面向云边协同无人机网络的高效切换认证协议

芮立[1,2]，张雄伟[1]，杨吉斌[1]，徐伟光[1]
（1.陆军工程大学指挥控制工程学院，江苏 南京 210007；2.南京审计大学金审学院信息科学与工程学院，江苏 南京 210023）

摘　要：针对在云边协同环境中现有无人机网络切换认证协议存在认证效率低下、物理安全属性缺失等问题，提出一种基于物理不可克隆函数（PUF）的高效切换认证协议，在云边架构条件下实现了无人机在不同地面站间的轻量级切换认证。所提协议设计了匿名响应分割方法，利用加法同余思想对认证使用的挑战-响应对进行分割保护，增强了对机器学习攻击的防御能力。构建了基于中国剩余定理的动态挑战-响应对分片批量同步机制，实现区域内非实时数据预协商，提高了实时切换认证效率和切换稳定性。安全分析与性能评估表明，与现有协议相比，所提协议提供了更加全面的安全属性，且地面站的计算开销降低了 9.1% 以上，整体通信开销降低了 13.8% 以上。

关键词：无人机网络；云边协同；切换认证协议；物理不可克隆函数；中国剩余定理
中图分类号：TN918.4
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025111

Efficient handover authentication protocol for cloud-edge collaborative UAV networks

RUI Li[1,2], ZHANG Xiongwei[1], YANG Jibin[1], XU Weiguang[1]
1. School of Command and Control Engineering, Army Engineering University, Nanjing 210007, China
2. School of Information Science and Engineering, Nanjing Audit University Jinshen College, Nanjing 210023, China

Abstract: For current unmanned aerial vehicle (UAV) network handover authentication protocols in cloud-edge collaborative environments suffered from low efficiency and lack of physical security, an efficient handover authentication protocol based on physical unclonable function was proposed, which achieved lightweight handover authentication for UAV between different ground stations within a cloud-edge architecture. The protocol employed an anonymous response segmentation method using additive congruence to protect challenge-response pair (CRP) against machine learning attacks. A Chinese remainder theorem-based dynamic CRP fragmentation mechanism was developed for batch synchronization, enabling regional non-real-time pre-negotiation to enhance efficiency and stability during real-time handover authentication. Security analysis and performance evaluation demonstrate that the proposed protocol achieves enhanced security attributes while reducing computational overhead at ground stations by over 9.1% and overall communication costs by over 13.8% compared to existing protocols.

Keywords: UAV network, cloud-edge collaboration, handover authentication protocol, physical unclonable function, Chinese remainder theorem

收稿日期：2025–03–31；**修回日期：**2025–06–05
通信作者：张雄伟，xwzhang9898@163.com
基金项目：国家自然科学基金资助项目（No.62371469）；江苏省高等学校自然科学研究基金资助项目（No.19KJD120001）
Foundation Items: The National Natural Science Foundation of China (No.62371469), The Natural Science Research Project of Jiangsu Universities (No.19KJD120001)

0　引言

无人机（UAV，unmanned aerial vehicle）凭借其灵活部署、快速响应以及强大的环境适应能力，被广泛应用于物流运输、环境监测、低空交通等多个领域。通过与地面基础设施组建网络，UAV可以实现复杂场景下的协同工作[1]。然而，传统云计算中心架构由于地理距离较远，数据从现场传送到云端服务器需要较长时间，由此产生的延迟使其难以满足动态路径优化等时延敏感型任务的需求[2]。为了解决这一问题，云边协同UAV网络通过将此类任务从云端的网络控制中心（NCC, network control center）卸载至靠近UAV的边缘地面站（GS, ground station），从而有效降低通信成本和传输时延[3]。

在云边协同UAV网络中，由于GS覆盖范围有限，高速移动的UAV会频繁切换GS服务节点。低效的切换认证协议会增加切换时延，甚至造成通信中断[4]。此外，切换认证过程中UAV和GS必须能够防范中间人攻击、重放攻击等安全威胁[5]。更为严峻的是，UAV存在低空飞行行为，且边缘端GS大多部署在室外空间，这使得攻击者还有可能对这些网络节点进行物理捕获，进而在切换认证过程中伪造身份[6]。因此，设计具备抗物理攻击能力的轻量级UAV网络切换认证协议显得尤为重要。

现有云边协同UAV网络切换认证协议虽能够满足基本切换认证需求，但由于采用传统加密原语以及协议设计中固有的缺陷，仍然存在物理安全属性缺失和认证效率低下的问题。物理不可克隆函数（PUF, physical unclonable function）作为一种新型加密原语，凭借其抗物理攻击特性以及轻量化等优点受到广泛关注[7]。PUF安全认证机制通过比对存储响应值与生成响应值之间的一致性实现身份鉴权。由于响应值基于物理设备的不可克隆特性，该机制能够有效抵御物理捕获攻击。

传统基于静态挑战-响应对（CRP, challenge-response pair）的PUF认证协议依赖存储安全的强假设，需要GS在注册阶段为所有UAV预存大量原始CRP。此类方案不仅会产生显著的存储开销，更为严重的是，实际部署中显式存储的CRP面临泄露风险，使得认证过程易遭受机器学习（ML，machine learning）攻击[8]。针对上述问题，研究者提出一种基于动态CRP更新机制的改进方案。该方案在注册阶段仅存储UAV的单对或少量原始CRP，后续通过动态更新机制维持运行。这种改进不仅有效降低了CRP存储开销，同时显著提升了认证节点抵御ML攻击的能力。

然而，在多GS场景中，由于攻击面扩大，攻击者可并行采集存储在多个GS节点上的原始CRP数据从而缩短ML攻击周期。此外，动态CRP更新机制虽然在单GS场景中有效降低了存储成本，但其依赖的本地化CRP更新策略难以实现多GS节点间的状态同步，导致跨GS切换时认证信息不一致。综上所述，当前基于PUF的认证协议虽然增强了物理安全防护能力，但在多GS切换场景中，仍然存在安全和同步等方面的不足。因此，如何基于PUF加密原语，设计一种兼具高效率和高安全性的云边协同UAV网络切换认证协议，成为当前亟待解决的关键问题。

为了应对上述挑战，本文提出一种基于PUF的高效切换认证协议，旨在实现云边协同环境下UAV网络高效、稳定且安全的切换认证。本文的主要贡献如下。

1) 针对多GS场景，提出了一种面向云边架构的轻量级UAV网络切换认证协议。该协议将认证计算任务下沉至边缘端GS，通过本地化处理实现UAV在不同GS间高效的切换认证，同时利用PUF提升了UAV和GS抗物理攻击能力。

2) 设计了一种基于加法同余的匿名响应分割方法。该方法采用分片机制避免原始CRP显式存储，利用加法同余思想破坏CRP的映射关系，通过匿名配对有效阻断了攻击者通过身份标识逆向重建CRP的可能性。

3) 构建了一种基于中国剩余定理（CRT, Chinese remainder theorem）的动态CRP分片批量同步机制。该机制在预切换认证阶段，利用CRT提前完成局部区域内多GS动态CRP分片批量同步，提升了实时切换认证阶段的效率和稳定性。

4) 通过形式化和非形式化安全分析验证了本文协议的安全性能。与近年来同类协议相比，本文协议GS的计算开销降低了9.1%以上，整体通信开销降低了13.8%以上。

1　相关工作

安全高效的切换认证协议是实现云边协同UAV网络稳定通信的关键。文献[9]基于椭圆曲线

密码设计了一种用于城市空中交通的UAV网络切换认证协议，并将认证计算任务卸载至边缘服务器。然而，由于切换认证阶段涉及多方参与，通信次数增加。文献[10]提出用AES-RSA混合加密方法实现UAV切换，虽然在一定程度上提高了安全性，但RSA加密算法引入了额外的计算开销。文献[11]针对5G异构网络提出一种基于对称加密的轻量级认证协议，该协议虽然具有轻量化计算优势，但其安全性严重依赖密钥的保密性，同时冗余的交互流程降低了认证效率。值得注意的是，文献[12]通过使用初始认证阶段生成的切换令牌提升单次切换认证效率。然而，由于该协议在切换认证阶段不支持动态令牌生成，后续切换认证需要重新使用复杂的初始认证算法，整体切换认证效率降低。上述文献中的协议设计均没有考虑物理安全问题，UAV物理安全属性的缺失使得协议无法抵御UAV物理捕获攻击。

