主组网、互联互通、动态变化的特点和集群内节点通信易被篡改、伪造、重放、仿冒身份攻击的限制，设计一个满足无人机集群节点身份认证和密钥同步的方案是解决无人机集群安全通信的关键。

2 无人机集群认证及密钥同步协议

本文协议采用基于秘密共享的方式，基于文献[11]的思想设计无人机集群认证及密钥同步协议。无人机根据预设的门限秘密共享方案，生成系统公开参数和秘密份额，地面站将参数和密钥发送给无人机。在使用无人机作为中继时，无人机的中继节点与普通节点之间存在着互相认证的问题，如果有非法的无人机进入无人机集群中冒充中继节点发送伪造的信息，则会使整个无人机集群面临被瘫痪的风险。为了防止这种情况发生，一种可靠的中继节点与普通节点之间的双向认证协议是必须的。当有外部节点需要加入时，需要与普通节点进行双向认证。簇首节点根据认证结果判断普通节点的身份是否合法，并计算出新的工作密钥发送给普通节点。普通节点接收到新的工作密钥后，使用存储的密钥对工作密钥进行解密，并更新本地的密钥。认证完成后，无人机集群可以使用新的工作密钥进行安全通信。

2.1 预处理工作

在地面站，我们将所有无人机视为秘密分发者，运用文献[11]改进的门限秘密共享方案，为每个无人机生成一套系统公开参数和一个秘密份额。在此过程中，地面站需要确保所有无人机的系统公开参数和密钥的安全性，防止泄露和被攻击。同时，每架无人机也要保证自己所对应的秘密份额不被泄露和被攻击，过程如图 2 所示：

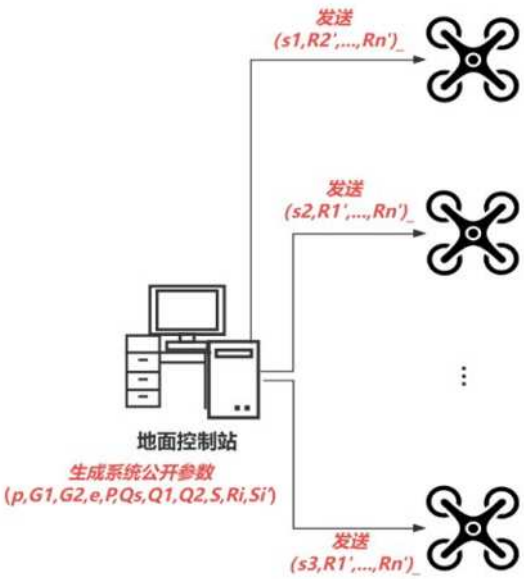

图 1 无人机集群预处理过程

①根据 2.2 节中的改进的门限秘密共享方案，首先在地面站将所有无人机都视为秘密分发者，生成 n 套系统公开参数和 n 个秘密$s_i,(i = 1,2,\ldots,n)$，n 为无人机的数量。其中，可根据具体任务来决定$(G_1,+)$和$(G_1,\cdot)$循环群是否变换；

②地面站根据秘密s_i分别计算出每个无人机为秘密分发者对应参与者的密钥$R_i',(i = 1,2,\ldots,n)$，将秘密分发者的秘密和对应其余参与者的密钥和参数分别发送给所有的无人机。

2.2 无人机集群认证及密钥同步协议

中继节点与普通节点构成的无人机集群作战时会遇到普通

节点被击毁、能量耗尽等情况，此时需要外部节点进行补充。但是由于在中继式无人机集群网络的拓扑结构中，中继节点已经承担了大量的计算指挥通信作用，为了减少中继节点的额外损耗，需要外部节点拥有与普通节点直接通信联系完成作战任务的能力。

