arXiv:2304.00795v1 [cs.RO] 3 Apr 2023

Alice 真的身处仙境吗？基于超宽带的位置证明：面向无人机的 Hyperledger Fabric 区块链方案

Lei Fu[1], Paola Torrico Mor´on[1], Jorge Pe˜na Queralta[1], DavidH¨astbacka[2],Harry Edelman[3],和 Tomi Westerlund[1]

[1] 图尔库智能与嵌入式机器人系统，图尔库大学，芬兰{leifu, pctomo, jopequ, tovewe}@utu.fi — https://tiers.utu.fi[2] 工程与商务系，图尔库应用科学大学，芬兰 — harry.edelman@turkuamk.fi[3] 计算科学，信息技术与传播科学学院，坦佩雷大学，芬兰 — david.hastbacka@tuni.fi

摘要。 由于越来越多的无人机被广泛用于城市区域的各种用途，无人驾驶航空器（无人机）的远程识别正变得日益重要。例如，在美国和欧盟，识别与位置广播已成为使用无人机的要求。然而，当前解决方案验证的是无人机的身份标识，而非其位置，并且会信任所提供的位置。因此，需要一种更先进的方案来证明位置，以避免位置欺骗。我们提出将由公共机构管理的许可型区块链与基于超宽带的通信相结合，以实现这一目标。具体而言，我们利用 Hyperledger Fabric 这一开源许可型区块链框架中的身份管理工具，以及超宽带（UWB）测距，从而实现定位通信（即同时进行通信与定位）。通过与部署在已知位置的地面基础设施交互，这一方案能够证明无人机的身份标识及其广播的位置。我们的初步实验表明，该方案切实可行，且可使用超宽带收发器与部署在已知位置的地面基础设施交互，验证无人机的身份标识和位置。

关键词： 无人机 · 远程识别 · 位置证明 · 区块链 · 超宽带 · 无人机 · 无人航空系统

1 引言

无人驾驶航空器（无人机）正越来越多地应用于各种领域，从航空测绘到无人机配送服务 [5, 15, 17]。然而，将无人机纳入空域会带来重大挑战，尤其是如何保障其他空域使用者和公众的安全与安保 [10, 18, 29]。其中一个关键挑战是需要一个可靠且

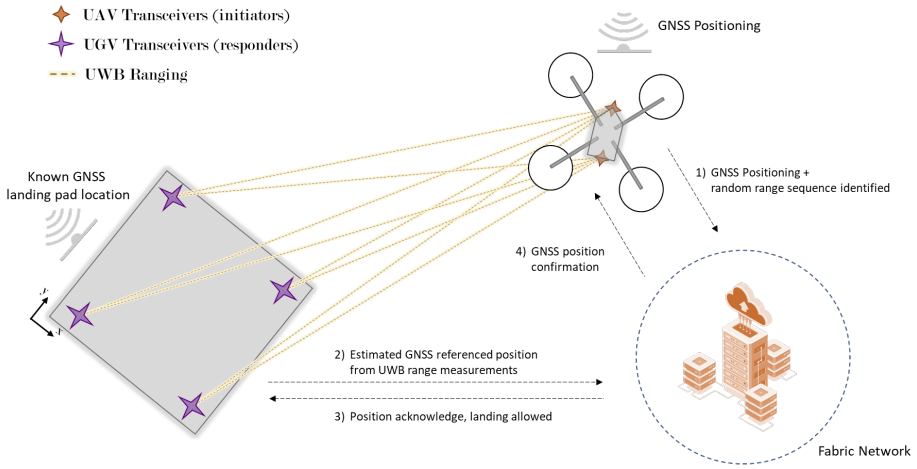

图 1：所提出的远程识别流程示意图。

可信的无人机位置证明系统。因此，直接远程识别应运而生，即在无法接触无人机的情况下，从远程位置识别无人机的过程 [4]。这是无人机监管和安全的重要方面，因为它使主管部门能够实时识别运营者和无人机，这对于确保遵守法规并防范潜在安全威胁至关重要 [11,25]。在欧洲，U-space 正在发展成为确保无人机安全、高效运行的监管框架，法规中更常采用标准术语 无人机系统（UAS）。U-space 涵盖多项措施，例如 UAS 注册、直接远程识别以及实时跟踪。同样在美国，美国联邦航空管理局（FAA）也已发布法规，要求无人机具备远程识别能力 [3]。

