FEN-AKA：面向动态噪声环境的无人机轻量级三方认证协议

宋建华[1,2,3,4]，刘世炜[5]，张龑[2,4,5]
（1.湖北大学网络空间安全学院，湖北 武汉 430062；2.智能感知系统与安全教育部重点实验室，湖北 武汉 430062；
3.智能网联汽车网络安全湖北省工程研究中心，湖北 武汉 430062；
4.大数据智能分析与行业应用湖北省重点实验室，湖北 武汉 430062；5.湖北大学计算机学院，湖北 武汉 430062）

摘　要：针对高噪声、强干扰环境下无人机通信可靠性受限问题，提出了基于噪声物理不可克隆函数（PUF）和模糊提取器的轻量级三方认证协议。该协议利用噪声PUF量化硬件固有噪声特征，规避传统PUF在恶劣环境下的环境扰动偏移，通过模糊提取器消除噪声并生成稳定可还原的密钥，解决输出不稳定问题。关键信息由硬件安全模块（HSM）存储，并设计事件驱动的挑战–响应对（CRP）更新机制，消除CRP存储泄露风险。经毛–博伊德（MB）逻辑与随机预言机（ROR）模型形式化验证，协议满足匿名性、不可追溯性及抗物理捕获攻击等安全属性。性能分析表明，相比现有方案，计算开销平均降低21.2%，存储成本减少14.4%，通信效率显著提升，特别适用于资源受限的无人机在高噪声、强干扰、动态变化复杂环境中的安全通信需求，有效增强系统可靠性。

关键词：噪声物理不可克隆函数；模糊提取器；硬件安全模块；噪声干扰；三方认证协议
中图分类号：TN918.4
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025212

FEN-AKA: a lightweight three-party authentication protocol for UAV in dynamic noise environments

SONG Jianhua[1,2,3,4], LIU Shiwei[5], ZHANG Yan[2,4,5]
1. School of Cyber Science and Technology, Hubei University, Wuhan 430062, China
2. Key Laboratory of Intelligent Sensing System and Security (Hubei University) Ministry of Education, Wuhan 430062, China
3. Hubei Provincial Engineering Research Center of Intelligent Connected Vehicle Network Security, Wuhan 430062, China
4. Hubei Key Laboratory of Big Data Intelligent Analysis and Application, Hubei University, Wuhan 430062, China
5. School of Computer Science, Hubei University, Wuhan 430062, China

Abstract: To address unreliable UAV communications in high-noise, strong-interference environments, a lightweight three-party authentication protocol was proposed using noisy physical unclonable function (PUF) and fuzzy extractors. Hardware-intrinsic noise was captured by noisy PUF to mitigate environmental drift, and stable keys were generated via fuzzy extractors to overcome output instability. Critical datas were protected by a hardware security module (HSM), and CRP leakage risk was eliminated through an event-driven update mechanism. The protocol was formally verified with Mao-Boyd logic and the random oracle model, demonstrating anonymity, untraceability, and resistance to physical capture. It reduced computational overhead by 21.2% and storage cost by 14.4%, while significantly improving communication efficiency over existing schemes. It is well suited for resource-constrained UAVs in harsh, dynamic environments and effectively enhances system reliability.

Keywords: noisy physical unclonable function, fuzzy extractor, hardware security module, noise interference, three-party authentication protocol

---

收稿日期：2025–07–10；**修回日期：**2025–10–29
通信作者：刘世炜，202321116012585@stu.hubu.edu.cn
基金项目：国家自然科学基金资助项目（No.62377009）；湖北省重大攻关基金资助项目（JD）（No.2023BAA018）；绩效评价信息管理研究湖北省人文社科基地课题基金资助项目（No.2025JX03）；湖北省科技计划重大科技专项基金资助项目（No.2024BAA008）
Foundation Items： The National Natural Science Foundation of China (No.62377009), The Major Project of Hubei Province (JD) (No.2023BAA018), The Research Center for Performance Evaluation and Information Management, Hubei Provincial Humanities and Social Sciences Research Base Project (No.2025JX03), The Major Science and Technology Special Project of Hubei Science and Technology Plan (No.2024BAA008)

0 引言

近年来，随着通信技术的快速发展，无人机（UAV）在复杂动态环境中的应用日益广泛，逐渐成为智能监测与远程数据采集的关键平台[1-3]。配备传感器的无人机可昼夜交替在山区、河谷、密林等人类难以抵达的区域灵活作业，实时获取地理信息、环境参数（如空气质量、水质、土壤状态）等关键数据[2]。此类应用显著提升了传统人工巡检的安全性与效率，并为生态评估、灾害预警及气象研究提供数据支撑[3]。然而，在高噪声、强干扰的动态通信环境中，现有无人机系统的身份认证机制易受信道扰动影响，导致密钥协商失败或安全漏洞，严重制约其在关键任务场景下的可靠性。

然而，随着无人机使用量的增加，通信安全和数据隐私的问题也越来越突出，通过开放信道进行通信存在重大风险，例如在无人机、物联网设备（IoT）和地面控制站（GCS）三方通信的场景中，无人机更容易受到物理捕获、窃听、重播和入侵攻击，恶意攻击者可能通过拦截通信消息提取敏感数据，对救援、监测活动实施严重干扰，造成恶劣影响，在其他场景下，网络犯罪分子可能利用关键设施和应急响应的漏洞，破坏通信和敏感数据来阻碍无人机的正常活动，例如网络攻击可能涉及黑客攻击、恶意软件攻击或拒绝服务（DoS）攻击，而许多物联网设备需要部署在特定区域，进行数据收集和传输实时的传感数据[4]，这些区域通常人力无法抵达，难以进行人工监测，使传感数据的收集更加困难，在这一环境下，无人机作为资源受限的通信设备，亟需设计兼具高安全性与低开销的轻量级通信协议，以保障在复杂环境下的可靠运行[5]，此外，传统的基于无人机与无人机进行通信的协议无法充分保障协议的安全性[6]，因此，设计一份保证物联网、无人机和地面控制站三方通信的安全协议，其重要性不言而喻。

无人机辅助认证的协议必须通过已认证的无人机远程执行认证过程，并且在复杂环境中，无人机的通信可能不稳定，导致信号丢失，且无人机的计算资源有限，无法实现快速进行复杂的加密计算和解密操作。物理网设备辅助认证的协议则存在物联网设备存储的关键信息过多，导致存储开销过大，设备易被物理破坏的问题，导致通信易丢失，且无人机传输数据时，传感数据的敏感性和隐私性面临更高的风险[7]，为了解决上述问题，目前已经为无人机设计了许多有效的通过物理网设备或无人机辅助认证的协议，但这两类协议均存在明显的缺陷，现有的协议不适合物联网设备、无人机和地面控制站的三方通信，此外，与普通的物联网设备相比，部署在高空环境中的无人机面临更多潜在的物理威胁。而针对物理网设备和无人机的物理安全问题，比较可采取的方法就是利用物理不可克隆函数（PUF, physical unclable function）的硬件安全技术。它可以作为数字指纹，唯一地识别任何半导体器件，是解决物理安全问题的有效途径。

但是许多现有的基于PUF的认证协议不适合应用于无人机场景下的安全通信[8-16]，Barbareschi等[8]提出一种不需要预共享密钥、不依赖公钥密码学的认证方案，利用PUF作为硬件信任根，实现物联网设备–边缘节点–云服务器之间的相互认证与会话密钥协商，但未考虑噪声对PUF响应的影响。Chatterjee等[9]提出了一种基于PUF的认证方案，通过引入篡改检测，支持单个PUF响应被读取后不可恢复，防止局部泄露扩散，该方案满足相互认证、会话密钥机密性，但未考虑动态环境噪对PUF输出稳定性的影响，Guo等[10]提出基于PUF与模糊提取器的认证方案，仅采用哈希运算与异或操作实现三方相互认证与会话密钥协商，并引入时间戳和随机数以抵抗重放攻击，但未考虑挑战–响应对（CRP）的泄露问题，也未考虑动态噪声对PUF响应稳定性的影响。Shao等[11]提出了一种面向无人机辅助网络的轻量级三方认证与密钥协商协议，仅依赖哈希运算和异或操作实现高效交互，并通过临时身份与时间戳保障匿名性与抗重放能力，但未考虑噪声和环境扰动对PUF响应稳定性的影响。Choi等[12]提出了一种基于外部噪声源与PUF相结合的双因子模糊承诺方案，用于在资源受限设备上实现高鲁棒性的密钥生成与身份认证，但其外部噪声源需在注册与再生阶段来自同一物理位置，在高移动性场景难以保证环境数据的一致性。Lu等[13]提出一种适合无人机编队的分散网络架构，只采用单向哈希函数，该方案利用PUF作为设备唯一标识，并通过轻量级密码操作完成相互认证与会话密钥协商，增强了抗重放和防窃听的能力，但该方案未考虑实际部署中环境噪声、温度变化或信道干扰对PUF响应稳定性的影响。Pu等[14]基于

PUF 和混沌系统，提出了一种轻量级、保密性强的相互认证和密钥协商协议，通过混沌映射的随机置乱机制，增强了抗窃听和抗篡改的能力，但未考虑无人机处于动态复杂环境对 PUF 响应的影响。Son 等[15]提出了一种面向轻量级物联网设备身份认证协议，通过改良一种基于配对的用户认证方案，该协议能够抵御特权内幕攻击和已知特定会话的临时信息攻击，但无法抵御物理捕获攻击。Mall 等[16]提出了无人机辅助物联网设备的身份认证协议，设计了一种不需要公钥密码、仅依赖低开销操作的认证方案，能够抵御 PUF 建模攻击，但考虑噪声对 PUF 稳定性的影响，物联网设备（IoT）、UAV、云服务器需要严格时钟同步。尽管上述基于 PUF 的认证协议在轻量级安全通信方面取得了一定进展，但仍存在以下问题影响无人机在动态复杂环境的部署。首先，这些协议都没有考虑环境噪声对 PUF 的影响，在噪声影响的复杂环境下，无人机需要部署到高空或人力无法抵达的区域，在这个场景下，更需要无人机能够在多种噪声存在的环境中进行通信，而普通的 PUF 基于挑战–响应的机制，容易受到噪声的干扰导致输出的不一致，从而干扰认证的过程。其次，即使有的方案可以通过引入模糊提取器[17]从带有噪声的响应中提取可恢复的稳定字符，来辅助认证，但没有通过验证规则[18-19]验证通过该字符产生密钥的安全性，依旧会降低认证过程的安全性。最后，基于 PUF 的认证协议通常是由验证方来存储 CRP[20-21]，当验证方的 CRP 被泄露，认证协议的安全将无法得到保证。

本文基于以上背景，提出了基于噪声物理不可克隆函数和模糊提取器的轻量级三方认证协议（FEN-AKA）。该协议引入了噪声 PUF、模糊提取器、硬件安全模块（HSM, hardware security module）显著提高了无人机通信过程的可靠性。

本文的主要工作如下。

1) 利用噪声 PUF、模糊提取器和 HSM 提出了基于噪声物理不可克隆函数和模糊提取器的轻量级三方认证协议，该协议不需要消耗大量计算能力的方法，如非对称加密（RSA）算法、椭圆曲线加密（ECC）算法等，仅使用异或（XOR）和哈希函数等基本加密操作。

2) 该协议在物联网设备被破坏或者无人机被捕获的情况下，也不会泄露认证的关键信息，利用模糊提取器的还原性，不在公共信道传输可供认证的密钥信息，保证了认证过程的密钥安全性。

3) 该协议通过事件触发 CRP 的动态更新，从而消除使用 PUF 的“挑战–响应”认证机制中存储 CRP 带来的安全风险，并能够抵御机器建模攻击，提高了无人机协议的安全性。

4) 本文协议可以通过毛–博伊德（MB）逻辑验证会话密钥的安全性，并通过随机预言机（ROR）安全模型进行安全证明。通过多个角度验证协议的安全性，验证本文协议可以抵御窃听、篡改、重播、伪装、中间人攻击等多种攻击。

1　相关工作

近年来，无人机通信涌现了多种认证协议设计。按照认证过程中辅助通信认证实体的网络拓扑关系，现有的协议可分为两大范式：无人机协作式认证协议（UAV-UAV-GCS）与异构终端协同认证协议（IoT-UAV-GCS），在无人机协作式认证中，中继无人机作为可信第三方协助目标无人机与地面控制站建立安全信道；而异构终端协同认证协议则引入物联网设备作为边缘节点，与无人机、GCS 形成三方认证架构。由于参与实体的异构性，这两类协议面临的安全威胁存在显著差异。

基于 IoT、UAV 与 GCS 的三方认证协议通常采用中心化信任架构，GCS 作为可信第三方集中管理秘密参数。例如文献[22]对无人机在物联网无人值守场景下的通信需求，提出了一种基于 PUF 的三方认证协议，为无人机设计了一种在物联网设备无人值守的情况下，三方进行安全通信的认证协议。首次建立 PUF 形式化推理规则，通过逻辑验证确保该协议对 CRP 进行源验证，但需预存大量 CRP，忽略环境噪声对 PUF 响应稳定性的影响且未防御建模攻击，攻击者可利用机器学习算法逆向推导 PUF 特征。文献[23]设计了一种包含物联网设备、地面控制站和无人机等多个参与方的认证协议，通过形式化证明和模拟攻击验证了该协议能够抵御多种攻击，但该协议要求严格的时钟同步，会因网络偏差影响更新的准确性。文献[24]提出了支持 IoT-UAV-GCS、UAV-GCS 和 UAV-UAV 3 种通信场景的认证协议，但未考虑到环境噪声对 PUF 响应的影响，若 PUF 响应存在偏差，会导致通信过程无法顺利进行。文献[25]利用超椭圆曲线（HECC）的数学