外部节点若需要与普通节点之间进行联系，首先要互相认证，协议流程如图 3 所示：

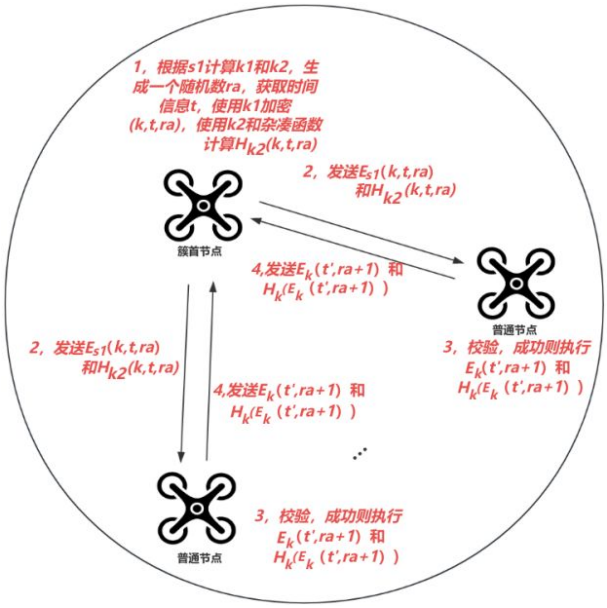

图 2 无人机集群簇首节点与普通节点双向认证及密钥同步流程

①根据被选择成为簇首节点的无人机根据S_1计算得到用于对称加密的密钥k_1和用于杂凑函数 HMAC 模式的密钥k_2，然后生成一个随机数ra同时获取当前的时间信息t用于防止重放攻击，再生成一个随机数k用于后续无人机集群安全通信的工作密钥k。利用k_1对(k,t,ra)进行加密，得到$E_{k_1}(k,t,ra)$，利用k_2对(k,t,ra)进行 HMAC 模式的杂凑函数处理得到$H_{k_2}(k,t,ra)$；

②簇首节点将$E_{k_1}(k,t,ra)$和$H_{k_2}(k,t,ra)$进行广播给集群内的普通节点无人机；

③集群内的普通节点在接收到簇首节点发送的$E_{k_1}(k,t,ra)$和$H_{k_2}(k,t,ra)$后，根据自身存储R_i计算得到相应的$k_{i,1}'$和$k_{i,2}'$。然后使用$k_{i,1}'$和对称算法对$E_{k_1}(k,t,ra)$进行解密$D_{k_{i,1}'}(E_{k_1}(k,t,ra))$得到$(k,t,ra)$。随后使用$k_{i,2}'$和杂凑函数 HMAC 模式计算$H_{k_{i,2}'}(k,t,ra)$，验证$H_{k_{i,2}'}(k,t,ra)$与$H_{k_2}(k,t,ra)$是否相等，若不相等则丢弃接收的数据，若相等则认可簇首节点的身份。再随后获取当前时间信息t'，并将ra进行加 1 处理，使用簇首节点发送的工作密钥k对$(t',ra+1)$进行加密得到$E_k(t',ra+1)$，并对$E_k(t',ra+1)$使用工作密钥k和杂凑函数 HMAC 模式计算$H_k(E_k(t',ra+1))$；

④无人机普通节点将$E_k(t',ra+1)$和$H_k(E_k(t',ra+1))$发送至簇首节点。

通过步骤①–④，簇首节点收到各个普通节点返回的$E_k(t',ra+1)$和$H_k(E_k(t',ra+1))$，需要首先计算$H_k(E_k(t',ra+1))$是否和一同发送的$E_k(t',ra+1)$是否相等作为认证的结果，然后计算$D_k(E_k(t',ra+1))$得到$(t',ra+1)$，判断时间t'和t的关系，再判断$ra+1$是否大于ra，作为防重放攻击的手段。若上述结果都正确，则完成对普通节点的认证。

3 协议安全性分析

协议的地面站预处理过程都是需要工作人员进行处理，有效的人员控制可以保证地面站预处理过程的安全性。协议的认证及密钥同步流程中，每一个在无线信道传输步骤中协议采用加密算法保证传输信息的机密性，采用杂凑函数 HMAC 模式保证信息的完整性。同时为了保证传输信息的新鲜性，协议采用时间戳加随机数的方式，若敌手通过截取无人机之间的通信数据进行重放攻击，因为敌手无法获取密钥，改变不了消息明文数据。无人机节点通过时间和随机数累加方式可以轻松地判断出接收的信息是否是被重复利用地，有效地保证了消息是新鲜的。