基于传统加密体制的认证协议普遍存在物理安全属性缺失与认证效率低下的问题。在此背景下，PUF凭借硬件指纹唯一性与响应不可预测性，为构建轻量级抗物理攻击认证协议提供了新的思路。文献[13]首次将PUF技术应用于UAV网络认证场景，提出一种基于预存储CRP的双向认证协议。该协议通过在GS预存储大量设备的CRP实现快速认证和密钥协商。然而，这种显式存储海量原始CRP的方式不仅显著增加了边缘服务器的存储开销，还为攻击者实施ML攻击创造了有利条件。为了缓解GS的存储压力，文献[14]提出PUF-区块链融合架构，通过智能合约将注册阶段生成的原始CRP列表上传至区块链。然而，随着网络规模增大，区块链共识机制存在的低吞吐量问题可能导致其难以满足实时认证需求。此外，这类协议中通常预存的CRP数量有限，长期运行过程中会出现CRP耗尽现象，且易遭受ML攻击，因此难以实际部署于云边协同UAV网络环境。

为了避免CRP耗尽导致的认证失败以及缓解边缘服务器的存储压力，文献[15]提出一种基于动态更新的CRP管理机制，但该协议仍显式存储原始CRP，使得攻击者可通过长期观测数据实施ML攻击。此外，文献[16]指出该协议缺乏不可链接性。文献[17]从隐私保护角度出发，为不同类型的数据建立独立会话密钥，并采用CRP逐次更新策略以降低存储压力。然而，该方案仍无法解决CRP可建模性问题。需要强调的是，现有这类协议主要针对单点认证场景，因缺乏同步机制，无法满足切换认证场景的需求。近年来，有学者提出可以利用CRT来解决移动物联网切换认证过程中跨节点同步问题。文献[18]结合预共享密钥机制提出一种基于CRT的同步方法，用于星地融合网络的切换认证。然而该方案在预切换认证阶段存在切换密钥明文传输和显式存储问题，易导致密钥泄露。随后，文献[19]基于混沌映射和CRT提出类似的解决方案用于航空通信网，该方案虽然解决了切换密钥明文传输的问题，但在面对物理攻击时仍存在脆弱性，无法有效防止攻击者获取存储的切换密钥。

针对攻击者通过CRP建模发起的ML攻击，现有防御机制主要采用信息隐藏与信息分割策略。文献[20]为了避免CRP显式存储，提出一种基于几何阈值秘密共享的认证协议，在数据库中用响应值的哈希替代原始响应值。但文献[21]指出该方法无法有效抵御数据泄露造成的伪造攻击。文献[22]提出多阶扩展CRP生成方法，通过增加响应维度的方式对明文进行隐藏，但这种方法基于认证双方在注册阶段即可安全通信的假设，无法扩展至大规模云边架构。文献[23]设计临时ID分割机制，利用异或操作隐藏原始CRP，然而固定分片规则使得攻击者可通过统计相关性分析重构原始响应。文献[24]创新性地采用分布式秘密共享存储CRP分片，该协议虽能抵御局部节点泄露，但Shamir门限机制的通信开销使其难以适用于时间敏感型应用场景。

综上所述，基于传统加密体制的UAV网络切换认证协议难以抵御UAV物理捕获攻击，而现有基于PUF的认证协议虽能够提升物理安全性，但均不满足云边架构场景下的高效切换认证需求。

2 系统概述

2.1 系统模型

本文构建的云边协同UAV网络系统模型如图1所示，主要包含NCC、GS和UAV这3类实体。

NCC作为系统中的可信实体，采用分布式架构部署于云端并具备强大的计算与存储能力，负责全网的管理调度、数据处理及系统参数的生成。此外，NCC承担UAV和GS的注册管理以及预切换认证阶段的计算工作。

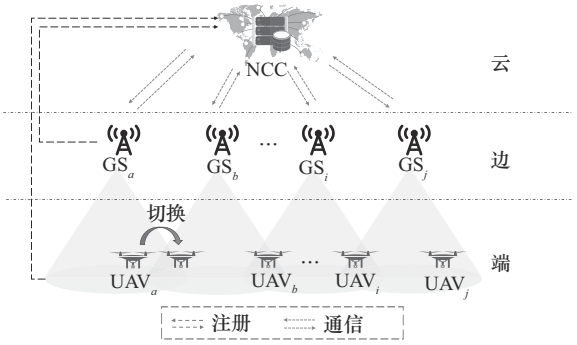


图1　云边协同UAV网络系统模型

GS属于半可信实体，作为边缘计算节点，GS具有中等计算能力和存储资源，可为区域内的UAV提供实时认证服务。由于部署于开放环境，GS存在易被物理捕获风险。此外，GS与NCC间通过预共享密钥进行通信，采用事件触发更新的方式向NCC发送位置信息、负载信息以及覆盖范围等状态信息。

UAV是资源受限的脆弱实体终端，仅具备有限的计算能力和存储空间。在无NCC协同情况下，UAV可与GS完成初始双向认证。此外，当UAV移动至不同GS的覆盖区域时，可与目标GS执行切换认证以维持通信连续性。

2.2　切换认证机制

当UAV从源GS覆盖范围进入目标GS覆盖范围时需要进行切换认证。本文根据切换认证计算任务的实时性需求，将整个流程划分为预切换认证阶段和切换认证阶段。

预切换认证阶段主要负责切换过程中非实时数据协商。UAV在飞行过程中不断探测与源GS之间的信号强度等参数信息，当触发预切换条件时（如信号强度持续低于预切换阈值），启动预切换认证机制。UAV通过源GS向NCC发送飞行轨迹、任务规划路径等信息。NCC根据这些信息构建预设时间窗口内UAV的轨迹分布预测模型，并分析收集到的GS负载、覆盖半径等状态信息，筛选出一组满足服务质量要求且通信覆盖区域与UAV预测飞行轨迹存在空间重叠的目标GS。最终，NCC利用CRT计算动态CRP分片等后续认证参数。

切换认证阶段主要负责切换过程中认证双方的实时认证。当UAV触发切换条件时（如信号强度持续低于切换阈值），启动实时切换认证。GS根据UAV切换请求解密动态更新CRP分片同步信息，认证双方基于动态CRP更新机制实现节点间认证交互。最终，认证双方完成切换认证并协商出用于安全通信的会话密钥。

2.3　威胁模型

在云边协同UAV网络中，实体间通过开放的无线信道进行通信，因此面临窃听、截获和分析等安全威胁。本文采用Dolev-Yao[25]攻击者模型，建立以下核心假设。

1) NCC是网络中唯一完全可信的实体，攻击者A不能获得存放在NCC上的关键数据。

2) 攻击者A可以窃听、截获、修改和删除公共信道上实体传输的消息。

3) 攻击者A可以对UAV和GS发动物理捕获攻击，但不能篡改节点的硬件设备。

4) 攻击者A可以通过查看存储在多个实体上的CRP明文信息发动ML攻击。

3　认证协议

本文认证协议分为系统初始化、注册阶段、初始认证、预切换认证、切换认证5个阶段。协议中的系统参数如表1所示。

表1　系统参数

符号	符号描述
ID_u,ID_g	UAV和GS的真实身份标识符
PID_u	UAV的假名身份标识符
TID_u	UAV的保密身份标识符
C,R	PUF的挑战值和响应值
$R_{u,1}$,$R_{u,2}$	UAV的响应值分片
n	随机数
t	时间戳
SK	会话密钥
pr	私钥
PU	公钥
$f_{PUF}(.)$	物理不可克隆函数
$f_{GEN}(.)$	模糊提取器生成函数
$f_{REP}(.)$	模糊提取器重构函数
$H(.)$	哈希函数
$\oplus$	异或运算

3.1　系统初始化

在这个阶段，NCC选择一个生成元是P的q阶

椭圆曲线、单向哈希函数$H(.)$、安全大素数p、身份标识符$\mathrm{ID}_{\mathrm{ncc}}$以及主密钥$K_s$。NCC通过哈希计算与GS的预共享密钥$k=H(\mathrm{ID}_{\mathrm{ncc}}\|K_s)$，并在网络中发布公共参数$\{\mathrm{ID}_{\mathrm{ncc}},P,H(.),p\}$。

3.2　注册阶段

1) GS注册

在这个阶段，GS完成设备注册，具体步骤如下。

步骤1　NCC为第i个GS生成唯一身份标识$\mathrm{ID}_{\mathrm{g}_i}$和大素数$\mathrm{pr}_{\mathrm{g}_i}$，并将$\{\mathrm{ID}_{\mathrm{g}_i},\mathrm{pr}_{\mathrm{g}_i},k\}$通过安全信道发送至GS。