优势改进三方认证协议，使用HECC替代ECC，显著降低了计算开销，但该协议追求轻量化未集成PUF模块，导致无人机身份易被克隆，攻击者仅需提取固件镜像即可复制设备身份。

在无人机协作式认证协议中，GCS作为可信根节点管理认证密钥材料，但受限于无人机节点的资源约束、物理暴露风险以及动态信道环境特性，协议设计需兼顾效率与鲁棒性平衡。文献[26]提出了一种基于HECC的辅助无人机网络与地面控制站通信的认证协议，减小了无人机的存储开销和通信开销，但没有考虑到克隆攻击和物理攻击的风险，对量子计算攻击只能达到有限的防御。文献[27]提出了基于无人机群与地面控制站进行通信的认证协议，将PUF模块部署在无人机上，确保了物理安全，但整个协议依赖时钟同步性，需要通信方保持时间的一致性，并且没有考虑到极端环境对PUF的产生影响，因此通信过程易受到客观因素的影响。文献[28]提出了一种新的会话密钥计算原则，在无人机辅助无人机与地面控制站进行安全通信的过程中，增强了密钥生成的规则，但没有做到各个参与方进行密钥协商，虽然提到了一种新的PUF设计，但是只讨论了理想条件PUF的响应，并未考虑无人机在恶劣环境会受到噪声的影响。文献[29]提出一种无人机辅助无人机与地面控制站进行两阶段通信的认证协议，利用PUF生成设备唯一指纹，防止物理捕获攻击，但单次认证需传输4轮交互消息，通信消息过高，只假设PUF在理想环境下运行，未考虑环境噪声的影响。

针对这两类认证协议，本文需要考虑无人机资源受限，以及保证无人机能在噪声环境下不受影响的问题，也有许多工作对此展开了研究。文献[30]利用载波频率偏移（CFO）和相位噪声（PHN）作为硬件指纹，在高动态和噪声场景下实现高效的身份认证，但只能抵御身份欺骗攻击、同位置攻击和高动态环境下的攻击，所能抵御的攻击类型较少。文献[31]提出了一种基于信噪比（SNR）的无人机认证方案，通过SNR在高噪声环境中的差异作为认证特征，能够在复杂的噪声环境中实现高效的身份认证，虽能抵御中间人攻击、重放攻击，依旧无法满足无人机场景下，高安全属性的要求。文献[32]提出了一种PUF结合模糊提取器的身份认证协议，考虑到PUF因环境噪声导致的响应不一致的问题，但没考虑到无人机需要面对高动态复杂的噪声环境，理想的PUF无法满足该场景的需求。文献[33]提出了PUF、模糊提取器和区块链3种加密方式相结合的身份认证协议，通过模糊提取器获取用户的生物特征信息，未考虑PUF因环境噪声导致响应不一致的问题，只设想了理想的PUF状态，也没有考虑攻击者可通过机器学习算法进行机器建模攻击。文献[34]提出了一种模糊提取器的架构，用于安全密钥的生成和恢复密钥，可以减少噪声带来的轻微变化，但无法面对动态变化的复杂噪声环境，也无法抵御机器建模攻击。文献[35]提出了PUF和HSM相结合的认证方案，充分利用HSM能够管理加密密钥、进行加密操作和存储安全信息的特点，但只针对中间人攻击这一种攻击形式，没有进行完整的安全属性分析，只验证了方案的可行性。

综上所述，现有方案在高动态复杂的噪声场景下存在如下问题，具体如表1所示。现有许多采用哈希函数、物理不可克隆函数、模糊提取器这些密码原语的无人机认证协议，或通过加密算法和噪声特征进行认证的安全协议，但都无法同时满足动态噪声场景下无人机的隐私保护、轻量级认证、密钥协商、物理抵御等安全需求。因此亟须提出一种新的认证协议和密钥协商协议来满足无人机认证协议的在噪声环境下的安全问题。本文在此背景下创新性地提出了基于噪声物理不可克隆函数和模糊提取器的轻量级三方认证协议。该协议面向高噪声、强干扰、资源受限的复杂通信环境，首先针对传统PUF在动态环境中易受环境扰动导致响应偏移的问题，引入噪声PUF，主动捕获并量化硬件中固有的动态噪声，并通过模糊提取器消除噪声，提取出稳定可还原的密钥，解决噪声PUF输出不稳定的问题，通过事件驱动的CRP动态更新机制，增强协议抗物理捕获和抗机器建模攻击的能力。此外，本文使用硬件安全模块保障设备在物理获取下仍能保障密钥安全，通过MB逻辑对密钥协商过程进行形式化分析，并基于ROR安全模型证明协议满足多种安全属性，在性能评估上，与现有方案对比，计算开销平均减少约21.2%，存储成本降低14.4%，证明协议更适用于高噪声的动态复杂环境。

表1　　相关方案

相关方案	认证实体	加密技术	性能缺失
文献[22]	IoT-UAV-GCS	PUF、对称加密算法、Hash	无法抵御机器建模攻击；未考虑噪声对PUF产生的影响
文献[23]	IoT-UAV-GCS	Hash、对称加密算法、非对称加密算法、椭圆曲线密码学	要求严格的时钟同步；无法抵御物理捕获攻击；无法保证各个设备相互认证；无法保证完全前向保密
文献[24]	IoT-UAV-GCS	PUF、Hash、超椭圆曲线密码学	无法抵御机器建模攻击；没有进行密钥协商；未考虑噪声对PUF产生的影响；要求时钟同步
文献[25]	IoT-UAV-GCS	超椭圆曲线密码学、Hash、模糊提取器	无法抵御克隆攻击；无法抵御对于物理网设备的物理捕获攻击
文献[26]	UAV-UAV-GCS	超椭圆曲线密码学、Hash	无法抵御克隆攻击；无法抵御物理捕获攻击
文献[27]	UAV-UAV-GCS	PUF、Hash	要求严格的时钟同步；未考虑噪声对PUF产生的影响；无法抵御机器建模攻击；没有进行密钥协商；无法保证完全前向保密
文献[28]	UAV-UAV-GCS	PUF、Hash	无法抵御窃听攻击；无法抵御机器建模攻击；未考虑噪声对PUF产生的影响
文献[29]	UAV-UAV-GCS	PUF、Hash、对称加密算法	无法抵御克隆攻击；无法抵御窃听攻击；无法抵御机器建模攻击；要求时钟同步；没有进行密钥协商
文献[30]	UAV-UAV-GCS	CFO、PHN	无法抵御重放攻击；无法抵御窃听攻击；无法保证匿名性和不可追溯性；无法保证完全前向保密
文献[31]	IoT-UAV-GCS	SNR	无法保证完全前向保密；要求时钟同步；无法抵御物理捕获攻击；无法抵御中间人攻击
文献[32]	UAV-UAV-GCS	PUF、模糊提取器、Hash	未考虑高动态复杂噪声环境对PUF的影响；无法抵御机器建模攻击；无法抵御窃听攻击
文献[33]	IoT-User-Server	PUF、模糊提取器、区块链	未考虑噪声对PUF产生的影响；无法抵御机器建模攻击；无法保证完全前向保密；无法抵御克隆攻击；无法抵御窃听攻击
文献[34]	IoT-Server	PUF、模糊提取器、椭圆曲线加密	未考虑高动态复杂噪声环境对PUF的影响无法抵御机器建模攻击；无法保证完全前向保密；无法抵御窃听攻击
文献[35]	IoT-Server	PUF、硬件安全模块	没有完整的安全属性分析；只针对中间人攻击进行重点抵御

2　预备知识

2.1　硬件安全模块

硬件安全模块在无人机场景下有着广泛应用，文献[36]提出了一种HSM算法，可以在任何时候允许密钥无存储地重建。文献[37]提出了一种由HSM支持的无人机认证系统，并对系统进行评估分析潜在威胁，HSM可以用于存储无人机、物联网设备、地面控制站相互认证所需要的关键密钥信息。本文考虑到无人机与物联网设备的计算机资源和存储资源有限，因此在地面控制站加入硬件安全模块，用于存储CRP，无人机与物联网设备的身份信息，以及组成密钥的关键信息。

2.2　物理不可克隆函数

PUF是一种基于物理硬件特性产生唯一响应的技术，它通过利用硬件组件的微小物理差异，生成独特的无法克隆或伪造的响应。例如芯片中某些元件的微小变化会导致不同芯片在相同操作条件下表现出不同的行为。其中噪声PUF通过对设备内固有的、随机的噪声进行测量和利用，从而生成唯一的、无法预测和复制的响应。噪声PUF利用的是硬件在制造过程中引入的噪声。具体来说，设备中如电容、电阻、半导体元件等微小差异会引入不可预测的噪声信号。PUF是基于挑战–响应的应对机制，将输入定义为挑战C，并生成一个定义为响应R的输出$\mathrm{PUF}\left(C:\{0,1\}^m\right)=R:\{0,1\}^n$。不同的PUF面对相同的挑战会产生不同的反应，即使是相同的PUF在不同的挑战下也会产生不同的反应，即

$$\mathrm{PUF}_i\left(c_1\right)\neq\mathrm{PUF}_j\left(c_1\right)\text{且}i\neq j \tag{1}$$

$$\mathrm{PUF}_i\left(c_1\right)\neq\mathrm{PUF}_j\left(c_2\right)\text{且}c_1\neq c_2 \tag{2}$$

2.3　模糊提取器

一般来说，模糊提取器是2个函数$(\mathrm{Gen},\mathrm{Rep})$的组合。生成函数Gen对响应$R$为字符串$k$和公开可用的辅助数据$a$，即$\mathrm{Gen}(R)=(k,\alpha)$即后一个再

现函数$\mathrm{Gen}(\mathrm{R})=(k,\alpha)$可以通过和辅助数据$a$获得字符串$k'$，即$\mathrm{Rep}(R',\alpha)=k'$。模糊提取器的处理过程如图1所示。如果2个响应$R$和$R'$之间的汉明距离不超过$\rho$，则$k$=$k'$。根据文献[38]中讨论的误差容忍阈值，如果$R$和$R'$之间的汉明距离是$\lambda$，则$\rho=\frac{\lambda}{n_b}$，其中，$n_b$是输入位数。

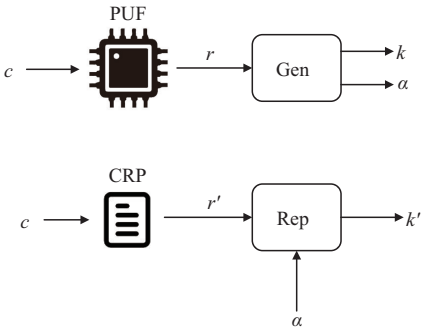

图1　模糊提取器的处理过程

2.4　系统模型

系统模型主要包括3个实体：GCS、无人机和一组物联网设备，物联网设备无法直接与GCS通信，需要通过无人机交换信息。在此之前，无人机需与GCS和物联网设备建立会话密钥，保证安全通信。协议所使用的符号及其定义如表2所示。系统模型如图2所示，系统模型清晰地描绘了地面控制站、无人机搭载传感器在多种不同场景下的通信架构。地面控制站通过向无人机发送指令，统筹调控整个数据采集流程。无人机作为移动平台，携载各类传感器可灵活前往并覆盖不同类型的场景区域，具体包括河流、高山、无人区以及专门用于监测非法活动的场景。在各特定场景中，传感器肩负着相应的数据采集任务，例如在河流场景下，重点收集水体温度、流速等水文特征数据；在高山场景，主要获取气象条件、地质结构的维度信息；在无人区场景，着重监测是否有危险生物出没的相关数据；而在非法活动监测场景，则专注收集非法入侵、违规作业等行为的关键信息。同时，系统也面临非法攻击者的威胁，非法攻击者会试图干扰或攻击无人机与地面控制站之间、传感器与无人机之间的数据传输和通信，针对无人机与地面控制站之间、传感器与无人机之间的数据传输链路实施干扰或攻击行为，企图破坏数据的完整性、篡改数据内容或窃取敏感信息。

表2　　符号及其定义

符号	定义
GCS、D_i、U_{av}	地面控制站、物联网设备、无人机
DID_i、$\mathrm{uid}_{\mathrm{av}}$	物联网设备和无人机的真实身份
ID_i、u_{av}	物联网设备和无人机的注册身份
TID_i、$\mathrm{TUID}_{\mathrm{av}}$	物联网设备和无人机的临时身份
(C_i,R_i)、$(C_{\mathrm{av}},R_{\mathrm{av}})$	物联网设备和无人机的挑战–响应对
r_x、N_x	具有生命周期ΔT_x的随机数
$h(\cdot)$	哈希函数
$\mathrm{Gen}(\cdot)$、$\mathrm{Rep}(\cdot)$	模糊提取器的生成和恢复函数
‖、⊕	连接符和异或运算
pk	会话钥
(k_i,α_i)、$(k_{\mathrm{av}},\alpha_v)$	由模糊提取器生成的辅助数据
Q_i、G_{av}	辅助物联网设备和无人机认证的加密参数
ΔT_x	随机数的生命周期
P_1、P_2、P_3、U_1、U_2、U_3	物理设备的身份标识符和无人机的身份标识符