协议中步骤①–③的过程中，只有簇首节点发送的数据才可以被普通节点正确的解密，其余节点发送的数据无法被解密，完成普通节点对簇首节点认证的过程。步骤④过程中，簇首节点通过自身在前面步骤中发送的密钥正确解密接收的信息，就会被认可为该无人机集群成员，其余的敌手发送的数据无法被解密，完成了簇首节点对于普通节点的认证。所以协议完成簇首节点和普通节点之间的双向认证，达到了双向可认证性的结果。同时，基于文献[]中安全性证明，可知协议具备可抵抗合谋

攻击。

通过上述论述，协议具有机密性、完整性、新鲜性、可认证性和抗合谋攻击的能力。

4 结语

本文针对无人机集群组网安全，利用门限秘密共享的思路，在基于文献[11]的基础上面向分簇结构的无人机集设计了一个簇首节点和成员节点双向认证和密钥同步协议。协议分为地面站秘密注入阶段和组网身份认证及密钥同步阶段。地面站人工操作保证了秘密注入的合法性，组网阶段双向认证确保了簇首节点和成员节点的身份认证，密钥同步使簇内成员间拥有了同步的群组密钥。在协议过程中，利用对称函数保证了协议过程的机密性不被敌手侦听，利用杂凑函数 HMAC 模式保证了协议的完整性不被敌手篡改，利用时间戳加随机数保证了协议的新鲜性不被敌手重放攻击，利用秘密共享技术和协议的流程保证了可认证性不被敌手伪冒。后续研究的重点在于簇与簇之间的成员快速认证及密钥同步协议。

参考文献：

[1] 谷康.外军无人蜂群作战概念研究进展及分析[J].航空兵器，2022，29（1）：52-57.

[2] Brand M, Masuda M, Wehner N,et al.Ant Colony Optimization algorithm for robot path planning[C]. 2010 International Conference On Computer Design and Applications, Qinghuangdao, 2010.

[3] Butenko S, Murphey S, Pardalos P. Cooperative Control: Model, Applications and Algorithms[M]. Kluwer Press, 2006.

[4] 曹建秋,张广言,徐鹏.A*初始化的变异灰狼优化的无人机路径规划[J].计算机工程与应用，2022，58(4):275-282.

[5] 袁德平.基于混合群智能算法的无人机集群任务分配[J].中国电子科学研究院学报,2023,18(06):531-538+553.

[6] Chamola V, Kotesh P, Agarwal A, et al. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques[J]. Ad hoc networks, 2021, 111: 102324.

[7] Kwon Y M, Yu J, Cho B M, et al. Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles[J]. IEEE Access, 2018, 6: 43203-43212.

[8] Huang X, Tian Y, He Y, et al. Exposing spoofing attack on flocking-based unmanned aerial vehicle cluster: A threat to swarm intelligence[J]. Security and Communication Networks, 2020, 2020: 1-15.

[9] Chien H Y, Lin R Y. Identity-based key agreement protocol for mobile ad-hoc networks using bilinear pairing[C]//IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06). IEEE, 2006, 1: 8-pp.

[10] Weidner M, Kleppmann M, Hugenroth D, et al. Key agreement for decentralized secure group messaging with strong security guarantees[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 2024-2045.

[11] 庞辽军;李慧贤;裴庆祺;柳毅;王育民.一个单方加密-多方解密的公钥加密方案[J].计算机学报,2012,35(05):1059-1066.

作者简介：杨　竞（1986—），男，博士，工程师，主要研究方向为网络空间安全、密码学；

曾　玲（1975—），女，硕士，研究院，主要研究方向为保密通信；

王小骥（1979—），男，学士，高级工程师，主要研究方向为信息安全与通信保密；

刘星江（1984—），男，硕士，高级工程师，主要研究方向为信息安全与通信保密。

--本课题得到国家自然科学基金企业创新发展联合基金重点项目（U19B2021）资助。