步骤2　收到消息后，GS将$\mathrm{pr}_{\mathrm{g}_i}$作为私钥，并计算对应公钥$\mathrm{PU}_{\mathrm{g}_i}=\mathrm{pr}_{\mathrm{g}_i}P$。接着，GS利用安全挑战值$C_{\mathrm{g}_i}$计算$R_{\mathrm{g}_i}=f_{\mathrm{PUF}}(C_{\mathrm{g}_i})$以及隐藏后的私钥$\mathrm{PR}_{\mathrm{g}_i}=\mathrm{pr}_{\mathrm{g}_i}\oplus R_{\mathrm{g}_i}$。最后，GS将$\mathrm{PR}_{\mathrm{g}_i}$和$C_{\mathrm{g}_i}$保存在数据库中。

2) UAV注册

UAV注册阶段实体间的信息交互如图2所示，在这个阶段，UAV完成设备注册，具体步骤如下。

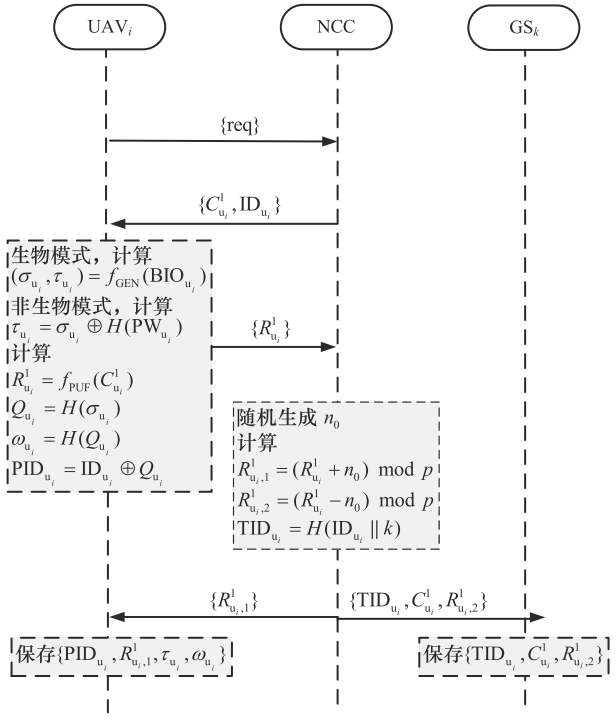


图2　UAV注册阶段实体间的信息交互

步骤1　UAV向NCC发送注册请求。NCC收到请求后，随机生成初始的挑战值$C^1_{\mathrm{u}_i}$和UAV的唯一标识符$\mathrm{ID}_{\mathrm{u}_i}$，并将$\{C^1_{\mathrm{u}_i},\mathrm{ID}_{\mathrm{u}_i}\}$通过安全信道发送至UAV。

步骤2　收到消息后，UAV通过内嵌的PUF计算$R^1_{\mathrm{u}_i}$，并根据Q_{u_i}计算假名$\mathrm{PID}_{\mathrm{u}_i}$，最后将$R^1_{\mathrm{u}_i}$返回给NCC。值得注意的是，用户可在支持生物模式的UAV上输入生物特征$\mathrm{BIO}_{\mathrm{u}_i}$，利用模糊提取器生成秘密值$\sigma_{\mathrm{u}_i}$和帮助值$\tau_{\mathrm{u}_i}$。对于不支持生物模式的UAV，用户随机生成$\sigma_{\mathrm{u}_i}$，并基于密码$\mathrm{PW}_{\mathrm{u}_i}$计算$\tau_{\mathrm{u}_i}$。

步骤3　收到返回的消息后，NCC生成随机数n_0，采用匿名响应分割方法计算$R^1_{\mathrm{u}_i,1}$和$R^1_{\mathrm{u}_i,2}$。接着，NCC利用预共享密钥k计算$\mathrm{TID}_{\mathrm{u}_i}$。最后，NCC通过安全信道将$\{R^1_{\mathrm{u}_i,1}\}$发送至UAV，并将$\{\mathrm{TID}_{\mathrm{u}_i},C^1_{\mathrm{u}_i},R^1_{\mathrm{u}_i,2}\}$发送至管理域内所有GS。

步骤4　UAV和GS收到消息后，分别将$\{\mathrm{PID}_{\mathrm{u}_i},R^1_{\mathrm{u}_i,1},\tau_{\mathrm{u}_i},\omega_{\mathrm{u}_i}\}$和$\{\mathrm{TID}_{\mathrm{u}_i},C^1_{\mathrm{u}_i},R^1_{\mathrm{u}_i,2}\}$存入数据库。

3.3　初始认证

初始认证阶段实体间的信息交互如图3所示，为了执行空中任务，UAV首先需要与当前区域边缘端的GS完成初始认证，具体步骤如下。

步骤1　UAV收到当前区域GS广播的消息$\{\mathrm{ID}_{\mathrm{g}_i},\mathrm{PU}_{\mathrm{g}_i}\}$后，通过用户输入的$\mathrm{PID}_{\mathrm{u}_i}$和密码（生物信息）恢复$\sigma^*_{\mathrm{u}_i}$。接着，UAV根据$\sigma^*_{\mathrm{u}_i}$计算$Q^*_{\mathrm{u}_i}$，如果不满足$H(Q^*_{\mathrm{u}_i})=\omega_{\mathrm{u}_i}$，认证终止。否则，UAV恢复真实身份$\mathrm{ID}_{\mathrm{u}_i}=\mathrm{PID}_{\mathrm{u}_i}\oplus Q^*_{\mathrm{u}_i}$，生成随机数$v_{\mathrm{u}_i}$和时间戳$t_1$，并计算$V_{\mathrm{u}_i}$、消息$M_1$以及消息$M_2$。最后，通过公共信道将消息$\{M_1,M_2,V_{\mathrm{u}_i},t_1\}$发送至GS。

步骤2　收到消息后，GS首先验证时间戳t_1的新鲜性。验证通过后，GS根据PUF响应值R_{g_i}恢复私钥$\mathrm{pr}_{\mathrm{g}_i}$。接着，GS通过椭圆曲线算法计算$V_{\mathrm{u}_i}\mathrm{pr}_{\mathrm{g}_i}$，进而解密消息$M_1$得到$\mathrm{ID}^*_{\mathrm{u}_i}$和响应值分片$R^{1*}_{\mathrm{u}_i,1}$。GS根据$\mathrm{ID}^*_{\mathrm{u}_i}$等关键参数计算认证消息$M^*_2$，如果不满足$M^*_2=M_2$，认证终止。否则，GS生成随机数$n_1$和时间戳$t_2$，并根据预共享密钥$k$计算$\mathrm{TID}_{\mathrm{u}_i}$，查询对应$\{C^1_{\mathrm{u}_i},R^1_{\mathrm{u}_i,2}\}$。完成查询后，GS通过恢复的参数$R^{1*}_{\mathrm{u}_i,1}$和查询到的参数$R^1_{\mathrm{u}_i,2}$重构$K_{\mathrm{u}_i}$。最后，GS根据$K_{\mathrm{u}_i}$计算消息$M_3$和$M_4$，并通过公共信道将消息$\{M_3,M_4,C^1_{\mathrm{u}_i},t_2\}$发送至UAV。