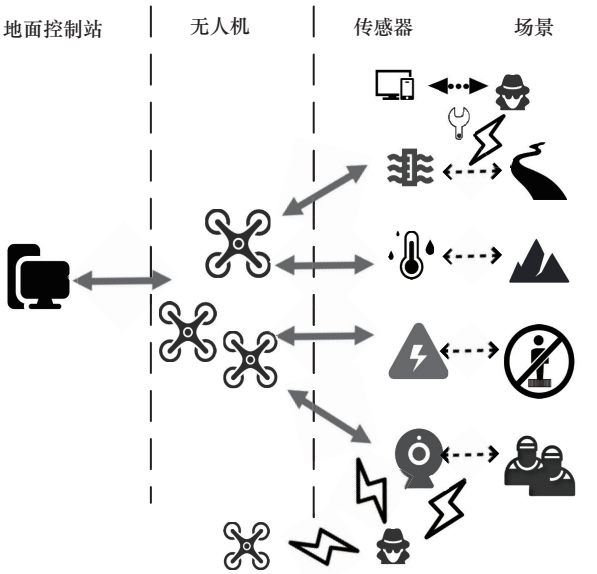

图2　系统模型

2.5　威胁模型

本文基于经典的多列夫–姚（Dolev-Yao）威胁模型[39]和卡内蒂–克拉夫奇克（Canetti-Krawczyk）对手模型[40]来分析认证协议的安全性，并对攻击者的能力作出如下假设。

1) 地面控制站可以免受外部攻击，但可能容易受到内部攻击，泄露敏感数据，无人机在高空恶劣环境中，传递的信息容易被攻击者窃听公共信道上的信息，并在网络中修改或重放这些消息，阻碍认证过程。

2) 物联网设备容易被恶意破坏，且无人机可以被物理捕获，攻击者可以从这两者中提取其中的关键信息。

3) 攻击者可以拦截和篡改无人机与地面控制站的通信，并操纵或隐藏数据、注入虚假信息、入侵或冒充网络内的授权节点。

4) 攻击者可以获取无人机和物联网设备的临时会话状态，例如随机数、临时密钥，不需要控制设备。

3　认证协议

本文方案的总体目标是在UAV、IoT与GCS之间实现安全通信，以保证感知数据的安全共享。为达成该目标，需在GCS、UAV和IoT设备三方之间建立相互认证机制，并协商生成会话密钥，以保障后续通信的机密性与完整性。为支持协议的正常运行，系统在启动阶段由GCS完成初始参数配置：GCS选择一个单向哈希函数 $h(): \{0,1\}^* \to \{0,1\}^l$ 生成和恢复函数 $\mathrm{Gen}(R)$ 和 $\mathrm{Rep}(R_i',\alpha)$，用于后续密钥生成与验证过程。

3.1　注册阶段

每个物联网设备和无人机在被部署之前，必须与GCS注册，以确保后续认证服务的正常实施，物理网设备和无人机的注册过程如图3和图4所示。

1) 物联网设备注册

步骤 1　每个IoT设备 D_i 首先需要为自己选择一个身份 ID_i，仅携带设备标识符 ID_i，用于启动认证流程。这一步骤对应图3中的第一个箭头，表示设备主动发起与GCS的通信。

步骤 2　GCS在收到 ID_i 后，生成随机数 r_i 和 N_i，并基于这些值计算出 $\mathrm{DID}_i = (\mathrm{ID}_i, r_i)$, $\mathrm{TID}_i = h(\mathrm{DID}_i \| N_i)$。此过程确保设备身份的唯一性和临时性，防止信息泄露。其中 DID_i 代表物理网设备的真实身份，TID_i 代表物联网设备的临时身份，然后GCS通过噪声PUF产生挑战 C_i，该挑战将用于后续PUF响应验证，以确保设备的真实性。这一操作对应图3中，GCS内部处理流程的第一部分。最后GCS将 C_i、TID_i、DID_i 发送给 D_i。

步骤 3　设备 D_i 收到 C_i、TID_i、DID_i、D_i 后，将 DID_i 拆分为 P_1、P_2 和 P_3，进行异或运算 $\mathrm{DID}_i = P_1 \oplus P_2 \| P_3$，生成最终的 DID_i，这一操作确保设备能够正确识别和使用其身份信息。D_i 将 C_i 作为输入，通过PUF得到一系列PUF响应 R_i，并利用模糊提取器生成 k_i，辅助数据 α_i 和提取后的响应 R_i'，即 $(k_i, \alpha_i) = \mathrm{Gen}(R_i)$。这一步骤是设备身份验证的核心，确保设备的身份不可伪造。最后 D_i 将 DID_i 设置为身份标识符，并存储 DID_i、TID_i 以用于后续验证。同时发送 $R_i, R_i', P_1, P_2, P_3, \alpha_i$ 给GCS，完成初始化阶段的信息交换。

步骤 4　GCS在收到来自 D_i 的消息，首先将 C_i 和 R_i' 结合成一系列挑战–响应对，用于后续的身份验证和安全性检查。GCS将所有关键数据，包括 $\mathrm{TID}_i, \mathrm{CRP}, R_i, \mathrm{DID}_i, \alpha_i, P_1, P_2, P_3$ 安全地存储到其HSM中。HSM提供了额外的安全保护层，防止数据被非法访问或篡改，确保整个协议流程的安全性。

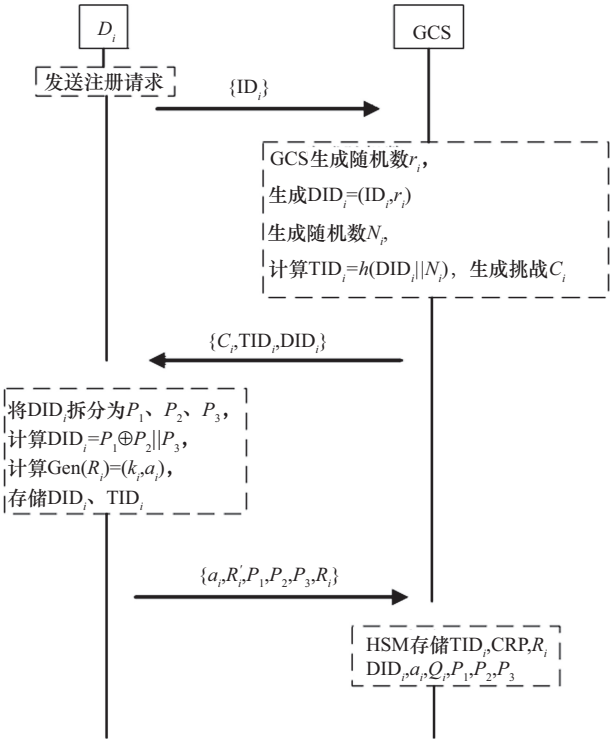

图3　物联网设备的注册过程

2) 无人机注册

步骤 1　每架无人机 U_{av} 向GCS发送注册请求，仅携带其身份标识 u_{av}。这一步骤对应图4中的第一个箭头，表示无人机主动发起与GCS的通信，启动认证流程。

步骤 2　GCS接收到 u_{av} 后，生成随机数 r_v 和 N_{av}，并基于这些值计算出 $\mathrm{uid}_{\mathrm{av}} = (u_{\mathrm{av}}, r_v)$, $\mathrm{TUID}_{\mathrm{av}} = h(\mathrm{uid}_{\mathrm{av}} \| N_{\mathrm{av}})$。此过程确保了无人机身份的唯一性和临时性，防止信息泄露。其中 $\mathrm{uid}_{\mathrm{av}}$ 代表无人机的真实身份，$\mathrm{TUID}_{\mathrm{av}}$ 代表无人机的临时

身份。GCS 利用噪声 PUF 生成挑战 C_{av}，该挑战将用于后续 PUF 响应验证，以确保无人机的真实性。这一操作对应图中 GCS 内部处理流程的第一部分。最后 GCS 将 $\mathrm{uid}_{\mathrm{av}}$、$\mathrm{TUID}_{\mathrm{av}}$、$C_{\mathrm{av}}$ 发送给 U_{av}。

步骤 3 无人机 U_{av} 收到 $\mathrm{uid}_{\mathrm{av}}$、$\mathrm{TUID}_{\mathrm{av}}$、$C_{\mathrm{av}}$ 后，U_{av} 将其拆分为 U_1、U_2 和 U_3 进行异或运算 $\mathrm{uid}_{\mathrm{av}} = U_1 \oplus U_2 || U_3$，生成最终的 $\mathrm{uid}_{\mathrm{av}}$。这一操作确保无人机能够正确识别和使用其身份信息。U_{av} 将 C_{av} 作为输入，通过 PUF 生成响应 R_{av}，即 $R_{\mathrm{av}} = \mathrm{PUF}_{\mathrm{u}}\left(C_{\mathrm{av}}\right)$。然后 U_{av} 使用模糊提取器生成 k_{av} 和辅助数 α_v 和提取后的响应 R'_{av},即 $\left(k_{\mathrm{av}},\alpha_v\right) = \mathrm{Gen}\left(R_{\mathrm{av}}\right)$。这一步骤是无人机身份验证的核心，确保了无人机的身份不可伪造。U_{av} 将 $\mathrm{uid}_{\mathrm{av}}$ 设置为其身份标识符，并存储 $\mathrm{uid}_{\mathrm{av}}$、$\mathrm{TUID}_{\mathrm{av}}$ 以用于后续认证。最后，U_{av} 将 R_{av}、R'_{av}、U_1、U_2、U_3、α_v 发送给 GCS，完成初始化阶段的信息交换。

步骤 4 GCS 收到 U_{av} 发送的数据后，将 C_{av} 和 R'_{av} 结合成一系列 CRP，用于后续的身份验证和安全性检查。GCS 将所有关键数据包括 $\mathrm{TUID}_{\mathrm{av}}$、$\mathrm{uid}_{\mathrm{av}}$、CRP、$R_{\mathrm{av}}$、$U_1$、$U_2$、$U_3$、$\alpha_v$ 安全地存储在 HSM 中。HSM 提供了额外的安全保护层，防止数据被非法访问和篡改，确保整个协议流程的安全性。

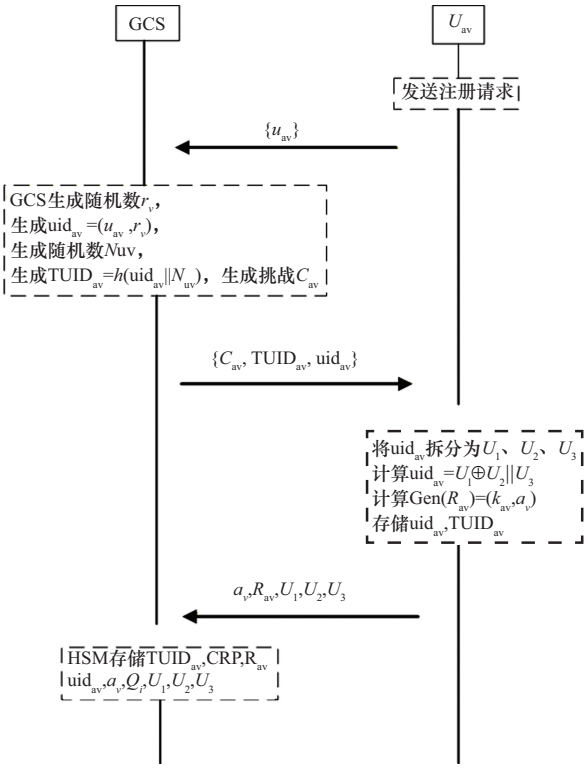

图4 无人机的注册过程

3.2 认证阶段

认证阶段是本文协议的关键部分，无人机、物联网设备和地面控制站需要完成相互认证，并生成一个可供三方认证的会话密钥，认证过程如图 5 所示。

步骤 1 当无人机 U_{av} 飞入特定区域时，物联网设备 D_i 将主动与 U_{av} 建立认证会话。R_i 是物联网设备 D_i 基于注册阶段 GCS 提供的挑战 C_i 生成的响应集合 R_i，通过模糊提取器将响应 R_i 转换为 k_i、提取后的响应 R'_i 和辅助数据 α_i,确保密钥的安全性和唯一性。D_i 生成一个随机数 N_d，然后物联网设备 D_i 计算 $Q_i = \left(k_i \oplus N_d\right) \oplus \left(P_1 || P_2 || P_3\right), M_1 = h(\mathrm{DID}_i || \mathrm{TID}_{\mathrm{i}} || N_d || k_i || Q_i)$，其中 Q_i 通过异或和哈希运算结合了密钥 k_i、随机数 N_d 和物联网设备的身份标识符 P_1、P_2、P_3，而 M_1 则是结合这些参数和 DID_i、$\mathrm{TID}_{\mathrm{i}}$ 的哈希值，用于后续身份验证。D_i 将计算得到的 $\{\mathrm{DID}_i, \mathrm{TID}_i, N_d, M_1\}$ 发送给 U_{av}，完成初步的身份信息互换。

步骤 2 在 U_{av} 收到来自 D_i 的消息后，U_{av} 首先检查随机数 N_d 的新鲜度，确保通信的实时性和安全性。如果 N_d 过期，U_{av} 将拒绝认证，防止重放攻击。如果没有过期，U_{av} 生成一个新的随机数 N_{uv}，并计算参数 G_{av} 和 M_2。G_{av} 结合密钥 k_{av}、随机数 N_{uv} 和身份标识符 U_1、U_2、U_3，即 $\mathrm{G}_{\mathrm{av}} = \left(k_{\mathrm{av}} \oplus N_{\mathrm{uv}}\right) \oplus (U_1 || U_2 || U_3)$，其中密钥 k_{av} 是无人机基于注册阶段生成的挑战集合 C_{av} 和响应集合 R_{av}，通过模糊提取器将响应 R_{av} 转化为 k_{av}、提取后的响应 R'_{av} 和辅助数据 α_v，而 M_2 是基于这些参数的哈希值，用于进一步的身份认证，即 $M_2 = h(\mathrm{TID}_i || N_d || M_1 || \mathrm{TUID}_{\mathrm{av}} || N_{\mathrm{uv}} || \mathrm{uid}_{\mathrm{av}} || \mathrm{k}_{\mathrm{av}})$，最后，$U_{\mathrm{av}}$ 将计算得到的 $\{\mathrm{TUID}_{\mathrm{av}}, \mathrm{TID}_{\mathrm{i}}, N_d, N_{\mathrm{uv}}, M_1, M_2, \}$ 发送给 GCS。