然而，全球导航卫星系统（GNSS）中的欺骗风险可能会对无人机的直接远程识别构成潜在问题 [6,14,24],；这种欺骗是指故意操纵信号以欺骗远程识别系统 [26]。至于位置证明（PoL），虽然它可用于验证无人机的位置，但并非始终安全。即使存在信任，也仍有发生错误或故意篡改位置数据的风险。例如，GNSS 信号可能受到干扰，或被伪造为包含错误的位置数据；此外，干扰等环境条件也可能影响位置数据的准确性。本章提出一种新颖的位置证明解决方案，用于为短距离无人机运行构建可信且安全的空地交互生态系统。该方案结合超宽带（UWB）技术与去中心化账本技术（DLT），例如 Hyperledger Fabric 区块链，以生成高度准确、可靠的无人机位置数据，并将其安全地存储在防篡改的去中心化区块链上，供验证使用。图 1 展示了这一概念。

本章其余内容安排如下。第 2 节介绍位置证明、UWB 技术和 Hyperledger Fabric 区块链框架领域的背景概念。第 3 节随后介绍无人机位置证明与远程识别领域的相关研究。

2 背景

本节将简要介绍基于超宽带的无人机位置证明方法及其背后的 Hyperledger Fabric 区块链关键技术。

位置证明 (PoL) 是一种技术，可将设备的物理位置坐标验证并广播到区块链网络 [2, 9, 27, 33]。它使其他设备无需信任广播设备，也能依赖这些位置数据。该技术使用密码学方法证明位置数据的真实性和准确性，从而使其成为安全、可靠的位置资讯来源。在无人机领域，位置证明可用于确保无人机配送和自主飞行等关键应用的责任落实与安全性。将位置证明与区块链身份相结合，可以更好地管理和监控无人机。这种整合能够提升安全性、可靠性和责任落实能力，确保无人机在执行着陆或起飞等关键操作时位于特定位置。此外，它在访问控制和安全机队管理方面也具有应用潜力。

超宽带 (UWB) 技术是实现位置证明（PoL）的精度最高的无线测距方案之一 [23, 28, 35]。UWB 利用射频信号高精度地确定设备的位置，并将加密数据和签名广播给其他节点，从而提供可靠的实时位置数据来源，并确保对无人机进行验证 [19] 。通过将数据分成较小的部分、加密、进行数字签名，然后将每部分作为单独的消息传输，可以提高位置数据的准确性和可信度。即使攻击者截获了其中一些部分，在无法获取全部部分的情况下，也无法利用这些信息，从而增添了一层安全保护。除位置证明外，UWB 技术还可应用于室内定位、资产追踪，甚至设备远程控制 [30]。其高精度和低功耗特性，使其成为众多物联网和无线通信应用的理想选择。文献中已提出基于 UWB 的空地协同和定位系统 [31]。

Hyperledger Fabric 是一个区块链平台，提供多种有利于分布式机器人系统的功能，包括用于参与者身份识别的安全身份管理和证书生成、用于增强数据安全性的许可型网络、支持实时机器人数据处理的高性能能力

、支持实时共识的低延迟交易确认，以及能够实现交易隐私和保密性的分区数据通道 [7,21]。此外，这些功能可以与 ROS 的发布/订阅系统集成，为分布式机器人系统提供可靠且可扩展的系统，使其成为无人机位置证明机制及类似应用的潜在选择；在这些场景中，安全数据交换和隐私保护至关重要。