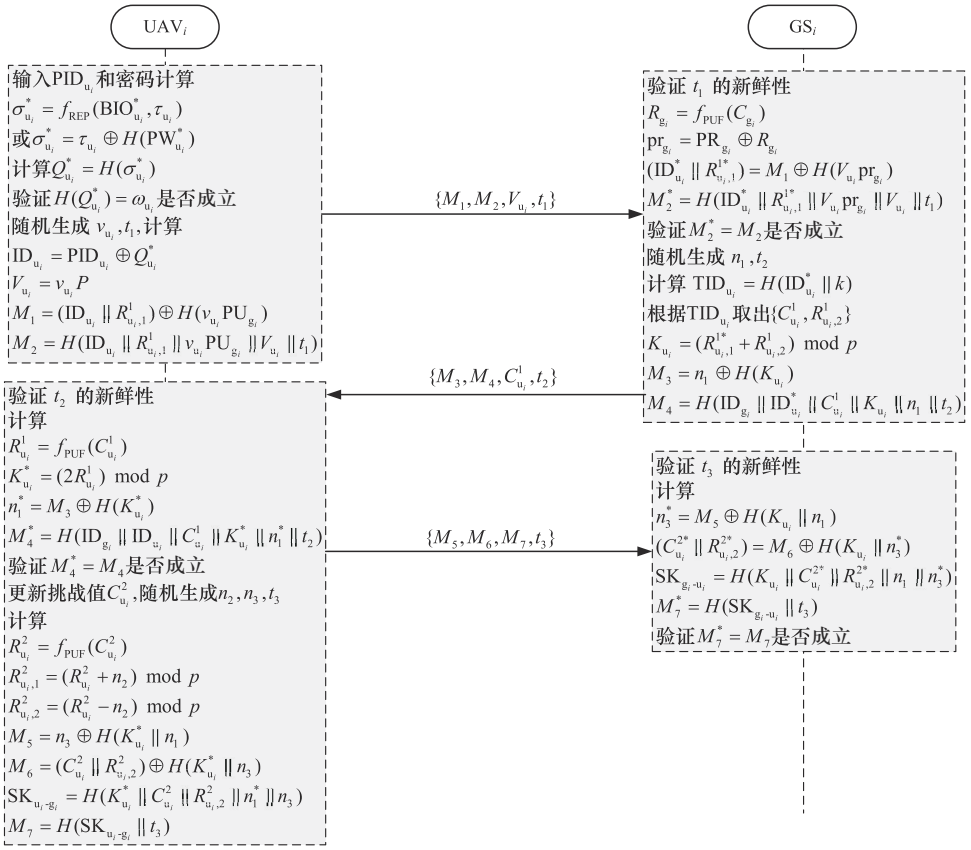


图3　初始认证阶段实体间的信息交互

步骤 3　收到消息后，UAV 首先验证时间戳 t_2 的新鲜性。验证通过后，将接收到的挑战值 $C^1_{u_i}$ 作为 PUF 的输入得到响应值 $R^1_{u_i}$，并以此计算对应参数 $K^*_{u_i}$。接着，UAV 根据 $K^*_{u_i}$ 恢复随机数 n^*_1 和认证消息 M^*_4。如果不满足 $M^*_4=M_4$，认证终止。否则，UAV 更新挑战值 $C^2_{u_i}$，随机生成 n_2、n_3 和 t_3，根据 $C^2_{u_i}$ 计算 PUF 响应值 $R^2_{u_i}$，并以此计算更新后的分片、消息 M_5 和消息 M_6。最后，UAV 通过 ID_{u_i}、$K^*_{u_i}$、随机数等关键参数计算出会话密钥 $SK_{u_i\text{-}g_i}$ 和认证消息 M_7，并将 $\{M_5,M_6,M_7,t_3\}$ 通过公共信道发送至 GS。

步骤 4　收到消息后，GS 首先验证时间戳 t_3 的新鲜性。验证通过后，GS 利用 K_{u_i} 恢复 n^*_3、$C^{2*}_{u_i}$ 以及 $R^{2*}_{u_i,2}$。接着，计算会话密钥 $SK_{g_i\text{-}u_i}$ 和认证消息 M^*_7。最后，GS 验证 $M^*_7=M_7$ 是否成立，如果成立，初始认证完成。

3.4　预切换认证

预切换认证阶段实体间的信息交互如图 4 所示，这个阶段主要完成切换认证流程中非实时性数据协商。NCC 会根据 UAV 和 GS 的状态信息提前为 UAV 选择一组可能发生切换的目标 GS，并计算用于后续实时切换认证所需的认证参数，具体步骤如下。

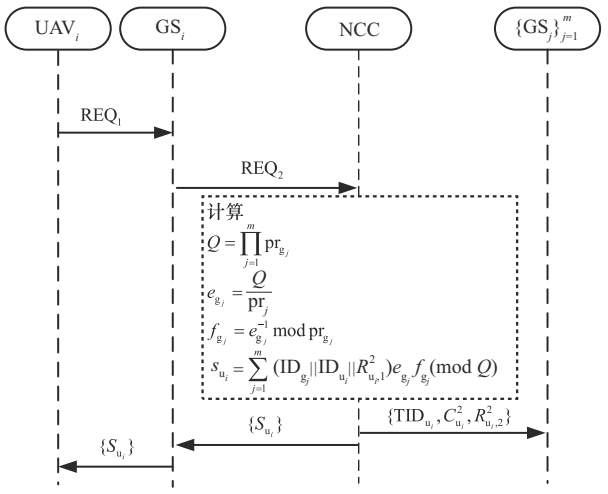


图4　预切换认证阶段实体间的信息交互

步骤 1　UAV 向当前连接的源 GS 发送用会话密钥加密的预切换认证请求消息 REQ_1:

$\{\mathrm{ID}_{u_i}, R^2_{u_i,1}, \mathrm{info}\}$，其中info包含UAV当前位置信息、飞行轨迹信息、任务路径规划信息等。

步骤2　源GS收到预切换认证请求后，根据ID_{u_i}计算TID_{u_i}，随后发送用预共享密钥加密的请求消息REQ_2:$\{\mathrm{ID}_{u_i}, R^2_{u_i,1}, \mathrm{info}, \mathrm{TID}_{u_i}, C^2_{u_i}, R^2_{u_i,2}\}$至NCC。

步骤3　NCC收到消息后，首先通过预共享密钥解密消息，并基于解析出的info字段构建UAV在预设时间窗口内的轨迹分布模型。接着，NCC通过评估相邻候选GS状态信息，筛选出m个满足服务质量要求的目标GS。完成上述操作后，NCC根据CRT以及预共享的大素数pr_{g_j}计算S_{u_i}。

步骤4　NCC通过公共信道将消息$\{\mathrm{TID}_{u_i}, C^2_{u_i}, R^2_{u_i,2}\}$发送至指定的多个目标GS，同时通过源GS将$\{S_{u_i}\}$转发至发起切换请求的UAV。至此，预切换认证协商完成。若协商成功，UAV将在后续切换过程中发送切换认证请求，否则，需重新发送初始认证请求。

3.5　切换认证

切换认证阶段实体间的信息交互如图5所示，这个阶段UAV与目标GS完成实时切换认证，并协商出用于安全通信的会话密钥，具体步骤如下。

步骤1　不同于初始认证阶段请求消息，UAV不需要执行椭圆曲线操作，仅向准备接入的目标GS发送切换认证请求消息$\{S_{u_i}\}$。

步骤2　收到消息后，目标GS首先通过内嵌的PUF恢复私钥pr_{g_j}，并通过私钥解密消息S_{u_i}得到$\mathrm{ID}^*_{g_j}$、$\mathrm{ID}^*_{u_i}$以及$R^{2*}_{u_i,1}$。这里，GS采用CRT解密消息，仅需一次轻量级模运算即可同步得到用于后续认证的相关参数。为了防止拒绝服务（DoS, denial of service）攻击，目标GS需要验证$\mathrm{ID}^*_{g_j} = \mathrm{ID}_{g_j}$是否成立，如果不成立，认证立即终止。否则，GS生成随机数n_4和时间戳t_4，通过预共享密钥k计算$\mathrm{TID}^*_{u_i}$，并以此检索得到$\{C^2_{u_i}, R^2_{u_i,2}\}$。接着，目标GS根据恢复的参数$R^{2*}_{u_i,1}$和查询到的参数$R^2_{u_i,2}$恢复完整$K_{u_i}$，再根据参数$K_{u_i}$计算消息$M_8$和$M_9$。最后，目标GS通过公共信道发送$\{M_8, M_9, C^2_{u_i}, t_4\}$至UAV。值得注意的是，这里采用匿名响应分割方法，UAV拥有的分片$R^{2*}_{u_i,1}$所对应的PID_{u_i}和GS拥有的分片$R^2_{u_i,2}$所对应的TID_{u_i}之间不存在直接映射关系。因此，即使这两部分信息显式存储，攻击者也无法合成正确的参数K_{u_i}。