步骤 3 在收到来自 U_{av} 的消息后，GCS 首先检查随机数 N_{uv} 的新鲜度和 $\mathrm{TUID}_{\mathrm{av}}$ 的有效性，确保通信的实时性和合法性，GCS 访问 HSM 中的数据，比对 $\mathrm{TUID}_{\mathrm{av}}$ 是否一致，若一致，则承认 $\mathrm{TUID}_{\mathrm{av}}$ 为合法无人机临时身份。如果 N_{uv} 已过期或 $\mathrm{TUID}_{\mathrm{av}}$ 未注册，GCS 将终止认证过程。然后 GCS 将根据 $\mathrm{TUID}_{\mathrm{av}}$ 选择 $\mathrm{uid}_{\mathrm{av}}$ 和 $\left(C_{\mathrm{av}}, R'_{\mathrm{av}}\right)$，从其数据库中检索 TID_i。并比对 $\mathrm{TID}_{\mathrm{i}}$ 是否一致，如果 TID_i 不存在或不一致，认证也将中止。如果存在，GCS 通过模糊提取器将响应的集合 R'_{av} 转化为 k'_{av}，即 $k'_{\mathrm{av}} =$

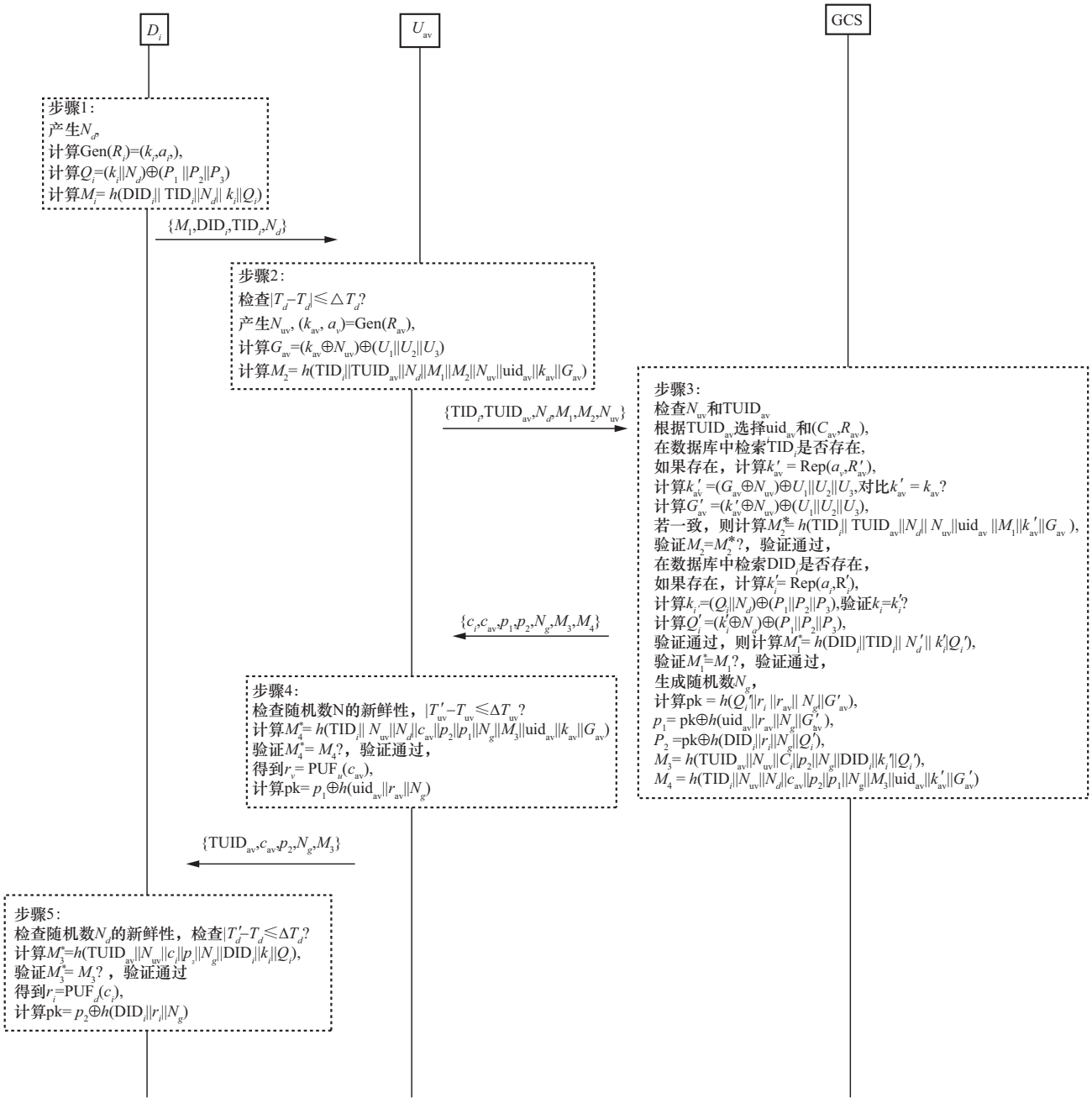

图5　认证过程

Rep$\left(\alpha_v,R'_{\mathrm{av}}\right)$，计算$k_{\mathrm{av}}=\left(G_{\mathrm{av}}\oplus N_{\mathrm{uv}}\right)\oplus\left(U_1\|U_2\|U_3\right)$,并比对$k'_{\mathrm{av}}$和$k_{\mathrm{av}}$，确保密钥的一致性和正确性。如果$R'_{\mathrm{av}}$与$R_{\mathrm{av}}$足够接近，则模糊提取器恢复的字符串$k'_{\mathrm{av}}$与$k_{\mathrm{av}}$一致，如果$R'_{\mathrm{av}}$偏差过大或挑战$C_{\mathrm{av}}$不匹配，则恢复失败。同时，GCS计算$G'_{\mathrm{av}}=\left(k'_{\mathrm{av}}\oplus N_{\mathrm{uv}}\right)\oplus\left(U_1\|U_2\|U_3\right)$，GCS将存储的$G_{\mathrm{av}}$与$G'_{\mathrm{av}}$进行比对，验证无人机的身份信息，若不一致则认证失败，若一致则GCS计算验证M_2=M_2^*是否成立，即$M_2^*=h\left(\mathrm{TID}_i\|N_d\|M_1\|\mathrm{TUID}_{\mathrm{av}}\|N_{\mathrm{uv}}\|\mathrm{uid}_{\mathrm{av}}\|\mathrm{k}'_{\mathrm{av}}\right)$。如果验证通过，则继续下一步认证流程，GCS将检验物联网设备D_i的身份信息，包括DID$_i$、TID$_i$、N_d、k_i和Q_i，并通过模糊提取器恢复密钥k_i'，确保设备的身份信息正确无误。GCS首先检查随机数N_d的新鲜度和TID$_i$的有效性，确保通信的实时性和合法性，然后检索TID$_i$，比对TID$_i$是否一致，若一致则承认TID$_i$为物联网设备的合法临时身份，如果N_d已过期或TID$_i$未注册，GCS将终止认证过程，GCS将根据TID$_i$选择挑战对$\left(C_i,R_i'\right)$，将响应R_i'

转化为稳定密钥k_i'，通过模糊提取器还原$k_i'=\mathrm{Rep}(\alpha_i,R_i')$，并计算$k_i=(Q_i\oplus N_d)\oplus(P_1||P_2||P_3)$，然后比对$k_i'$和$k_i$，确保密钥的一致性和准确性，如果$R_i'$与$R_i$足够接近，则模糊提取器恢复的字符串$k_i'$与$k_i$一致，如果$R_i'$偏差过大或挑战$R_i'$不匹配，则恢复失败。同时，GCS计算$Q_i'=(k_i'\oplus N_d)\oplus(P_1||P_2||P_3)$，GCS将$Q_i'$与存储的$Q_i$进行比对，验证物理网设备的身份信息，若不一致则认证失败，若一致则GCS计算验证$M_1^*=M_1$是否成立，即$M_1^*=h(\mathrm{DID}_i||\mathrm{TID}_i||N_d||k_i'||Q_i')$。如果验证通过，GCS从$(C_i,R_i')$和$(C_{\mathrm{av}},R_{\mathrm{av}}')$中分别选择$(c_i,r_i)$和$(c_{\mathrm{av}},r_{\mathrm{av}})$，并生成新的随机数$N_g$和时间戳$T_g$，用于后续的会话密钥的计算。GCS计算会话密钥pk及其派生密钥p_1和p_2，并计算哈希值M_3和M_4，为了完成与无人机、物联网设备的通信认证，确保通信的安全性和私密性，首先，GCS计算$\mathrm{pk}=h(N_g||r_i||G_{\mathrm{av}}'||r_{av}||Q_i')$，$p_1=\mathrm{pk}\oplus h(\mathrm{uid}_{\mathrm{av}}||r_{\mathrm{av}}||N_g||G_{\mathrm{av}}')$，$p_2=\mathrm{pk}\oplus h(\mathrm{DID}_i||r||_iN_g||Q_i')$。接下来，GCS计算$M_3$和$M_4$，即$M_3=h(\mathrm{TUID}_{\mathrm{av}}||N_{\mathrm{uv}}||c_i||p_2||N_g||\mathrm{DID}_i||Q_i'||k_i')$，$M_4=h(\mathrm{TID}_i||N_{\mathrm{uv}}||N_d||c_{\mathrm{av}}||p_2||p_1||N_g||M_3||\mathrm{uid}_{\mathrm{av}}||G_{\mathrm{av}}'||k_{\mathrm{av}}')$，$M_4$用于与无人机的身份认证，$M_3$用于与物联网设备的身份认证，最终达到相互认证的目的。最后，GCS发送消息$\{c_i,c_{\mathrm{av}},p_1,p_2,N_g,M_3,M_4\}$给$U_{\mathrm{av}}$。

步骤4 在收到来自GCS的消息后，U_{av}检查随机数N_g的新鲜度并获取当前时间戳T_g'，确保通信的实时性和安全性。如果N_g过期，则拒绝认证，防止重放攻击。如果N_g仍然有效，U_{av}使用$\Delta T_{\mathrm{uv}}=|T_{\mathrm{uv}}'-T_{\mathrm{uv}}|$检查$N_{\mathrm{uv}}$是否仍在有效期内。如果$N_{\mathrm{uv}}$仍在有效期内，$U_{\mathrm{av}}$计算并验证$M_4^*=M_4$是否成立，即$M_4^*=h(\mathrm{TID}_i||N_{\mathrm{uv}}||\mathrm{N}_d||c_{\mathrm{av}}||p_2||p_1||N_g||M_3||\mathrm{uid}_{\mathrm{av}}||G_{\mathrm{av}}||k_{\mathrm{av}})$。如果验证成功，$U_{\mathrm{av}}$使用$c_{\mathrm{av}}$作为挑战，并生成响应$r_{\mathrm{av}}=\mathrm{PUF}_u(c_{\mathrm{av}})$，然后计算出会话密钥$\mathrm{pk}=p_1\oplus h(\mathrm{uid}_{\mathrm{av}}||r_{\mathrm{av}}||N_g||G_{\mathrm{av}})$，完成无人机与地面控制站之间的身份认证，其中$G_{\mathrm{av}}$是结合了密钥和身份标识符的参数，会话密钥pk确保了后续通信的安全性和私密性。最后，U_{av}发送消息$\{\mathrm{TUID}_{\mathrm{av}},c_i,p_2,N_g,N_d,M_3\}$给$D_i$。

步骤5 在收到U_{av}的消息后，D_i检查随机数N_g的新鲜度并获取当前时间戳T_g'，确保通信的实时性和安全性。如果N_g已过期，D_i将终止认证。如果N_g仍然有效，D_i使用$\Delta T_d=|T_d'-T_d|$检查N_d是否仍在有效期内。如果不是，D_i也将终止认证。如果还在有效期，D_i计算并验证$M_3^*=M_3$是否成立，即$M_3^*=h(\mathrm{TUID}_{\mathrm{av}}||N_{\mathrm{uv}}||c_i||p_2||N_g||\mathrm{DID}_i||Q_i||k_i)$。如果验证成功，$D_i$使用$c_i$作为挑战，生成响应$r_i=\mathrm{PUF}_d(c_i)$，并计算出会话密钥$\mathrm{pk}=p_2\oplus h(\mathrm{DID}_i||r_i||N_g||Q_i)$，其中$Q_i$是结合了密钥和身份标识符的参数，会话密钥pk确保了后续通信的安全性和私密性。完成认证后，参与者D_i、U_{av}和GCS已成功建立会话密钥pk用于后续的安全通信和数据共享。这标志整个认证流程的结束，各方可以使用会话密钥进行加密通信，确保数据传输的安全性和完整性。

3.3 动态更新CRP

每次认证结束，将触发CRP动态更新机制，确保每次认证过程中的挑战–响应的唯一性和不可逆性，减少存储资源的浪费。

步骤1 HSM使用2个计数器计算无人机的响应R_{av}'的数量为N，物联网设备的响应R_i'的数量为M，用存储的DID_i对应相应的物联网设备的响应R_i'，$\mathrm{TUID}_{\mathrm{av}}$对应相应的无人机响应$R_{\mathrm{av}}'$，设置一个阈值$\rho=\frac{\lambda}{n_b}$。判断响应$R_{\mathrm{av}}'$和$R_{\mathrm{av}}$之间的比特翻转数量是否在允许范围内，同理判断，$R_i'$和$R_i$是否在允许范围内，若在允许范围内，则继续认证，否则终止认证。