在这一场景中，将超宽带（UWB）与 Hyperledger Fabric 等区块链技术相结合，可以成为无人机领域位置证明（PoL）机制的有效解决方案。正如我们在先前关于将空地机器人系统与 UWB 和 Hyperledger Fabric 相结合的论文中所展示的，UWB 能够提供实时位置信息，并且借助最新标准，还能以高精度和低延迟实现加密数据传输；与此同时，区块链充当安全账本，用于存储和验证位置信息的真实性 [20]。这种组合使其成为提高无人机位置准确性的潜在解决方案，并可广泛应用于配送、物流和《航空航天》等行业。通过利用这些技术，位置证明（PoL）可以得到扩展，从而提高基于位置的应用的效率、安全性和透明度。

3 相关工作

位置证明（PoL）的概念已在多项研究中被提出，用于验证用户位置。最初，Brent Waters 和 Felten Edward 在集中式环境中提出了位置证明（PoL）的概念：可信位置管理器根据与证明者之间的往返通信测量值对证明进行签名 [27]。位置证明的概念最早由 Brent Waters 和 FeltenEdward 在集中式环境中提出，在该环境中，可信位置管理器根据与证明者之间的往返通信测量值对证明进行签名。最近，研究人员提出了生成位置证明（PoL）的新方法，以确保无人机以及物联网（IoT）这一更广泛领域中的其他移动资产的位置。

例如，Khan 等人提出了面向见证者的背书概念，以及一种用于生成声明式位置证明并识别非联邦环境中可能出现的漏洞的抗串谋协议 [12]。在另一项研究中，Chitra 等人提出了一种生成和验证安全位置证明的新协议 [9]。该协议采用信息论安全的模糊保险库方案和独特的时空无线信道特性，并提供密码学安全性。较近期的一项研究中，Amoretti 等人结合分布式账本技术，在 2018 [2] 中提出了一种新颖的基于区块链的位置证明方法。该方法采用去中心化的点对点方案生成数字证书，以证明某一特定时间在某个地理位置的存在，同时确保位置的可信度和用户隐私。

近年来，除了上述方法外，人们也越来越关注无人机远程识别系统的开发，以此提升

空域的安全性与安保水平。人们提出了多种方法，包括射频识别和其他基于传感器的方法。在无人机远程检测与识别方面，Mohammad 等人在 [1]开发了一个综合数据库，其中包含无人机在不同飞行模式下发射的射频信号。基于该数据库，人们提出了新型算法，用于检测和识别无人机，并确定其类型和飞行模式。

关于用于无人机远程识别的区块链集成， [8] 的作者介绍了一种新的无人机远程识别协议（DRIP），该协议基于 Hyperledger Iroha 框架，用于安全地识别无人机。这项工作的主要思路是注册新无人机，将其身份标识存储到区块链网络中，并通过公钥和证书验证收到的数据。然而，该系统只处理身份识别，并未考虑位置证明。因此，现有文献在无人机远程直接识别与位置证明方面仍有不足。

4 提出的系统架构

我们提出将超宽带测距集成到无人机远程标识中，以便在无人机与基础设施（例如位于已知地点的起降坪）交互时实现位置证明。无人机和基础设施都必须属于同一个 Fabric 区块链。

在此场景中，无人机可以通过超宽带将其身份证书发送至地面系统，随后地面系统可利用区块链技术验证证书的真实性。地面系统能够访问区块链账本，以确认无人机符合必要要求，例如已获得适当授权，或维护检查处于最新状态。

这一流程有望显著提升无人机着陆系统的安全性和效率，因为它能够实时验证无人机的身份标识和状态。区块链的去中心化和安全特性还可以防止身份证书遭到未授权访问或篡改，确保只有经过授权的无人机才能着陆。

具体的软件实现方面，设想中的系统架构如图 2 所示。本章仅实际实现了该系统的一部分。不过，我们设想的系统架构包含云端后端系统、无人航空器系统和地面基础设施（例如着陆垫）等关键组件，其中地面基础设施充当连接云端的边缘网关。在这一架构中，我们展示了如何利用基于超宽带的情境通信实现远程识别和位置证明，并协助着陆过程，从而提高定位精度。此外，这种交互还可扩展到获取停靠许可或起飞许可等用途。在云端，我们认为 Zenoh 是此类分布式系统中最有前景的技术之一；近期研究表明，它能够支持高性能、可扩展的通信与计算 [13,32]。在机队管理和接口方面，除了 Hyperledger Fabric 之外，一个适配无人机的 Open-RMF 版本