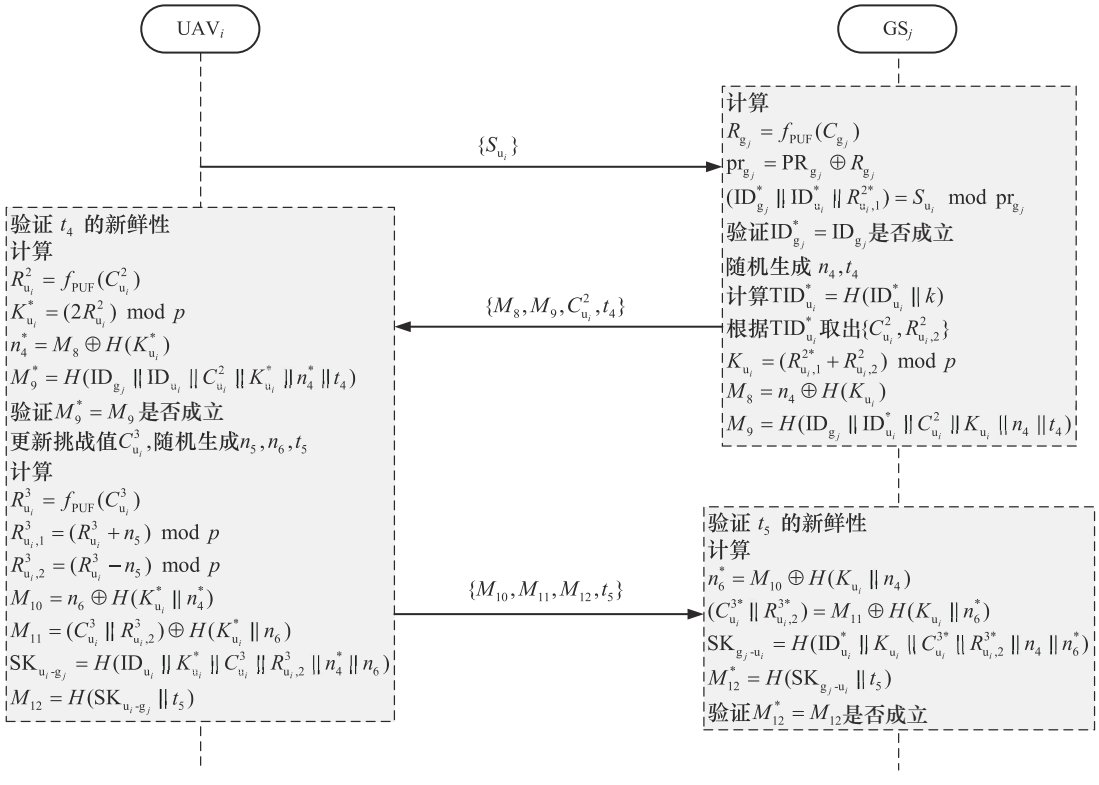


图5　切换认证阶段实体间的信息交互

步骤 3　UAV 收到消息后，首先验证时间戳 t_4 的新鲜性。验证通过后，UAV 将接收到的挑战值 $C_{u_i}^2$ 作为 PUF 的输入得到响应值 $R_{u_i}^2$，并以此计算得到对应参数 $K_{u_i}^*$。接着，UAV 根据 $K_{u_i}^*$ 恢复随机数 n_4^* 以及消息 M_9^*。如果不满足 $M_9^* = M_9$，则认证终止。否则，UAV 更新挑战值 $C_{u_i}^3$，随机生成 n_5、n_6 和 t_5，根据 $C_{u_i}^3$ 计算 PUF 响应值 $R_{u_i}^3$，并以此计算更新后的分片、消息 M_{10} 和消息 M_{11}。最后，UAV 根据 ID_{u_i}、$K_{u_i}^*$、随机数等关键参数计算出会话密钥 $SK_{u_i-g_j}$ 以及认证消息 M_{12}，并将 $\{M_{10},M_{11},M_{12},t_5\}$ 通过公共信道发送至 GS。

步骤 4　收到消息后，GS 首先验证时间戳 t_5 的新鲜性，新鲜性验证通过后，利用 K_{u_i} 恢复 n_6^*、$C_{u_i}^{3*}$ 以及 $R_{u_i,2}^{3*}$。接着，计算会话密钥 $SK_{g_j-u_i}$ 和认证消息 M_{12}^*。最后，GS 验证 $M_{12}^* = M_{12}$ 是否成立，如果成立，切换认证完成。

4　安全分析

4.1　非形式化分析

1) 双向认证。在本文协议中，UAV 首先发送切换认证请求至 GS。GS 在收到认证请求后，计算动态认证参数，并发送消息 M_9 至 UAV。UAV 通过验证 $M_9^* = M_9$ 是否成立来确认 GS 身份的合法性。同理，GS 也需要通过验证 $M_{12}^* = M_{12}$ 是否成立来确认 UAV 身份的合法性。因此本文协议满足双向认证要求。

2) 匿名性和不可链接性。本文协议采用分层标识隐藏策略，在切换认证阶段，UAV 真实身份 ID_{u_i} 分别被替换为假名标识符 PID_{u_i}（UAV 侧）和加密标识符 TID_{u_i}（GS 侧）。值得注意的是，在整个通信过程中，所有身份标识均未以明文形式传输。因此，攻击者既无法从传输数据中推导出真实身份 ID_{u_i}，也无法建立 TID_{u_i} 和 PID_{u_i} 之间的映射关系，从而确保身份信息的匿名性和不可链接性。

3) 完美前向安全。本文协议会话密钥 SK 的生成融合了长期秘密参数与短期秘密参数。即使长期秘密参数 ID_{u_i} 或 k 泄露，攻击者仍然无法通过关联响应值分片或 PUF 重新生成的方式获得短期秘密参数 K_{u_i}，且每次会话均引入动态随机数 n_4 和 n_6。因此，攻击者无法根据当前会话密钥逆向推导先前会话密钥或预测后续会话密钥。

4) 伪装攻击。针对 GS 伪装攻击，攻击者需要伪造 $\{M_8,M_9,C_{u_i},t_4\}$。然而，消息 M_8 和 M_9 均包含秘密值 K_{u_i}，恢复该值所需的私钥被 GS 的 PUF 所保护。根据 PUF 的物理不可克隆特性，攻击者无法通过物理探测获取有效私钥信息，因此无法构造合法认证消息。同理，UAV 伪装攻击需伪造 $\{M_{10},M_{11},M_{12},t_5\}$。消息 M_{10}、M_{11} 和 M_{12} 均包含 $K_{u_i}^*$，然而 $K_{u_i}^*$ 的正确性依赖于 UAV 设备的 PUF 响应，攻击者同样无法复制目标设备的物理特征，因此不能通过伪造消息进行伪装攻击。

5) 中间人攻击。假设攻击者具备截获并篡改公共信道消息的能力。攻击者需构造合法的消息发送给 GS 和 UAV。但由于攻击者无法通过 UAV 的 PUF 获得 $K_{u_i}^*$，也无法通过 ID 之间的映射获得完整响应值，因此无法合成合法的加密消息 M_9 和 M_{12}。

6) 重放攻击。本文协议在公共信道传送的认证消息 M_9 和 M_{12} 中采用时间戳-随机数双重防护机制。接收方在收到消息后会验证时间戳的新鲜性。此外，协议还通过更新每轮认证的随机数，进一步确保历史认证消息无法通过重放通过验证，从而消除重放攻击威胁。

7) DoS 攻击。攻击者试图向 GS 发送大量虚假认证请求，使其无法向合法 UAV 提供正常服务。在认证过程中，攻击者需要向 GS 提供消息 $\{S_{u_i}\}$。GS 使用自己的私钥解密该消息，当 GS 验证 $ID_{g_j}^* = ID_{g_j}$ 不成立后，认证立即终止。该方法使得非法请求在初始阶段即被过滤，能够降低 GS 的计算负载，缓解 DoS 攻击的影响。

8) UAV 物理捕获攻击。本文协议中，会话密钥中 K_{u_i} 是根据 UAV 的 PUF 响应值生成的秘密值。然而，攻击者即使物理捕获 UAV，也无法恢复该 UAV 正确的 PUF 响应值。这是因为攻击者对设备的任何篡改都会影响 PUF 函数的输出响应值，本文协议可以抵御 UAV 物理捕获攻击。

9) GS 物理捕获攻击。当攻击者捕获 GS 后，试图读取存储在 GS 上的私钥信息，然而该参数受到 GS 的 PUF 响应值保护。一旦攻击者分析 GS 存储的参数，PUF 的输出将发生变化[26]。因此，攻击者同样无法获得存储在 GS 上的关键认证参数，本文

协议可以抵御GS物理捕获攻击。

10) 短期密钥泄露（ESL, ephemeral secret leakage）攻击。本文协议中会话密钥的机密性由长期密钥和短期密钥组成。因此，即使攻击者通过侧道攻击等方式获取短期密钥，在没有$\mathrm{ID}_{\mathrm{u}_i}$和$k$等长期密钥的情况下依然无法计算出正确的会话密钥。

11) 恶意UAV撤销。在UAV网络中，可能存在合法UAV传递恶意消息的情况。匿名策略增加了恶意UAV追踪的难度，但在本文协议中，GS可以通过私钥解密消息S_{u_i}，从而获得UAV的真实身份标识$\mathrm{ID}_{\mathrm{u}_i}$。当UAV出现恶意行为时，NCC会及时根据GS上传的$\mathrm{ID}_{\mathrm{u}_i}$对恶意UAV身份进行注销。