步骤2 为无人机响应R_{av}'设定最小阈值$N_{\min}$，同理为R_i'设定最小阈值$M_{\min}$，如果响应验证成功，HSM将k_i与k_i'进行比对，若匹配成功，则继续认证，否则，认证失败，同理将k_{av}'与k_{av}也进行比对，同时更新计数器，记录已使用的CRPS的数量。并根据随机数N_g的生命周期删除已使用的CRP。

步骤3 如果被收集的CRP数量达到最小阈值$N_{\min}$或$M_{\min}$，HSM将更新k_i'和k_{av}'，终止认证，当已使用的CRP数量达到N或M时，更新相应的计数器，GCS产生新的挑战发送给物理网设备和无人机。如果超时或没有收到无人机与物理网设备返回的响应信息，则重新生成挑战，直到正常更新。

4　安全分析

本节首先基于MB逻辑[19]和ROR模型[41]对协议的安全目标进行形式化分析，验证其可达性以及各类攻击的不可行性。随后通过非形式化安全分析进一步论证所提出的协议的安全性，最后将所提出的协议与最近提出的方案进行对比，以评估其综合性能与优势。

4.1　基于MB逻辑的形式化证明

在形式化安全性分析中，本文采用MB逻辑[19]，利用其认证规则、机密性规则、超级主体规则、非验证规则、好密钥规则和新鲜推理规则进行推理验证。其中，符号D、A、S表示物理网设备D_i、无人机U_{av}和GCS。MB逻辑使用的符号表示如下。

1) $S\left|\equiv Q_i\right.$：S相信Q_i。

2) $S\left|\overset{k_i}{\sim} Q_i\right.$：$S$使用$k_i$对$Q_i$进行加密。

3) $S \overset{k_i}{\lhd} Q_i$：$S$可以用$Q_i$破译$k_i$。

4) $\#(Q_i)$：Q_i是唯一的，以前没有使用过。

5) $\sup(D)$：D是安全可靠的。

6) $S \lhd \|Q_i$：S无法获取消息Q_i。

7) $D \overset{Q_i}{\leftrightarrow} S$：$Q_i$是有效的共享密钥。

MB逻辑的规则如下。

1) 认证规则

$$\frac{S\models S \overset{K}{\leftrightarrow} D \wedge S \overset{K}{\lhd} M}{S\models D \overset{K}{\sim} M} \tag{3}$$

2) 保密规则

$$\frac{S\models S \overset{K}{\leftrightarrow} \mathrm{D} \wedge S\models A^c \lhd \|M \wedge S \overset{K}{\sim} M}{S\models (A \cup \{D\})^c \lhd \|M} \tag{4}$$

3) 好键规则

$$\frac{S\models \{S,D\}^c \lhd \|K \wedge S\models \#(K)}{S\models S \overset{K}{\leftrightarrow} D} \tag{5}$$

提议协议的假设如下。

1) S相信Q_i是D和S之间的一个很好的密钥。

Q_i以加密形式存储在D中，S使用存储在其数据库中的α_i和R_i，通过模糊提取器还原k_i，通过k_i计算Q_i。因此，“S相信Q_i是D和S之间的一个很好的密钥”，即

$$S\left|\equiv D \overset{Q_i}{\leftrightarrow} S\right. \tag{6}$$

S可以用Q_i破译k_i，因而

$$S \overset{k_i}{\lhd} Q_i \tag{7}$$

本文使用认证规则验证式(6)和式(7)，得到推论：“S相信D使用k_i加密了Q_i”，即

$$S\left|\equiv D \overset{k_i}{\sim} Q_i\right. \tag{8}$$

由于D在每个身份验证过程中都需要验证随机数N_d的新鲜性，而Q_i通过N_d加密，因此“S相信Q_i是新鲜的”，即

$$S\left|\equiv \#(Q_i)\right. \tag{9}$$

将非验证规则应用于式(8)和式(9)，得到结论：“S相信D相信$\mathrm{k_i}$是S和D之间的一个好的秘密密钥”，即

$$S\left|\equiv D\right|\equiv \overset{k_i}{\leftrightarrow} S \tag{10}$$

由于D每次验证时都需要验证随机数N_d的新鲜性，所以S认为除了D之外没有人可以访问Q_i。因此得出结论：“S认为除了D之外没有人可以访问Q_i”。即

$$S\left|\equiv D\right|\equiv \{S\}^c \lhd \|Q_i \tag{11}$$

将保密规则应用于式(8)、式(10)和式(11)，得到结论：“S相信D相信除了S和D之外没有其他人可以访问Q_i”，即

$$S\left|\equiv D\right|\equiv \{D,S\}^c \lhd \|Q_i \tag{12}$$

假设D是合法的物联网设备，S相信D是可信的，这表示为

$$S\left|\equiv \sup(D)\right. \tag{13}$$

将超级主体规则应用于式(11)和式(12)，得到结论：“S相信除了S和D之外没有其他人可以访问Q_i”，即

$$S \equiv \{D,S\}^c \lhd \|Q_i \tag{14}$$

现在，将好密钥规则应用于式(9)和式(12)，可以证明：“S相信Q_i是D和S之间的好秘密密钥”，即

$$S\left|\equiv D \overset{Q_i}{\leftrightarrow} S\right. \tag{15}$$

接下来，通过相关逻辑推理，可以证明语句：

“D相信Q_i是S和D之间一个很好的密钥”。

2) D相信Q_i是S和D之间一个很好的密钥。

由于k_i是由物联网设备D通过模糊提取器提取PUF响应R_i生成，而地面控制站S通过存储在其数据库中的α_i和R_i还原k_i，且需要经过一致性验证，因此可得：“D相信Q_i是S和D之间一个很好的密钥”。此外，D每次验证时都需要验证随机数N_d的新鲜性，而Q_i由N_d参与生成并通过k_i加密，且不通过信道传输，仅在本地通过确定性方式生成。因此“D认为除了S，没有其他人可以访问k_i”。由于D使用k_i加密Q_i。将保密规则应用于式(16)~式(18)，可得：“D相信除了D和S之外没有其他人可以访问Q_i”。

$$D\left|\equiv D\overset{Q_i}{\leftrightarrow}S\right. \tag{16}$$

$$D\left|\equiv \{\ S\ \}^{c}\lhd\|Q_i\right. \tag{17}$$

$$D\overset{k_i}{\sim}Q_i \tag{18}$$

$$S\equiv\{\ D,S\ \}^{c}\lhd\|Q_i \tag{19}$$

由于每次身份验证都需要验证随机数N_d的新鲜性而Q_i通过N_d加密，因此可得：“D认为Q_i是新鲜的”。将好密钥规则应用于式(19)和式(20)，可证明“D相信Q_i是D和S之间一个好的秘密密钥”。

$$D\left|\equiv\#(Q_i)\right. \tag{20}$$

$$D\left|\equiv D\overset{Q_i}{\leftrightarrow}S\right. \tag{21}$$

3) S相信G_{av}是S和A之间一个很好的密钥。

G_{av}以加密的形式存储在无人机A中，地面控制站S使用存储在其数据库中的α_v和R_{av}，通过模糊提取器还原k_{av}，通过k_{av}计算G_{av}。因此，“S相信G_{av}是A和S之间的一个很好的密钥”，即

$$S\left|\equiv A\overset{G_{\mathrm{av}}}{\leftrightarrow}S\right. \tag{22}$$

S可以用G_{av}破译k_{av}，因而

$$S\overset{k_{\mathrm{av}}}{\lhd}G_{\mathrm{av}} \tag{23}$$

通过认证规则验证式(22)和式(23)，可以得到：“S相信A使用k_{av}加密了G_{av}，即

$$S\left|\equiv A\overset{k_{\mathrm{av}}}{\sim}G_{\mathrm{av}}\right. \tag{24}$$

由于无人机A在每个身份验证过程中都需要验证随机数N_{uv}的新鲜性，而G_{av}通过N_{uv}加密，因此“S相信G_{av}是新鲜的”，即

$$S\left|\equiv\#(G_{\mathrm{av}})\right. \tag{25}$$

将非验证规则应用于式(24)和式(25)，可以推导出：“S相信A相信k_{av}是S和A之间的一个好的秘密密钥”，即

$$S|\ \equiv A|\equiv\overset{k_{\mathrm{av}}}{\leftrightarrow}S \tag{26}$$

由于无人机A每次验证时都需要验证随机数N_{uv}的新鲜性，所以“S认为除了A之外没有人可以访问G_{av}”，即

$$S|\ \equiv A|\equiv\{\ S\ \}^{c}\lhd\|G_{\mathrm{av}} \tag{27}$$

将保密规则应用于式(24)~式(27)，可以推导出：“S相信A相信除了S和A之外没有其他人可以访问G_{av}”，即

$$S|\ \equiv A|\equiv\{\ A,S\ \}^{c}\lhd\|G_{\mathrm{av}} \tag{28}$$

假设A是合法的无人机设备，“S相信A是可信的”，这表示为

$$S\left|\equiv\sup(A)\right. \tag{29}$$

将超级主体规则应用于式(27)和式(28)，可以推导出：“S相信除了S和A之外没有其他人可以访问G_{av}”，即

$$S\equiv\{\ A,S\ \}^{c}\lhd\|G_{\mathrm{av}} \tag{30}$$

将好密钥规则应用于式(25)和式(28)，可以证明“S相信G_{av}是D和A之间的好秘密密钥”，即

$$S\left|\equiv A\overset{G_{\mathrm{av}}}{\leftrightarrow}S\right. \tag{31}$$

4)A相信G_{av}是S和A之间一个很好的密钥。

由于k_{av}是由无人机A通过模糊提取器提取PUF响应R_{av}生成，而地面控制站S可利用存储在其数据库中的α_v和R_{av}还原k_{av}，且需经过一致性验证，因此可得：“A相信G_{av}是S和A之间一个很好的密钥”。而且A每次验证时都需要验证随机数N_{uv}的新鲜性，而G_{av}通过N_{uv}加密，并且G_{av}并不传输，只通过特殊方式生成，因此“A认为除了S，没有其他人可以访问k_{av}”。A使用k_{av}加密G_{av}。将保密规则应用于式(32)、式(33)和式(34)，可以证明：“A相信除了A和S之外没有其他人可以访问G_{av}”。

$$A\left|\equiv A\overset{G_{\mathrm{av}}}{\leftrightarrow}S\right. \tag{32}$$

$$A\left|\equiv\{S\}^{c}\lhd\|G_{\mathrm{av}}\right. \tag{33}$$

$$A\overset{k_{\mathrm{av}}}{\sim}Q_i \tag{34}$$

$$A\equiv\{A,S\}^{c}\lhd\|G_{\mathrm{av}} \tag{35}$$

由于每次身份验证还需要验证随机数N_{uv}的新鲜性而G_{av}通过N_{uv}加密，因此“A认为G_{av}是新鲜的。”将好密钥规则应用于，并证明“A相信G_{av}是A和S之间一个好的秘密密钥”。

$$A\left|\equiv\#(G_{\mathrm{av}})\right. \tag{36}$$

$$A\left|\equiv A\overset{G_{\mathrm{av}}}{\leftrightarrow}S\right. \tag{37}$$

因此，攻击者无法访问G_{av}和Q_i，同理可以证明k_{av}和k_i不能被对手访问。因此攻击者无法解密这些数据，无论攻击类型如何，例如中间人攻击、伪装攻击和重放攻击，k_{av}和k_i是由模糊提取器计算PUF的输出得出，并需要α_i和α_v来还原，通过模糊提取器的这种方式，有助于加密在PUF的计算和提高哈希函数的加密级别，加密的密钥无法被攻击者获取。

4.2　基于ROR模型的形式化证明

本节首先介绍ROR模型[41]，然后利用它对本文协议进行正式的安全性分析。ROR的组成部分含义如下。

参与者：本文协议包括地面控制站GCS、物联网设备D_i和无人机U_{av}这3个参与者，每个参与者可以执行多个实例，参与者的实例也称为预言机。令Π_{GCS}^{g}、$\Pi_{D_i}^{d}$、$\Pi_{U_{\mathrm{av}}}^{v}$表示GCS、$D_i$、$U_{\mathrm{av}}$的实例$g$、$d$和$v$。

新鲜性：如果2个参与方的会话钥没有泄露给攻击者A，那么实例Π_X^l或者Π_Y^l被称为新鲜的。

攻击者：在ROR模型中，攻击者能够完全控制通信信道，并对预言机进行执行查询、发送查询、无人机捕获查询、物理网设备捕获查询、测试查询等以下的查询。

$\mathrm{Execute}\left(\Pi_{\mathrm{GCS}}^{g},\Pi_{D_i}^{d},\Pi_{U_{\mathrm{av}}}^{v}\right)$：该查询模拟被动攻击。攻击者A用该查询能够获取协议参与者之间交换的所有消息。

$\mathrm{Send}\left(\Pi_X^l,m\right)$：该查询模拟主动攻击。执行该查询时，攻击者A向实例Π_X^l发送一个消息m，他能够收到该实例的响应消息。

$\mathrm{CorruptDevice}\left(\Pi_{U_{\mathrm{av}}}^{u}\right)$：该查询模拟无人机设备被捕获攻击，用此查询时，存储在无人机U_{av}的秘密信息将显示给攻击者A。

$\mathrm{CorruptIoTDevice}\left(\Pi_{D_i}^{\mathrm{d}}\right)$：该查询模拟物联网设备被捕获攻击，使用此查询时，攻击者A能够提取存储在物联网设备D_i中的秘密信息。