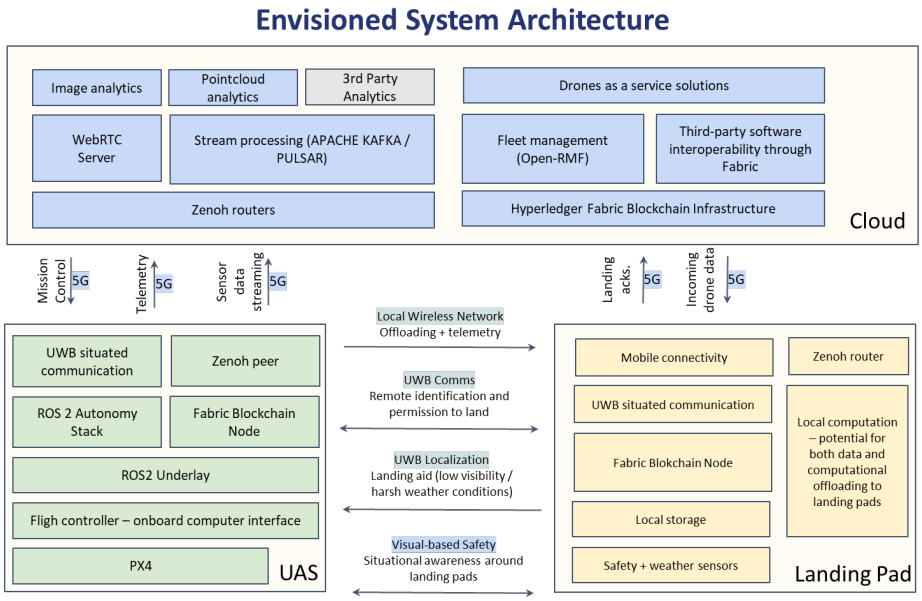

图 2：构想中的系统软件架构。

也有望成为解决这一问题的开源方案 [22, 34]。

我们提出的位置证明流程如图 3 所示，具体运行方式如下：

1. 无人机将带时间戳的通知作为 Fabric 区块链交易发布，并为无人机和地面平台生成唯一标识码，用于测距和验证。随后，无人机启动位置证明流程。2. 地面平台通过区块链接收请求，并通过超宽带向附近潜在的接收器发送轮询消息，其中包含收到的无人机 ID 和平台 ID。3. 无人机收到消息后，将区块链中的唯一 ID 进行比对。如果身份标识匹配，无人机便回复地面平台的轮询消息。4. 平台接收来自超宽带轮询消息的回复。5. 平台的超宽带节点启动与无人机的双向测距。此外，还会发送其加密身份标识。6. 无人机接收部分加密信息，用于平台识别。如果身份标识匹配，无人机便通过超宽带回复轮询消息。7. 平台能够计算与无人机之间的距离，以进行定位。智能合约将 GPS 位置数据与超宽带位置数据进行比较。如果二者匹配，智能合约便发送消息，以证明无人机位置并验证其交互授权，例如着陆。