12) ML攻击。攻击者试图通过从多个分布式节点收集足够的原始CRP，从而对合法UAV的PUF进行建模。然而，本文协议采用匿名响应分片策略，正确的响应值被分割成$R_{\mathrm{u}_i,1}$和$R_{\mathrm{u}_i,2}$这2个部分，分别保存在UAV和GS上，且无法根据$\mathrm{PID}_{\mathrm{u}_i}$或$\mathrm{TID}_{\mathrm{u}_i}$关联数据。因此，攻击者无法建模原始CRP映射关系，可以有效抵御ML攻击。

4.2 形式化分析

为了验证所提协议的语义安全性，本文使用了真实或随机（ROR, real-or-random）模型进行形式化证明。

定义1 在本文的ROR模型中，系统参与者包括UAV和GS。第k个会话实例中，参与者分别被记为$I_{\mathrm{u}_i}^k$和$I_{\mathrm{g}_i}^k(I_{\mathrm{g}_j}^k)$。攻击者$A$可以伪造、窃听、修改公共信道传递的消息，表2模拟了A的能力。

定义2 攻击者A在多项式时间内最多执行一次$\mathrm{Test}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k,\alpha)$和多次其他查询来确定返回值$\alpha$的正确性，其中不能通过$\mathrm{Reveal}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k)$来直接获得会话密钥。如果$\alpha=1$，说明$A$猜测成功。那么$A$在多项式时间里成功打破协议$S$的会话密钥的语义安全概率为

$$\mathrm{Adv}_S^A=\left|2\mathrm{PR}(\alpha=1)-1\right| \tag{1}$$

如果对于一个小到可以忽略的ζ，满足$\mathrm{Adv}_S^A<\zeta$，则称协议S是语义安全的。

定理1 在多项式时间内，攻击者A获取会话密钥的优势为

$$\mathrm{Adv}_S^A\leqslant\frac{q_{\mathrm{H}}^2}{2^{l_{\mathrm{H}}}}+\frac{q_{\mathrm{P}}^2}{2^{l_{\mathrm{P}}}}+\frac{q_{\mathrm{S}}}{2^{l-1}} \tag{2}$$

其中，q_{H}、q_{P}和q_{S}分别代表哈希操作、PUF操作和发送查询的执行次数，l_{H}代表哈希的长度，l_{P}表示PUF输出响应值的长度。

证明 $\mathrm{Game}_i(i=0,1,2,3,4)$用来模拟攻击者$A$发起的攻击。$\mathrm{Suc}_i(i=0,1,2,3,4)$表示$A$能够在$\mathrm{Game}_i$中成功猜中随机位$\alpha$的事件。

Game_0：在此次博弈中，攻击者A首先发起攻击，根据定义可得到

$$\mathrm{Adv}_S^A=\left|2\mathrm{PR}\left(\mathrm{Suc}_0\right)-1\right| \tag{3}$$

Game_1：在此次博弈中，A可以获取公共信道上传输的所有消息。A执行查询$\mathrm{Execute}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k)$和$\mathrm{Test}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k,\alpha)$。在切换认证过程中$A$想要通过公共信道获取的信息计算$\mathrm{SK}_{\mathrm{u}_i\text{-}\mathrm{g}_j}$，则需要解决哈希和PUF碰撞问题。因此，在窃听攻击中，Game_1和Game_0的优势是相同的，可得到

$$\mathrm{PR}\left(\mathrm{Suc}_0\right)=\mathrm{PR}\left(\mathrm{Suc}_1\right) \tag{4}$$

Game_2：此次博弈中模拟了哈希碰撞攻击。A可以通过哈希查询发起攻击，但根据生日悖论的定

表2 ROR模型下查询及对应描述

查询	描述
$\mathrm{Execute}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k)$	A可以窃听$I_{\mathrm{u}_i}^k$、$I_{\mathrm{g}_i}^k$或$I_{\mathrm{g}_j}^k$在公共信道上传输的所有消息
$\mathrm{Send}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k,m)$	A可以伪造消息m，并发送给$I_{\mathrm{u}_i}^k$、$I_{\mathrm{g}_i}^k$或$I_{\mathrm{g}_j}^k$。如果m正确，$I_{\mathrm{u}_i}^k$、$I_{\mathrm{g}_i}^k$或$I_{\mathrm{g}_j}^k$收到消息后，处理并产生一个回复消息给A
$\mathrm{Corrupt}(I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k)$	A可以通过此查询来破坏GS，从而获得存储在GS上的认证信息
$\mathrm{Corrupt}(I_{\mathrm{u}_i}^k)$	A可以通过此查询来破坏UAV，从而获得存储在UAV上的认证信息
$\mathrm{Reveal}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k)$	A可以通过此查询获取$I_{\mathrm{u}_i}^k$、$I_{\mathrm{g}_i}^k$或$I_{\mathrm{g}_j}^k$之间的会话密钥
$\mathrm{Test}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k,\alpha)$	该查询会生成一个随机数α，若$\alpha=1$，则A获得正确的会话密钥，否则A获得一个随机数

义，可得到

$$\left|\mathrm{PR}\left(\mathrm{Suc}_2\right)-\mathrm{PR}\left(\mathrm{Suc}_1\right)\right|\leqslant\frac{q_{\mathrm{H}}^2}{2^{1+l_{\mathrm{H}}}}\tag{5}$$

Game_3：在此次博弈中，A 执行查询 $\mathrm{Corrupt}(I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k)$ 和 $\mathrm{Corrupt}(I_{\mathrm{u}_i}^k)$，获取存储在 UAV 和 GS 上的认证信息，其中 R_{u_i} 被 PUF 加密保护。根据 PUF 的唯一性，不同的 PUF 即使在相同的挑战值 C_{u_i} 下也无法获得相同的响应值，且当电路发生变化时，产生的响应值也会改变，可得到

$$\left|\mathrm{PR}\left(\mathrm{Suc}_3\right)-\mathrm{PR}\left(\mathrm{Suc}_2\right)\right|\leqslant\frac{q_{\mathrm{P}}^2}{2^{1+l_{\mathrm{P}}}}\tag{6}$$

Game_4：在此次博弈中，A 执行查询 $\mathrm{Send}(I_{\mathrm{u}_i}^k,I_{\mathrm{g}_i}^k,I_{\mathrm{g}_j}^k,m)$ 来拦截消息并计算会话密钥，尝试估计 l 比特的会话密钥，可得到

$$\left|\mathrm{PR}\left(\mathrm{Suc}_4\right)-\mathrm{PR}\left(\mathrm{Suc}_3\right)\right|\leqslant\frac{q_{\mathrm{S}}}{2^l}\tag{7}$$

完成 $\mathrm{Game}_i(i=0,1,2,3,4)$ 后，A 没有其他不可忽视的优势猜测 α，可得到

$$\mathrm{PR}\left(\mathrm{Suc}_4\right)=\frac{1}{2}\tag{8}$$

根据式(3)~式(8)，可得到

$$\frac{1}{2}\mathrm{Adv}_S^A=\left|\mathrm{PR}\left(\mathrm{Suc}_0\right)-\frac{1}{2}\right|\leqslant\frac{q_{\mathrm{H}}^2}{2^{1+l_{\mathrm{H}}}}+\frac{q_{\mathrm{P}}^2}{2^{1+l_{\mathrm{P}}}}+\frac{q_{\mathrm{S}}}{2^l}$$

$$\mathrm{Adv}_S^A\leqslant\frac{q_{\mathrm{H}}^2}{2^{l_{\mathrm{H}}}}+\frac{q_{\mathrm{P}}^2}{2^{l_{\mathrm{P}}}}+\frac{q_{\mathrm{S}}}{2^{l-1}}\tag{9}$$

5　性能评估

为了体现本文协议性能的优越性，本节将从安全性能、计算开销以及通信开销 3 个方面进行分析，并与文献[9]、文献[11]、文献[12]、文献[14]和文献[18]提出的相关协议进行对比。

5.1　安全性能

本节将本文协议与相关协议中的 12 项关键安全属性进行了对比评估，具体如表 3 所示，其中，S_1 为双向认证，S_2 为匿名性和不可链接性，S_3 为完美前向安全，S_4 为伪装攻击，S_5 为中间人攻击，S_6 为重放攻击，S_7 为 DoS 攻击，S_8 为 UAV 物理捕获攻击，S_9 为 GS 物理捕获攻击，S_{10} 为 ESL 攻击，S_{11} 为恶意 UAV 撤销，S_{12} 为 ML 攻击。由表 3 可知，只有本文协议可以满足全部安全需求。