$\mathrm{Test}\left(\Pi_X^l\right)$：此查询根据ROR模型[41]的不可区分性来模拟会话钥的语义安全性。首先，攻击者A抛掷一枚无偏硬币c，其结果决定Test查询的输出。如果会话钥pk是一个新值，当$c=1$时，由GCS、D_i和U_{av}生成pk；当$c=0$时，生成一个随机数；否则生成一个空值。

会话钥的语义安全：根据ROR模型需要攻击者A来区分真实的会话钥和等长随机数。A可以对实例Π_X^l执行多次Test查询游戏Test查询中c的值为c'，如果$c'=c$，则表明A能够赢得该游戏。用$\mathrm{Adv}_{\mathrm{TN}}^{\mathrm{ake}}(\mathrm{A})=\left|2.\Pr[\mathrm{SUCCESS}]-1\right|$表示攻击者破坏协议TN的优势，其中SUCCESS表示赢得游戏的实例。对于任一概率多项式时间攻击者A，如果存在一个可忽略的函数m，满足$\mathrm{Adv}_{\mathrm{TN}}^{\mathrm{ake}}(\mathrm{A})\leqslant m$，则称协议TN在ROR模型下是语义安全的。

随机预言机：协议中所有的参与者和攻击者A都可以访问哈希函数$h(\cdot)$和$\mathrm{PUF}(\cdot)$，这2个函数都用随机预言机模拟的空间范围。

安全证明如下。

定理1　令TN表示本文协议FEN-AKE，A为ROR模型中破坏协议TN的攻击者，设q_{h}、q_{p}、q_{s}分别表示哈希函数（Hash）查询次数，物理不可克隆函数（PUF）查询次数，A主动发动消息的操作次数（Send）查询次数，$|\mathrm{Hash}|$和$|\mathrm{PUF}|$表示$h(\cdot)$和$\mathrm{PUF}(\cdot)$的空间范围，l表示会话密钥的位数。

$$\mathrm{Adv}_{\mathrm{TN}}^{\mathrm{ake}}(\mathrm{A})\leqslant\frac{q_{\mathrm{h}}^{2}}{|\mathrm{Hash}|}+\frac{q_{\mathrm{p}}^{2}}{|\mathrm{PUF}|}+\frac{2q_{\mathrm{s}}}{2^{l}} \tag{38}$$

证明　本文的证明类似于文献[42]中给出的证明。为了证明FEN-AKE的语义安全性，定义一系列游戏G_i（i=0,1,2,3,4,5）。令$\mathrm{SUCCESS}_i$表示攻击者在游戏G_i中猜出隐藏位c的事件。

游戏G_0：该游戏模拟对协议TN的真实攻击，由于在游戏开始就要求猜测隐藏位c，因此攻击者A的优势为

$$\mathrm{Adv}_{\mathrm{TN}}^{\mathrm{ake}}(\mathrm{A})=\left|2.\Pr\left[\mathrm{SUCCESS}_0\right]-1\right| \tag{39}$$

游戏G_1：该游戏模拟在公共信道上的窃听攻击。在该游戏中，A能通过执行查询$\mathrm{Execute}\left(\Pi_{\mathrm{GCS}}^{g},\Pi_{D_i}^{d},\Pi_{U_{\mathrm{av}}}^{v}\right)$，获取协议中参数方传输的所有消息，之后，A可以执行$\mathrm{Test}\left(\Pi_X^l\right)$查询，以确定Test的输出是真实会话钥还是一个随机数。攻击者需要DID_i、$\mathrm{uid}_{\mathrm{av}}$的分解技术，并需要通过模糊提取器还原的$k_i'$和$k_{\mathrm{av}}'$来计算$G_{\mathrm{av}}'$和$Q_i'$，由于这些值对A不可用，因此只有GCS、物联网设备D_i和无人机U_{av}才能计算会话密钥pk。因此，A赢得游戏G_1的概率不会更高。因此有

$$\Pr\left[\mathrm{SUCCESS}_1\right]=\Pr\left[\mathrm{SUCCESS}_0\right] \tag{40}$$

游戏G_2：游戏G_2在游戏G_1的基础上增加了Send查询和Hash查询。该游戏模拟一个主动攻击。在这种攻击中，攻击者A先通过执行Send查询欺骗参与者接受伪造消息，再重复使用Hash查询来检查是否发生哈希冲突。由于$\mathrm{TUID}_{\mathrm{av}}$和$\mathrm{TID}_i$被修改后将无法再合法参与者得到验证，并且交换的消息都包含了随机数，需要验证随机数的新鲜性，此外哈希操作是动态的，因此基于生日悖论，可以证明

$$\left|\Pr\left[\mathrm{SUCCESS}_2\right]-\Pr\left[\mathrm{SUCCESS}_1\right]\right|\leqslant\frac{q_h^2}{2|\mathrm{Hash}|} \tag{41}$$

游戏G_3：游戏G_3是在游戏G_2的基础上增加了PUF查询。由于$h(\cdot)$函数和$\mathrm{PUF}(\cdot)$函数都是单向函数，因此游戏G_3类似于游戏G_2，可以证明

$$\left|\Pr\left[\mathrm{SUCCESS}_3\right]-\Pr\left[\mathrm{SUCCESS}_2\right]\right|\leqslant\frac{q_{\mathrm{p}}^2}{2|\mathrm{PUF}|} \tag{42}$$

游戏G_4：游戏G_4增加了$\mathrm{CorruptIoTDevice}\left(\Pi_{D_i}^{d}\right)$查询，模拟物联网设备被捕获攻击。由于物联网设备中存储了DID_i、TID_i、α_i、Q_i，攻击者不能根据这些信息计算会话钥$\mathrm{pk}=h\left(N_g\|r_i\|G_{\mathrm{av}}'\|r_{\mathrm{av}}\|Q_i'\right)$。攻击者A在游戏$G_4$中没有增加任何优势，因此可以证明

$$\left|\Pr\left[\mathrm{SUCCESS}_4\right]-\Pr\left[\mathrm{SUCCESS}_3\right]\right|=0 \tag{43}$$

游戏G_5：游戏G_5增加了$\mathrm{CorruptDevice}\left(\Pi_{U_{\mathrm{av}}}^{u}\right)$查询，模拟无人机被捕获攻击，由于无人机$D_i$中存储了$\mathrm{uid}_{\mathrm{av}}$、$\mathrm{TUID}_{\mathrm{av}}$、$\mathrm{G}_{\mathrm{av}}$、$\alpha_v$，同理攻击者不能根据这些信息计算会话钥$\mathrm{pk}=h\left(N_g\|r_i\|G_{\mathrm{av}}'\|r_{\mathrm{av}}\|Q_i'\right)$。攻击者尝试利用Send查询拦截消息来计算会话密钥pk，其估计l位的会话密钥的概率为$\frac{1}{2^l}$。因此可以证明

$$\left|\Pr\left[\mathrm{SUCCESS}_5\right]-\Pr\left[\mathrm{SUCCESS}_4\right]\right|\leqslant\frac{q_{\mathrm{s}}}{2^l} \tag{44}$$

最后，要赢得G_5，需要在$\mathrm{Test}\left(\Pi_X^l\right)$查询猜测$c'$。因此，可以证明

$$\Pr\left[\mathrm{SUCCESS}_5\right]=\frac{1}{2} \tag{45}$$

根据式(38)~式(45)，可以得到

$$\begin{aligned}\mathrm{Adv}_{\mathrm{TN}}^{\mathrm{ake}}(\mathrm{A})&=2\left|\Pr\left[\mathrm{SUCCESS}_0\right]-\frac{1}{2}\right|\leqslant\\&2\left|\Pr\left[\mathrm{SUCCESS}_1\right]-\Pr\left[\mathrm{SUCCESS}_2\right]\right|+\\&2\left|\Pr\left[\mathrm{SUCCESS}_2\right]-\Pr\left[\mathrm{SUCCESS}_3\right]\right|+\\&2\left|\Pr\left[\mathrm{SUCCESS}_3\right]-\Pr\left[\mathrm{SUCCESS}_4\right]\right|+\\&2\left|\Pr\left[\mathrm{SUCCESS}_4\right]-\Pr\left[\mathrm{SUCCESS}_5\right]\right|\leqslant\\&\frac{q_{\mathrm{h}}^2}{|\mathrm{Hash}|}+\frac{q_{\mathrm{p}}^2}{|\mathrm{PUF}|}+\frac{2q_{\mathrm{s}}}{2^l}\end{aligned} \tag{46}$$

4.3 非形式化安全分析

1) 匿名性和不可追溯性（A1）：在认证阶段，攻击者可以窃听在安全通道上交换的信息，但是GCS、物联网设备D_i和无人机U_{av}的真实信息通过哈希函数加密，攻击者无法计算出其真实身份，因此该方案具有匿名性，并且在GCS、D_i和U_{av}的消息传递中，都包含随机数，并且下一步的认证过程传递的消息不同，是动态变化的，因此这个方案是不可跟踪的。

2) 相互认证（A2）：在提出的协议中，GCS认证U_{av}和D_i需要验证$M_2^*=h(\mathrm{TID}_i\|N_d\|M_1\|\mathrm{TUID}_{\mathrm{av}}\|N_{\mathrm{uv}}\|\mathrm{uid}_{\mathrm{av}}\|k_{\mathrm{av}}')$和$M_1^*=h\left(\mathrm{DID}_i\|\mathrm{TID}_i\|N_d\|k_i'\|Q_i'\right)$，如果攻击者想要假装$U_{\mathrm{av}}$和$D_i$，那它需要获取$M_1$和$M_2$的值，但它们都通过模糊提取器生成密钥加密，而这个密钥不会直接传输，只能通过模糊提取器来恢复，并且U_{av}和D_i的真实身份无法被计算出，相同的，U_{av}认证GCS，U_{av}需要通过验证$M_4=h\left(\mathrm{TID}_i\|N_{\mathrm{uv}}\|N_d\|c_{\mathrm{av}}\|p_2\|p_1\|N_g\|M_3\|\mathrm{uid}_{\mathrm{av}}\|G_{\mathrm{av}}'\|k_{\mathrm{av}}'\right)$，但攻击者无法计算出无人机的真实身份$\mathrm{uid}_{\mathrm{av}}$，它们通过会话密钥与哈希函数进行了加密，$D_i$验证$U_{\mathrm{av}}$也是相同的道理，通过验证$M_3=h(\mathrm{TUID}_{\mathrm{av}}\|N_{\mathrm{uv}}\|c_i\|p_2\|$

$N_g\|\mathrm{DID}_i\|Q_i'\|k_i'$)，但攻击者无法计算物联网设备 D_i 的真实身份 DID_i，且并不会传输，只存储在物联网设备中，并且通过随机数的新鲜度验证不通过，则 Q_i 失效，而 GCS 虽然知道计算方式，但需要通过模糊提取器恢复 k_i'，并且要对比认证 k_i，同理 G_{av}' 也是如此，并且 GCS 可以通过 U_{av} 传输的 M_1 的值来认证 D_i，即 GCS 与 D_i 实现的相互认证，而 D_i 与 U_{av} 通过 M_3 进行验证，即 D_i 与 U_{av} 实现的相互认证。所以该方案满足相互认证的要求。

3) 完全前向保密（A3）：本文通过 PUF 产生的响应对会话密钥 pk 进行加密，而 D_i 和 U_{av} 的身份信息 DID_i 和 $\mathrm{uid}_{\mathrm{av}}$ 分别存储在自身中，而 G_{av}' 和 Q_i' 在 GCS 中的安全模块中，攻击者无法访问，攻击者可以获取其中的一项，来计算会话密钥 pk，$\mathrm{pk} = h\left(N_g\|r_i\|G_{\mathrm{av}}'\|r_{\mathrm{av}}\|Q_i'\right)$，$p_1 = \mathrm{pk}\oplus h\left(\mathrm{uid}_{\mathrm{av}}\|r_{\mathrm{av}}\|N_g\|G_{\mathrm{av}}'\right)$，$p_2 = \mathrm{pk}\oplus h\left(\mathrm{DID}_i\|r_i\|N_g\|Q_i'\right)$ 而使用过的挑战响应 CRP，在 GCS 中已经被删除，因此攻击者无法获取之前的 CRP。所以，提议的协议保证了完全的前向保密。

4) 抗物理捕获攻击（A4）：由于 PUF 具有防物理篡改的属性，所以攻击者物理访问物联网设备，任何对 PUF 直接或间接的篡改 PUF，破坏其身份认证，都是无法实现的。根据 PUF 的不可克隆性，攻击者无法复制无人机上的 PUF，即使捕获到无人机也无法获得数据，因此，提出的协议能防止物理捕获攻击。

5) 抗重放攻击（A5）：重放攻击是攻击者截获合法的数据传输并重新发送，以欺骗接收方，本文协议为防止攻击者试图通过转发给 GCS、D_i 和 U_{av} 重复相同的消息，在每个生成消息中都应用到随机数，而不同的设备会通过验证随机数的新鲜度来验证消息的新鲜度，如果验证消息发送的随机数与接受的随机数不在一个生命周期内，则无效，因此提出的协议可以抵御重放攻击。

6) 抗克隆攻击（A6）：克隆攻击是攻击者通过复制合法用户的设备或身份信息，创建一个与合法用户完全相同的克隆实体。由于 PUF 的固有属性，攻击者任何试图物理访问 D_i 和 U_{av} 都会改变 PUF 的特性，导致其无法使用，所以该协议能够抵御克隆攻击。