8. 如果无人机获得授权，便允许其着陆。

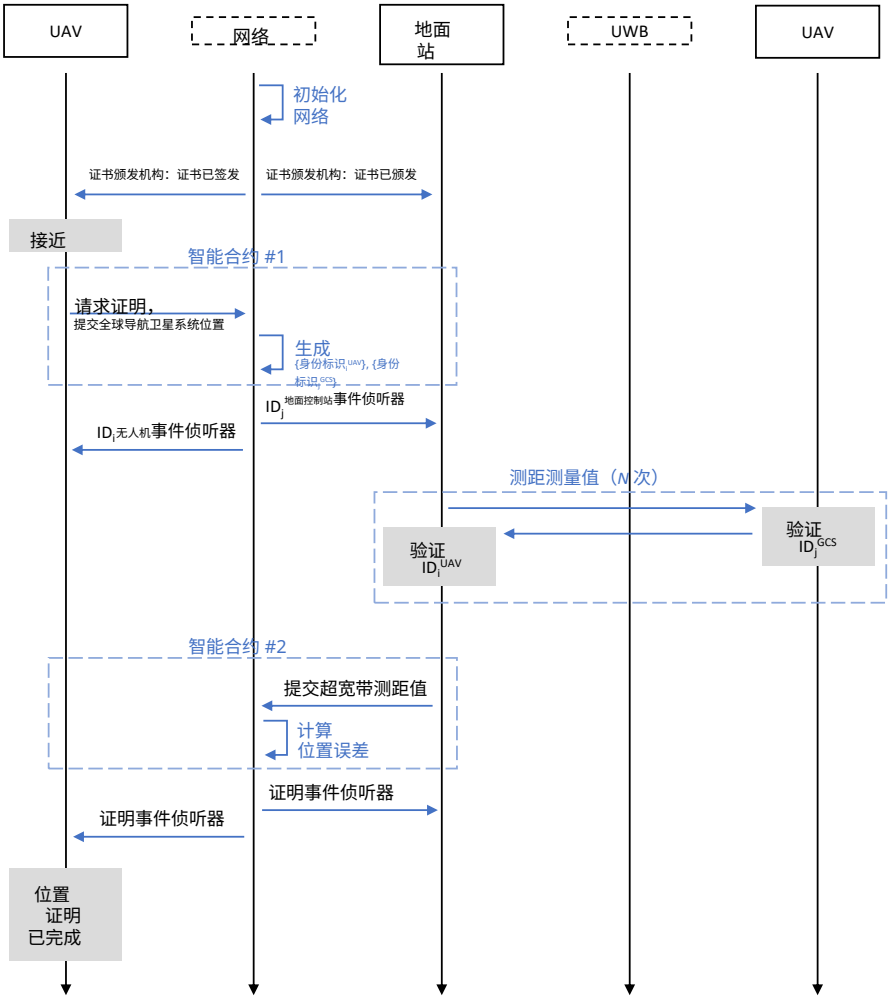

图3：定位证明流程示意图。纵轴表示时间（自上而下流动）。图中两侧均显示无人机，以区分无人机与地面平台（地面控制站）之间通过网络（Fabric列）或超宽带无线电（超宽带列）进行的通信。

5 方法与实验

为证明所提出方法的可行性，我们开展了概念验证演示，重点实现基于超宽带的定位证明方法与 Hyperledger Fabric 的结合。该方法可增强安全性、可靠性和问责性，确保无人机在执行关键操作期间位于指定位置。

5.1 超宽带测距

用于定位的超宽带可通过不同的测距模式实现，我们采用的是飞行时间。该模式通过测量一对超宽带设备之间交换消息所需的时间来获取它们之间的距离，再对不同设备对测得的距离进行三角测量以确定位置 [16]。在去中心化系统中，计算距离至少需要两条消息，确定位置至少需要四个节点。利用超宽带定位需要交换消息这一特点，我们还利用这些消息交换无人机与地面平台的唯一标识码，以进行身份验证。Hyperledger Fabric 中的事件触发并生成代码后，平台端的超宽带设备会将自身代码嵌入用于飞行时间测距的一条消息中，发送给无人机端的超宽带设备。如果无人机收到的代码与从网络获得的代码匹配，无人机端的超宽带设备便会返回自身代码，供平台验证。这样，无人机端和平台端都能完成验证，同时也能交换相对定位所需的消息。随后，系统可比对 GPS 位置，并验证无人机计算出的位置是否匹配，以决定是否授权交互。

5.2 Hyperledger Fabric网络

Hyperledger Fabric网络充当安全的数据传输层，用于连接不同的 ROS 子系统。我们采用了近期提出的事件驱动架构，该架构利用 ROS-Fabric应用程序处理来自 ROS 和 Fabric 网络的回调 [7]。每当有新消息发布到特定主题时，就会生成一个 ROS事件。根据桥接应用程序的指定配置，这些消息随后可以作为交易转发至 Fabric网络，其中可能涉及创建或修改位于不同通道链码中的资产。Fabric 通道事件由区块链上新交易的确认触发，是系统事件驱动架构的重要组成部分。在我们的案例中，无人机和着陆垫均作为 Fabric网络中的一个主机，相关请求则以事件的形式在区块链中传输。