表 3　　不同协议的安全性分析

目标	文献[9]	文献[11]	文献[12]	文献[14]	文献[18]	本文
S_1	√	√	√	√	√	√
S_2	√	√	√	√	√	√
S_3	√	√	×	√	√	√
S_4	×	√	×	√	√	√
S_5	√	√	√	√	√	√
S_6	√	√	√	√	√	√
S_7	√	√	√	√	√	√
S_8	×	×	×	√	×	√
S_9	×	×	√	×	×	√
S_{10}	×	×	×	×	×	√
S_{11}	×	×	×	√	×	√
S_{12}	—	—	—	×	—	√

为了验证本文提出的匿名响应分割方法在逻辑回归模型下抵抗 ML 攻击的能力，本文采用并行 Arbiter PUF 生成了 10 036 组 64 位响应值用于实验测试。ML 攻击对不同方法 CRP 建模的准确率对比如图 6 所示，在不同汉明距离（HD, Hamming distance）阈值下，攻击模型的预测准确率呈现显著差异。当 HD=3 时，原始 CRP 建模的响应值准确率可达到 97.8%，表明攻击者可通过收集足够 CRP 样本有效建立预测模型。本文方法即使在汉明距离阈值为 3 且训练样本数达到 10 000 时，仍然无法通过建模生成正确的响应值，因此能够有效抵御分布式节点下的 ML 攻击。

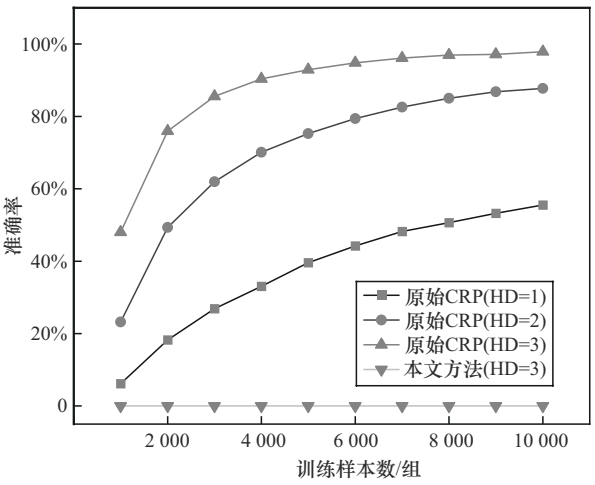


图 6　ML 攻击对不同方法 CRP 建模的准确率对比

5.2 计算开销

为了验证本文协议在计算开销方面的优势，将其与近年来相关协议进行比较。协议中涉及的主要操作包括椭圆曲线乘法T_m、哈希（SHA256）T_h、密钥派生函数T_k以及对称密钥加解密（AES128）T_s。由于PUF运算、模运算、异或运算的开销均低于1 ns，因此本文忽略这些操作的计算开销。为了模拟真实场景网络节点的开销情况，本文基于Miracl库分别在Raspberry PI 5和计算机（Intel core ultra 9 2.3 GHz）上模拟UAV和GS，并统计了各个操作的计算开销，相关密码操作的执行时间如表4所示。

表4 相关密码操作的执行时间

操作	UAV执行时间/ms	GS执行时间/ms
T_m	0.540 0	0.340 0
T_h	0.001 2	0.001 0
T_k	0.012 5	0.004 7
T_s	0.018 0	0.001 0

不同协议的计算开销如表5和图7所示，此外，图7还进行了安全级别对比。在UAV端，本文协议和文献[12]相当，具有最低的计算开销。在GS端，本文协议仍保持最低的计算开销，相较于当前计算开销最少的文献[18]降低了9.1%。这主要归因于本方案只采用轻量级密码操作构建认证协议，并且部分非实时参数计算在预切换认证阶段已协商完成。这一特性对于资源受限的UAV网络具有重要的实践意义。此外，本文协议在保证计算开销最低的同时，还具备了更高的安全级别。

表5 不同协议的计算开销

协议	UAV/ms	GS/ms
文献[9]	$7T_h + 2T_m \approx 1.088\,4$	$13T_h + 2T_m \approx 0.693\,0$
文献[11]	$T_h + 4T_s \approx 0.073\,2$	$T_h + 10T_s \approx 0.011\,0$
文献[12]	$6T_h \approx 0.007\,2$	$10T_h \approx 0.010\,0$
文献[14]	$8T_h \approx 0.009\,6$	$11T_h \approx 0.011\,0$
文献[18]	$4T_k + 3T_h + T_s \approx 0.071\,6$	$2T_h + T_k + T_s \approx 0.007\,7$
本文协议	$6T_h \approx 0.007\,2$	$7T_h \approx 0.007\,0$

为了验证本文协议在多UAV场景下的性能表现，本文选取了文献[27]作为对比对象。该协议采用聚合签名实现批量认证，是目前具有代表性的UAV批量认证方案。由于现有批量认证协议未对UAV端进行优化，本文重点比较协议在GS端的计算开销，结果如图8所示。由图8可知，本文协议在多UAV场景中，GS端的计算开销仍保持显著优势。这一优势源于协议设计的底层机制差异，现有批量认证方案普遍采用基于椭圆曲线的聚合签名技术，而本文协议仅通过轻量化操作实现身份验证，计算开销始终维持在较低水平。

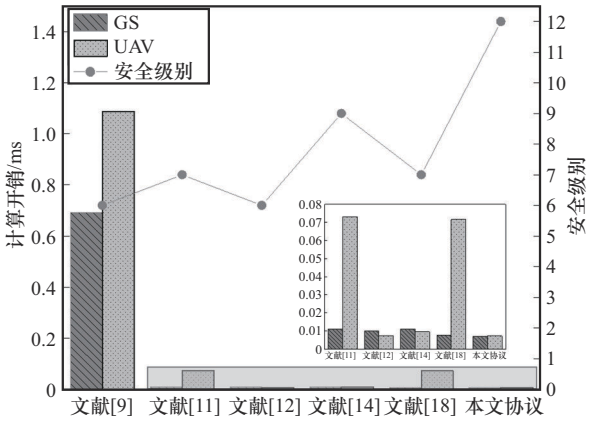


图7 不同协议的计算开销和安全级别对比

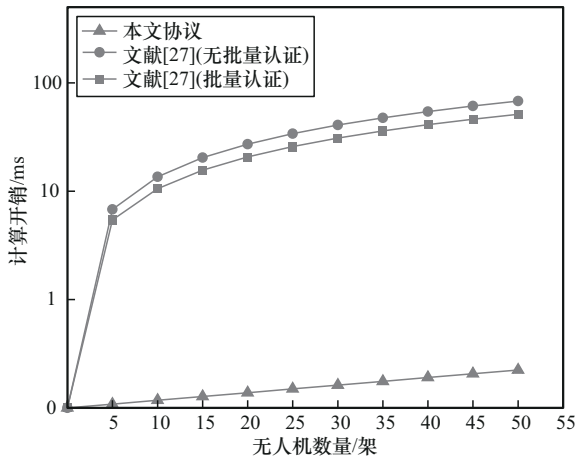


图8 不同协议在多UAV场景下GS的计算开销对比

5.3 通信开销

在通信开销评估方面，将本文协议与相关协议进行了对比。通信开销中涉及的操作标识符与长度定义如下：椭圆曲线点乘（ECC=320 bit），哈希函数（Hash=256 bit），身份标识（ID=64 bit），随机数（Nonce=256 bit），密钥派生函数（KDF=256 bit），PUF挑战值和响应值（PUF=64 bit），时间戳（Time=32 bit）。不同协议的通信开销如表6和图9所示。由表6和图9可知，本文协议具有最低的通

信开销，相较于对比组性能最好的文献[12]降低了13.8%。分析原因主要有以下两点：一方面，在切换认证过程中，本文协议采用预切换认证机制提前完成了部分参数协商，降低了后续切换认证中的通信开销；另一方面，本文协议将切换认证任务从云端卸载至边缘端的GS，认证过程只需要完成UAV和GS之间的双向通信。

表6　　不同协议的通信开销

协议	消息数	通信开销/bit
文献[9]	4	3ECC + 6Hash + 4ID + 5Time = 2 912
文献[11]	6	3Hash + 7Nonce = 2 560
文献[12]	2	7Hash + 2Time = 1 856
文献[14]	3	8Hash + 3Time = 2 144
文献[18]	6	5Hash + KDF + ID + 4Nonce = 2 624
本文协议	3	5Hash + 2ID + 2PUF + 2Time = 1 600