7) 抗中间人攻击（A7）：中间人攻击是一种网络攻击，攻击者通过窃听或假装是合法参与者来拦截现有的对话或数据传输，为了发动中间人攻击，攻击者必须修改截获的消息，但是，在 GCS、D_i 和 U_{av} 在传输消息时都通过随机数和时间戳验证，并通过模糊提取器生成密钥 k_i，后面通过 PUF 响应还原密钥，由于 PUF 的响应不可克隆和修改，因此该协议也能够抵御中间人攻击。

8) 抗伪装攻击（A8）：协议利用了噪声物理不可克隆函数和模糊提取器来生成与设备硬件特性绑定的唯一身份标识符。这些标识符基于设备的物理特性，具有唯一性和不可克隆性。具体来说，每个设备在注册阶段都会生成一个基于其硬件噪声特性的 PUF 响应，并通过模糊提取器生成稳定的密钥和辅助数据。这些密钥和辅助数据用于后续的认证过程，只有合法设备才能通过其物理特性再现正确的响应，从而生成有效的认证信息。协议中也设计了严格的相互认证流程。在认证阶段，物联网设备、无人机和地面控制站需要相互验证对方的身份和合法性。这一过程涉及多个步骤的挑战–响应机制，每个实体都需要证明其拥有正确的密钥和身份信息，而这些信息是基于其硬件特性生成的，攻击者无法在未授权的设备上复制或生成。例如，物联网设备在与无人机进行通信时，会向无人机发送挑战，无人机必须使用其内部生成的密钥来生成响应，该响应随后会被物联网设备验证。同样，无人机和地面控制站之间也会进行类似的相互认证过程。这种相互认证确保了通信双方的真实身份，防止了攻击者伪装成合法实体进行通信，此外，协议通过事件驱动的挑战–响应对更新机制进一步增强了抗伪装攻击的能力。每次认证完成后，系统会动态更新 CRP，确保每次通信都基于最新的认证信息。这使得攻击者即使截获了之前的通信内容，也无法利用过时的 CRP 进行伪装攻击，因为旧的 CRP 已经被系统废弃，无法再用于有效的认证。

9) 避免时钟同步（A9）：本文协议不使用时间戳，而是通过使用具有生命周期的随机数，通过验证随机数的新鲜性，保证消息的新鲜性。因此，不需要考虑时钟同步和时间延迟，即 D_i 与 GCS 不需要同步系统时钟，U_{av} 与 GCS 不需要同步系统时钟，D_i 与 U_{av} 也不需要同步系统时钟。

10)密钥协商（A10）：在协议中，会话密钥首先由 GCS 进行计算 $\mathrm{pk} = h\left(N_g\|r_i\|G_{\mathrm{av}}'\|r_{\mathrm{av}}\|Q_i'\right)$，虽然

N_g可以被获取，但依旧需要经过时间戳的验证其新鲜度，而r_i和r_{av}都是PUF生成的响应，只有在U_{av}和D_i上才能获取生成，而通过pk = $p_2 \oplus h\left(\text{DID}_i \| r_i \| N_g\right)$获取会话密钥，需要计算$\text{DID}_i$和$r_i$，这2个值只有$D_i$知道，无人机通过pk = $p_1 \oplus h\left(\text{uid}_{\text{av}} \| r_{\text{av}} \| N_g\right)$时，需要计算$\text{uid}_{\text{av}}$和$r_{\text{av}}$，这2个值也只有$\text{U}_{\text{av}}$知道，这些都是动态值，因此，该协议支持会话密钥协议。

11) 抗窃听攻击（A11）：攻击者可以拦截在公共通道上传输的任何消息。本文协议攻击者可以获得{TID_i,N_d,M_1}，{TUID_{av},N_{uv},M_2}，{c_i,c_{av},p_1,p_2,N_g,M_3,M_4}，然而，攻击者仍然不能得到会话密钥，因为生成密钥所需的Q_i和G_{av}没有直接传输，需要通过模糊提取器生成的k_i和k_{av}，才能还原，因此不会向攻击者披露。

12) 机器建模攻击（A12）：协议引入了事件驱动的CRP动态更新机制。每次认证完成后，系统会根据预设的事件触发条件，当认证次数达到一定阈值或检测到潜在的攻击行为，自动更新CRP。更新后的CRP将替换旧的CRP，并用于后续的认证过程。由于攻击者无法预知新的CRP内容，即使截获了部分旧的CRP，也无法利用这些信息对设备进行建模或预测未来的响应，通过模糊提取器生成稳定的密钥和辅助数据，用于后续的认证和会话密钥协商过程中。利用模糊提取器的还原性，需要CRP变化在一定的阈值，否则也无法提取准确的密钥信息，然而噪声PUF产生的响应并不唯一，即使攻击者能够截获部分通信数据，也无法从中提取到足够的信息来重建合法设备的PUF响应或生成有效的认证信息。最后，本文协议结合HSM存储关键信息，如CRP和设备身份信息，提供了高度安全的存储环境，能够有效防止信息泄露。由于攻击者无法轻易获取这些关键信息，即使他们试图通过机器学习等技术进行建模，也会因为缺乏完整的数据集而难以成功。这样就进一步增强了协议抵御机器建模攻击的能力。

5 性能分析

本节将从安全功能、计算开销和通信开销3个方面对本文协议进行分析，并与文献[29,42-45]的协议进行对比。文献[29]构建了现场无人机−中心无人机−地面控制站的三方架构，与本文协议在拓扑结构上具有同构性，其创新性地引入混沌多项式实现密钥随机化，而本文协议则通过量化PUF固有噪声生成可还原密钥。两者目标相近，但本文协议不需要额外混沌运算，显著降低了存储开销，对比可凸显本文协议在资源效率方面的优势。文献[42]未考虑环境噪声导致的PUF输出偏移，两者对比可量化评估噪声适应机制对成功率的提升，该文献采用BAN逻辑和ROR模型，与本文协议的形式化分析框架一致，确保安全对比的方法论对等性。文献[43]是车辆−RSU−信任机构的三方架构，与本文在实体模型、信任模型和通信模式存在同构性，确保性能对比的结构公平，该文献采用纯哈希、异或运算实现轻量化，两者对比可清晰量化硬件安全模块在噪声环境下的额外开销边际成本，证明本文协议的实用性。文献[44]采用跟随无人机−领导无人机−地面控制站的三方模型，同样与本文协议同构，该文献提出了一种专用PUF集成电路以增强响应鲁棒性，旨在解决环境扰动下的稳定性问题，与本文协议虽目标一致，但是其通过噪声PUF建模与模糊提取器协同设计，在更少的通信轮次内完成三方认证，从而在保持鲁棒性的同时提升了协议效率。文献[45]代表一类传统密码学方案，仅依赖哈希函数与对称加密操作实现认证，未利用硬件特征（如PUF）实现设备唯一性绑定，亦未考虑信道噪声对密钥生成的影响。尽管其计算开销较低，但在匿名性、抗物理捕获、前向安全性等关键安全属性上存在不足，且通信开销较高。将其作为经典基线，可凸显本文协议在复杂动态场景下综合安全能力与适应性的优越性。最终得出，本文协议在综合性能上具有更大优势，适用于资源受限的无人机在高动态的复杂噪声环境下的应用。

5.1 安全功能对比

表3将其他协议的安全属性进行对比，其中√表示满足该安全属性，×表示不满足该安全属性。在这些协议中，虽然文献[29,43,45]实现了设备之间的相互认证，但文献[43,45]中的协议都不能抵御中间人攻击和窃听攻击，文献[45]没有实现完全的前向保密，在克隆攻击和窃听攻击下存在着安全隐患。文献[44-45]和本文协议满足密钥协商的属性，但文献[44]提出的协议对克隆攻击的防御依旧是不安全的。这些协议都需要使用时间戳以保

证严格的时钟同步，而本文协议通过使用具有生命周期的随机数，验证其新鲜性避免了时钟同步。有的协议虽然使用了PUF，但只是预存足够多的CRP，没有考虑到攻击者可以通过收集足量的CRP进行机器建模攻击，而本文协议通过基于事件触发的CRP更新机制，对CRP进行更新，达到了抵御机器建模攻击的目的。因此FEN-AKA实现了更多的安全属性，能够抵抗各种已知攻击。

表3　　安全功能对比

安全属性	文献[29]	文献[42]	文献[43]	文献[44]	文献[45]	FEN-AKA
A1	√	√	√	√	√	√
A2	√	×	√	×	√	√
A3	√	√	√	√	×	√
A4	√	√	√	√	√	√
A5	√	√	√	√	√	√
A6	√	×	√	×	×	√
A7	×	×	×	√	√	√
A8	√	√	√	√	√	√
A9	×	×	×	×	×	√
A10	×	×	×	√	√	√
A11	×	√	×	√	×	√
A12	×	×	×	×	×	√

5.2　通信开销对比

本文将FEN-AKA与其他协议进行通信成本的对比，考虑安全参数的位长如下：真实身份、临时身份、哈希输出的位大小都为160 bit，随机数由128 bit组成，模糊提取器密钥、PUF质询和响应都为128 bit，时间戳为64 bit，ECC标量点乘为320 bit，身份标识符为32 bit，辅助数据为32 bit。各个协议的通信开销对比如表4所示。文献[29]进行了4轮通信交互，其长度分别为672 bit、832 bit、704 bit、704 bit，总通信开销为2 912 bit。文献[42]进行了4轮通信交互，其长度分别为544 bit、704 bit、1 024 bit、544 bit，总通信开销为2 816 bit。文献[43]进行了4轮通信交互，其长度分别为704 bit、1 248 bit、1 024 bit、704 bit，总通信开销为3 680 bit。文献[44]进行了6轮通信交互，其长度分别为544 bit、544 bit、864 bit、1 024 bit、544 bit、544 bit，总通信开销为4 064 bit。文献[45]中通信4轮，其长度分别为864 bit、640 bit、1 152 bit、1 088 bit，总通信开销为3 744 bit。FEN-AKA进行了4轮通信交互，其长度分别为448 bit、864 bit、896 bit、1 024 bit，总通信开销为3 232 bit。

表4　　各个协议的通信开销对比

协议	通信轮次/轮	总通信开销/bit
文献[29]	4	2 912
文献[42]	4	2 816
文献[43]	4	3 680
文献[44]	6	4 064
文献[45]	4	3 744
FEN-AKA	4	3 232

由表4通信代价对比结果可知，文献[42]和文献[29]的通信代价最低，但由表3可知，两者不满足一些关键的安全属性。由计算开销对比可知，其计算代价也比本文提出的协议要高。FEN-AKA在保障安全特性的基础上，与多数方案保持相同的通信轮次，并且实现了较低的通信代价。因此，FEN-AKA在通信效率和安全性之间取得了更好的平衡。

5.3　计算开销对比

本文用协议中所有参与方执行密码原语的总运行时间来评估计算代价。令T_h、T_e、T_p、T_{epm}、T_{mac}、T_{hmac}、T_x、T_{ch}、T_{fe}和T_{puf}分别表示哈希函数、对称密码加密或者解密、对称多项式、ECC点乘、MAC、哈希MAC、XOR运算、切比雪夫混沌运算、模糊提取器和PUF的运算时间，并且$T_h \approx T_{mac} \approx T_{hmac}$。基于已有的测试结果[42-45]同一标准下对对比协议的计算代价进行估算，现有实验在以下设备进行了模拟实验：物联网设备使用Android 4.4.2OS下具有2.45 GHz处理器和2 GB RAM的移动设备，使用Cortex-A53(ARMv8) 64位SoC @ 1.4 GHz处理器的Pi3 B+，使用1 GB LPDDR2 SDRAM RAM来模拟无人机，使用ICPU 2.90 GHz、RAM 4 GB、操作系统Windows10的笔记本电脑模拟了地面站控制站，实验中使用了PBC-0.5.14加密库来评估密码原语的执行时间。这些密码原语的近似操作时间如表5所示，其中N/A代表GCS未使用PUF。

表 5 密码原语近似运行时间

设备	T_h	T_e	T_x	T_{fe}	T_{puf}	T_{ch}
无人机 U_{av}	0.015	0.005 2	0.018	0.097	0.031	0.841
物联网设备 D_i	0.011	0.005 2	0.011	0.063	0.039	0.262
GCS	0.006	0.046	0.001	0.062	N/A	0.095

各个协议的计算开销对比如表 6 所示，其中 N/A 代表未使用物理网设备。文献[29]中，物联网设备的执行时间为 $3T_h + T_{ch} + 2T_e + 2T_{puf} + 2T_x \approx 0.455\,4$ ms，无人机的执行时间为 $6T_h + T_{ch} + 3T_e + 2T_{puf} + 4T_x \approx 1.080\,6$ ms，地面控制站的执行时间为 $4T_h + T_{ch} + 3T_e + 4T_x \approx 0.261$ ms，总计算代价大约为 1.797 ms。文献[42]中，物联网设备的执行时间为 $5T_h + 8T_x + T_e \approx 0.195$ ms，无人机的执行时间为 $7T_h + 14T_x + 2T_e \approx 0.367\,4$ ms，地面控制站的执行时间为 $15T_h + 6T_x \approx 0.906$ ms，总计算代价约为 1.123 ms。文献[43]中，物联网设备的执行时间为 $6T_h + 5T_x \approx 0.121$ ms，无人机的执行时间 $4T_h + 2T_x \approx 0.096$ ms，地面控制站的执行时间为 $15T_h + 6T_x \approx 0.906$ ms，总计算代价约为 1.123 ms。文献[44]中，物联网设备的执行时间为 $5T_h + 8T_x + T_e + 2T_{puf} \approx 0.226\,2$ ms，无人机的执行时间为 $9T_h + 15T_x + T_e \approx 0.410\,2$ ms，地面控制站的执行时间为 $5T_h + 12T_x + T_e + T_{fe} \approx 0.15$ ms，总计算代价约为 0.786 4 ms。文献[45]中，无人机的执行时间为 $7T_h + 8T_x + 2T_e \approx 0.259$ ms，地面控制站的执行时间为 $6T_h + 7T_x + 2T_e \approx 0.039$ ms，总计算代价约为 0.394 ms。

FEN-AKA 的计算代价为 0.541 ms，其中物联网设备的执行时间为 $2T_h + 3T_x + T_{fe} + T_{puf} \approx 0.157$ ms，无人机的执行时间为 $2T_h + 3T_x + T_{fe} + T_{puf} \approx 0.212$ ms，地面控制站的执行时间为 $7T_h + 6T_x + 2T_{fe} \approx 0.172$ ms，只比文献[45]略高一些，但文献[45]并未使用到物联网设备，只有 2 个参与方，而其他协议有 3 个参与方，并且计算代价都比本文的要高。虽然文献[45]比本文协议略低，但本文协议平均减少了 21.2% 的计算开销。

5.4 存储开销对比

本文将 FEN-AKA 与其他协议进行存储成本的对比，如表 7 所示。由表 7 可知，FEN-AKA 的总存储成本为 3 808 bit，仅略高于文献[43]，展现出优异的存储效率，尽管文献[43]在车联网场景下实现了更低的存储成本，但其在通信开销和计算代价以及安全属性的全面性方面存在不足，相比之下，FEN-AKA 在保障安全特性的基础上，相较于本文对比的其他协议，实现了更低的存储开销。综合来看，FEN-AKA 在存储成本上相较其他对比协议方案平均降低了 14.4%，在资源效率与安全性之间取得了更优的平衡，具备更强的综合优势和应用潜力。

表 7 存储开销对比

协议	物联网设备 D_i/bit	无人机 U_{av}/bit	地面控制站/bit	总存储成本/bit
文献[29]	1 536	1 536	2 912	5 984
文献[42]	1 664	1 664	1 696	5 024
文献[43]	1 280	608	1 728	3 616
文献[44]	1 472	1 472	1 600	4 544
文献[45]	896	1 440	2 528	4 864
FEN-AKA	1 120	1 120	1 568	3 808

6 结束语

FEN-AKA 为无人机、物联网设备和地面控制站建立了基于三方通信的相互认证的安全会话。为

表 6 计算开销对比

协议	物联网设备 D_i/ms	无人机 U_{av}/ms	地面控制站/ms	总计算开销/ms
文献[29]	$3T_h + T_{ch} + 2T_e + 2T_{puf} + 2T_x \approx 0.455\,4$	$6T_h + T_{ch} + 3T_e + 2T_{puf} + 4T_x \approx 1.080\,6$	$4T_h + T_{ch} + 3T_e + 4T_x \approx 0.261$	1.797
文献[42]	$5T_h + 8T_x + T_e \approx 0.195$	$7T_h + 14T_x + 2T_e \approx 0.367\,4$	$6T_h + 12T_x + T_e \approx 0.094$	0.656 4
文献[43]	$6T_h + 5T_x \approx 0.121$	$4T_h + 2T_x \approx 0.096$	$15T_h + 6T_x \approx 0.906$	1.12 3
文献[44]	$5T_h + 8T_x + T_e + 2T_{puf} \approx 0.226\,2$	$9T_h + 15T_x + T_e \approx 0.410\,2$	$5T_h + 12T_x + T_e + T_{fe} \approx 0.15$	0.786 4
文献[45]	N/A	$7T_h + 8T_x + 2T_e \approx 0.259$	$6T_h + 7T_x + 2T_e \approx 0.135$	0.394
FEN-AKA	$2T_h + 3T_x + T_{fe} + T_{puf} \approx 0.157$	$2T_h + 3T_x + T_{fe} + T_{puf} \approx 0.212$	$7T_h + 6T_x + 2T_{fe} \approx 0.172$	0.541

了保证物理安全，协议联合使用了噪声 PUF 和模糊提取器，利用模糊提取器的可还原性，确保生成密钥的关键信息不会在公共信道传输。同时，通过硬件安全模块存储一些关键性的数据，保证这些数据不易被物理破坏所获取。FEN-AKA 利用随机数的生命周期来代替时间戳的使用，有效防范重放攻击。会话密钥的安全性通过 MB 逻辑形式化验证得以保证，而整体协议的安全性则在 ROR 模型下得到证明。此外，非形式化安全分析表明，该协议能够抵抗多种已知攻击。对比实验结果显示，本文协议在支持更全面安全属性的同时，具备更低的通信与计算开销，更适用于无人机在高空复杂环境下的安全通信需求。未来工作将探索该协议在无人机集群场景下的扩展方案，设计支持群组认证与动态成员管理的轻量级密钥协商机制，通过引入分簇结构，降低中心节点的负担，提升系统的扩展性与容错能力，进一步推动 FEN-AKA 在复杂空地一体化网络中的实际部署。

参考文献：

[1] XIE M L, ZHAO W H, JU N P, et al. Landslide evolution assessment based on InSAR and real-time monitoring of a large reactivated landslide, Wenchuan, China[J]. Engineering Geology, 2020, 277: 105781.

[2] LI X, TAN J W, LIU A F, et al. A novel UAV-enabled data collection scheme for intelligent transportation system through UAV speed control[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(4): 2100-2110.

[3] MUALLA Y, NAJJAR A, DAOUD A, et al. Agent-based simulation of unmanned aerial vehicles in civilian applications: a systematic literature review and research directions[J]. Future Generation Computer Systems, 2019, 100: 344-364.

[4] VANGALA A, DAS A K, MITRA A, et al. Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural IoT networks[J]. IEEE Transactions on Information Forensics and Security, 2022, 18: 904-919.

[5] GUO Y M, GUO Y J, XIONG P, et al. Deeper insight into why authentication schemes in IoT environments fail to achieve the desired security[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4615-4627.

[6] KARMAKAR R, KADDOUM G, AKHRIF O. A blockchain-based distributed and intelligent clustering-enabled authentication protocol for UAV swarms[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 6178-6195.

[7] ALABA F A, OTHMAN M, HASHEM I A T, et al. Internet of Things security: a survey[J]. Journal of Network and Computer Applications, 2017, 88: 10-28.

[8] BARBARESCHI M, DE BENEDICTIS A, LA MONTAGNA E, et al. A PUF-based mutual authentication scheme for Cloud-Edges IoT systems[J]. Future Generation Computer Systems, 2019, 101: 246-261.

[9] CHATTERJEE B, DAS D, MAITY S, et al. RF-PUF: enhancing IoT security through authentication of wireless nodes using *in situ* machine learning[J]. IEEE Internet of Things Journal, 2019, 6(1): 388-398.

[10] GUO Y M, GUO Y J. CS-LAKA: a lightweight authenticated key agreement protocol with critical security properties for IoT environments[J]. IEEE Transactions on Services Computing, 2023, 16(6): 4102-4114.

[11] SHAO X W, GUO Y J, GUO Y M. A PUF-based anonymous authentication protocol for wireless medical sensor networks[J]. Wireless Networks, 2022, 28(8): 3753-3770.

[12] CHOI D, SEO S H, OH Y S, et al. Two-factor fuzzy commitment for unmanned IoT devices security[J]. IEEE Internet of Things Journal, 2019, 6(1): 335-348.

[13] LU C, LIU Y, JIN K, et al. A lightweight and secure access authentication scheme for UAV formation[C]//Proceedings of the 2025 IEEE 19th International Conference on Control & Automation (ICCA). Piscataway: IEEE Press, 2025: 656-660.

[14] 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.

[15] SON S, PARK Y, PARK Y. A secure, lightweight, and anonymous user authentication protocol for IoT environments[J]. Sustainability, 2021, 13(16): 9241.

[16] MALL P, AMIN R, OBAIDAT M S, et al. CoMSeC++: PUF-based secured light-weight mutual authentication protocol for Drone-enabled WSN[J]. Computer Networks, 2021, 199: 108476.

[17] DELVAUX J, GU D W, VERBAUWHEDE I, et al. Efficient fuzzy extraction of PUF-induced secrets: theory and applications[C]//Cryptographic Hardware and Embedded Systems – CHES 2016. Berlin: Springer, 2016: 412-431.

[18] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

[19] MAO W, BOYD C. Towards formal analysis of security protocols[C]//Proceedings of Computer Security Foundations Workshop VI. Piscataway: IEEE Press, 1993: 147-158.

[20] 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.

[21] 郭奕旻, 张振峰, 熊平, 等. 基于 PUF 的轻量级雾辅助物联网认证协议[J]. 计算机学报, 2022, 45(7): 1412-1430.
GUO Y M, ZHANG Z F, XIONG P, et al. PUF-based lightweight authentication protocols for fog assisted IoT[J]. Chinese Journal of Computers, 2022, 45(7): 1412-1430.

[22] TIAN C, MA J F, LI T, et al. Provably and physically secure UAV-assisted authentication protocol for IoT devices in unattended settings[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4448-4463.

[23] ADIL M, ABULKASIM H, FAROUK A, et al. R3ACWU: a lightweight, trustworthy authentication scheme for UAV-assisted IoT applications[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(6): 6161-6172.

[24] SHARMA J, SINGH MEHRA P. G2CAIUN: a novel Genus-2 curve-based authentication for secure data transmission in IoT-based UAV networks[J]. Physical Communication, 2025, 71: 102647.

[25] SHARMA J, MEHRA P S. HCFAIUN: a novel hyperelliptic curve and fuzzy extractor-based authentication for secure data transmission in

IoT-based UAV networks[J]. Vehicular Communications, 2024, 49: 100834.
[26] RAHMAN K, KHAN M A, AFGHAH F, et al. An efficient authentication and access control protocol for securing UAV networks against anomaly-based intrusion[J]. IEEE Access, 2024, 12: 62750-62764.
[27] BANSAL G, NAREN, CHAMOLA V, et al. SHOTS: scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms[J]. IEEE Transactions on Vehicular Technology, 2022, 71(6): 5827-5836.
[28] BENSSALAH M, DROUICHE K. On the security of the novel authentication scheme for UAV-ground station and UAV-UAV communication[C]// Proceedings of the 20th International Conference on Security and Cryptography. SCITEPRESS - Science and Technology Publications. Setúbal: Science and Technology Publications, Lda., 2023: 361-368.
[29] ASHRAF CHAUDHRY S, IRSHAD A, ALZAHRANI B A, et al. TS-PAID: a two-stage PUF-based lightweight authentication protocol for Internet of drones[J]. IEEE Access, 2024, 13: 1458-1469.
[30] TENG Y L, ZHANG P C, LIU Y Y, et al. Exploiting carrier frequency offset and phase noise for physical layer authentication in UAV-aided communication systems[J]. IEEE Transactions on Communications, 2024, 72(8): 4708-4724.
[31] ZHOU Y, MA Z, LIU H, et al. Signal-to-noise ratio based physical layer authentication in UAV communications[C]//Proceedings of the 2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). Piscataway: IEEE Press, 2023: 1-6.
[32] 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.
[33] SINGH N, DAS A K. TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor[J]. The Journal of Supercomputing, 2024, 80(1): 865-914.
[34] MA W B, FANG W C. A PUF-based mutual authentication protocol with fuzzy extractors for biometric identification[C]//Proceedings of the 2024 International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan). Piscataway: IEEE Press, 2024: 679-680.
[35] AMAEL J T, NATAN O, ISTIYANTO J E. High-security hardware module with PUF and hybrid cryptography for data security[J]. arXiv Preprint, arXiv: 2409.09928, 2024.
[36] MURTAZA M H, TAHIR H, TAHIR S, et al. A portable hardware security module and cryptographic key generator[J]. Journal of Information Security and Applications, 2022, 70: 103332.
[37] PIRKER D, FISCHER T, LESJAK C, et al. Global and secured UAV authentication system based on hardware-security[C]//Proceedings of the 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). Piscataway: IEEE Press, 2020: 84-89.
[38] CHEON J H, JEONG J, KIM D, et al. A reusable fuzzy extractor with-Practical storage size: modifying Canettiet al.'s construction[C]//Information Security and Privacy. Berlin: Springer, 2018: 28-44.
[39] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.
[40] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]//Advances in Cryptology-EUROCRYPT 2001. Berlin: Springer, 2001: 453-474.
[41] ROY S, DAS A K, CHATTERJEE S, et al. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications[J]. IEEE Transactions on Industrial Informatics, 2019, 15(1): 457-468.
[42] ZHANG L, XU J B, OBAIDAT M S, et al. A PUF-based lightweight authentication and key agreement protocol for smart UAV networks[J]. IET Communications, 2022, 16(10): 1142-1159.
[43] LI X, LIU T, OBAIDAT M S, et al. A lightweight privacy-preserving authentication protocol for VANETs[J]. IEEE Systems Journal, 2020, 14(3): 3547-3557.
[44] CHANDRAN I, VIPIN K. A PUF secured lightweight mutual authentication protocol for multi-UAV networks[J]. Computer Networks, 2024, 253: 110717.
[45] JAN S U, QAYUM F, KHAN H U. Design and analysis of lightweight authentication protocol for securing IoD[J]. IEEE Access, 2021, 9: 69287-69306.

[作者简介]

宋建华（1973– ），女，湖北襄阳人，博士，湖北大学教授、硕士生导师，主要研究方向为网络与信息安全。

刘世炜（2000– ），男，湖北孝感人，湖北大学硕士生，主要研究方向为网络安全、身份认证协议。

张龑（1974– ），男，湖北宜昌人，博士，湖北大学教授、博士生导师，主要研究方向为代码安全。