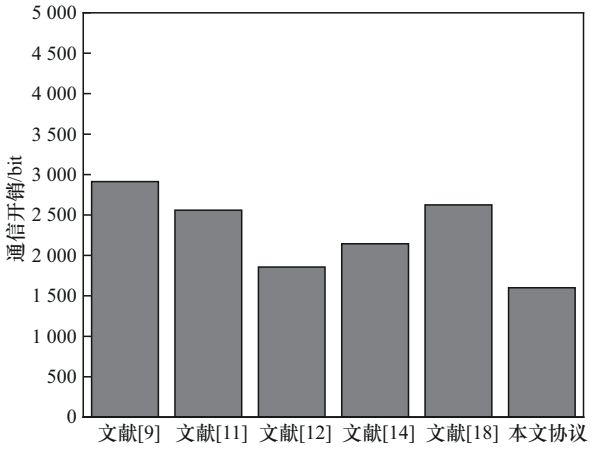


图9　不同协议的通信开销对比

此外，本文协议采用CRT确保了在主切换节点失效的情况下，UAV可以与备用切换节点实现快速切换，这在需要实现稳定切换的场景下是非常重要的，而其他协议不具备相关特性。

6　结束语

本文提出了一种适用于云边协同UAV网络的高效切换认证协议，旨在降低切换认证过程中的计算开销和通信开销，同时有效抵御物理捕获攻击、ML攻击等安全威胁。首先，本文协议将认证计算过程从可信中心NCC卸载至边缘端的GS，结合PUF实现了云边协同场景下UAV网络的切换认证。其次，设计了CRP匿名响应分割方法，避免了攻击者对合法实体进行ML攻击的可能性。此外，基于CRT构建了一种动态挑战−响应对分片批量同步机制，在增强切换稳定性的同时有效降低了性能开销。最后，通过ROR模型证明了本文协议的语义安全性。实验结果表明，相较于同类协议，本文协议计算开销和通信开销均具有优越性，适合部署于资源受限的云边协同UAV网络。

参考文献：

[1] LI Y B, ZHANG H J, LONG K P, et al. Resource allocation for optimizing energy efficiency in NOMA-based fog UAV wireless networks[J]. IEEE Network, 2020, 34(2): 158-163.

[2] YUAN Y Z, GAO S C, ZHANG Z T, et al. Edge-cloud collaborative UAV object detection: edge-embedded lightweight algorithm design and task offloading using fuzzy neural network[J]. IEEE Transactions on Cloud Computing, 2024, 12(1): 306-318.

[3] REN C, GONG C, LIU L C. Task-oriented multimodal communication based on cloud-edge-UAV collaboration[J]. IEEE Internet of Things Journal, 2024, 11(1): 125-136.

[4] AYDIN Y, KURT G K, OZDEMIR E, et al. Authentication and handover challenges and methods for drone swarms[J]. IEEE Journal of Radio Frequency Identification, 2022, 6: 220-228.

[5] MOZAFFARI M, SAAD W, BENNIS M, et al. A tutorial on UAVs for wireless networks: applications, challenges, and open problems[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2334-2360.

[6] TANVEER M, ALDOSARY A, KHOKHAR S U D, et al. PAF-IoD: PUF-enabled authentication framework for the Internet of drones[J]. IEEE Transactions on Vehicular Technology, 2024, 73(7): 9560-9574.

[7] 范馨月, 刘洁, 何嘉辉. V2G中基于PUF的轻量级匿名认证协议[J]. 通信学报, 2024, 45(10): 129-141.
FAN X Y, LIU J, HE J H. Lightweight PUF-based anonymous authentication protocol in V2G[J]. Journal on Communications, 2024, 45(10): 129-141.

[8] CHEN S, LI B, CHEN Z H, et al. Novel strong-PUF-based authentication protocols leveraging Shamir's secret sharing[J]. IEEE Internet of Things Journal, 2022, 9(16): 14408-14425.

[9] KWON D, SON S, PARK Y, et al. Design of secure handover authentication scheme for urban air mobility environments[J]. IEEE Access, 2022, 10: 42529-42541.

[10] KHALID H, HASHIM S J, HASHIM F, et al. HOOPOE: high performance and efficient anonymous handover authentication protocol for flying out of zone UAVs[J]. IEEE Transactions on Vehicular Technology, 2023, 72(8): 10906-10920.

[11] LIU Y B, HUO L J, WU J, et al. MRSA: mask random array protocol for efficient secure handover authentication in 5G HetNets[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(5): 3809-3827.

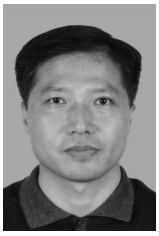
[12] WEN K, WANG S B, WU Y X, et al. A secure authentication protocol supporting efficient handover for UAV[J]. Mathematics, 2024, 12(5): 716.

[13] GOPE P, SIKDAR B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of drones[J]. IEEE

Transactions on Vehicular Technology, 2020, 69(11): 13621-13630.
[14] SON S, KWON D, LEE S, et al. Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF[J]. IEEE Access, 2023, 11: 60240-60253.
[15] PU C, WALL A, CHOO K R, et al. A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of drones environment[J]. IEEE Internet of Things Journal, 2022, 9(12): 9918-9933.
[16] BADSHAH A, ABBAS G, WAQAS M, et al. USAF-IoD: ultralightweight and secure authenticated key agreement framework for Internet of drones environment[J]. IEEE Transactions on Vehicular Technology, 2024, 73(8): 10963-10977.
[17] BHATTARAI I, PU C, CHOO K R, et al. A lightweight and anonymous application-aware authentication and key agreement protocol for the Internet of drones[J]. IEEE Internet of Things Journal, 2024, 11(11): 19790-19803.
[18] YANG Y Y, CAO J, MA R H, et al. FHAP: fast handover authentication protocol for high-speed mobile terminals in 5G satellite–terrestrial-integrated networks[J]. IEEE Internet of Things Journal, 2023, 10(15): 13959-13973.
[19] 尚涛, 田格格, 姜亚彤, 等. 基于中国剩余定理的ATN地空切换认证协议[J]. 西安电子科技大学学报, doi: 10.19665/j.issn1001-2400.20241106.
SHANG T, TIAN G G, JIANG Y T, et al. Ground-air handover authentication scheme for ATN based on the Chinese remainder theorem[J]. Journal of Xidian University, doi: 10.19665/j.issn1001-2400.20241106.
[20] NIMMY K, SANKARAN S, ACHUTHAN K. A novel lightweight PUF based authentication protocol for IoT without explicit CRPs in verifier database[J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 14(5): 6227-6242.
[21] LI D W, LIU D, REN Y K, et al. CPAKA: mutual authentication and key agreement scheme based on conditional PUF in space-air-ground integrated network[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 3487-3500.
[22] LOUNIS K, DING S H H, ZULKERNINE M. D2D-MAP: a drone to drone authentication protocol using physical unclonable functions[J]. IEEE Transactions on Vehicular Technology, 2023, 72(4): 5079-5093.
[23] KARMAKAR R, KADDOUM G, AKHRIF O. A PUF and fuzzy extractor-based UAV-ground station and UAV-UAV authentication mechanism with intelligent adaptation of secure sessions[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 3858-3875.
[24] ZHANG Y, LI B, LIU B, et al. Building PUF as a service: distributed authentication and recoverable data sharing with multidimensional CRPs security protection[J]. IEEE Internet of Things Journal, 2024, 11(10): 17301-17316.
[25] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.
[26] XIE Q, DING Z X, TANG W, et al. Provable secure and lightweight blockchain-based V2I handover authentication and V2V broadcast protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2023, 72(12): 15200-15212.
[27] ALI I, LI J Q, CHEN J, et al. IOOSC-U2G: an identity-based online/offline signcryption scheme for unmanned aerial vehicle to ground station communication[J]. IEEE Internet of Things Journal, 2024, 11(18): 29941-29955.

[作者简介]

芮立（1986–），男，江苏南京人，陆军工程大学博士生，南京审计大学金审学院副教授，主要研究方向为无人机网络安全、安全认证。



张雄伟（1965–），男，浙江嘉兴人，博士，陆军工程大学教授、博士生导师，主要研究方向为信息安全、人工智能。

杨吉斌（1978–），男，安徽明光人，博士，陆军工程大学副教授、硕士生导师，主要研究方向为信息安全、人工智能。

徐伟光（1984–），男，安徽宿州人，博士，陆军工程大学副教授，主要研究方向为信息安全、密码学。