5.3 位置证明

我们为实验设置实现了一个链码（智能合约）和两个 Fabric 应用程序。该智能合约采用简单的数据结构，

可支持任意 ROS 消息类型和基本功能，包括资产的创建、编辑、查询和删除。核心思路是通过交易类型和载荷注册通道事件，使 Fabric 应用程序无需预先了解其结构或方法即可监听通道事件。这两个应用程序专为给定系统的 Hyperledger Fabric 网络与 ROS 计算图之间的交互而设计。为管理资产，每台主机都配备两个应用程序，分别称为 *Fabric 发布者* 和 *Fabric 订阅者*，前者负责将数据从 ROS 传输到 Fabric，后者则执行反向操作。在本例中，无人机通过发起一条带时间戳的通知（作为 Fabric 区块链交易），并为无人机和着陆平台分别生成唯一代码，启动整个流程。随后，平台接收请求，并向附近的潜在接收器发送包含身份标识的轮询消息。如果身份标识匹配，无人机便通过超宽带响应轮询消息，使平台能够在智能合约中计算无人机的距离以进行定位。如果位置数据匹配，平台便通过区块链发送消息，以验证着陆授权和位置证明。

5.4 实验设置

当前实现依赖 PX4 飞行控制栈，以及一台通过机器人操作系统（ROS）运行我们自主飞行栈的伴随计算机。超宽带测距采用 Decawave DWM1001 收发器和定制固件实现。无人机采用 TDrone M690B 机架组装，飞行时间超过 50 分钟，载荷为 2 千克。

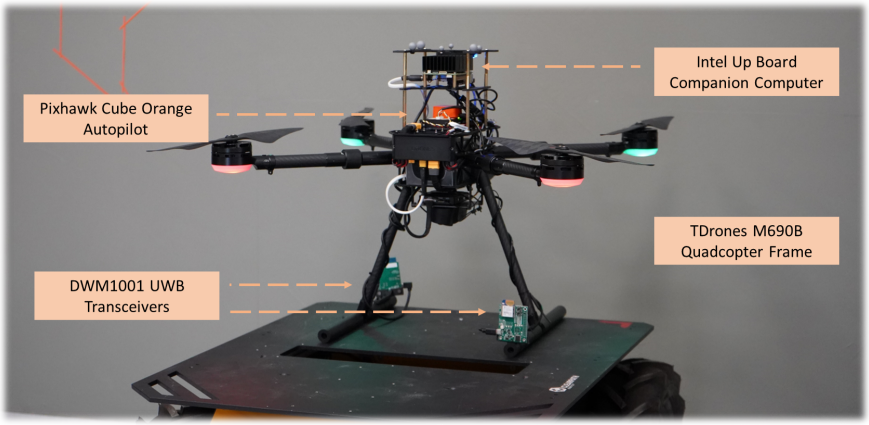

图 4：我们实验中使用的无人机和超宽带传感器示意图。

硬件。 Fabric网络由两台不同的计算机组成，分别用于无人机和着陆平台，硬件配置各不相同。正如我们此前的研究所示，运行 Fabric 网络的计算负载几乎可以忽略不计 [7, 21]。两台主机分别配备 Intel i7-9750H 和 Intel i3-1215U 处理器，内存分别为 64GB 和 16GB。我们使用配备定制固件的 DWM1001 超宽带节点。目前实验中仅使用一个超宽带节点。平台配备了四个超宽带节点，以获取更精确的无人机位置数据。

软件。 Fabric 应用程序采用 NodeJS 实现，链码则使用 Golang 编写。无人机和着陆平台均在 Ubuntu 20.04 上运行 ROS Noetic。随后在每台主机上部署两个 Fabric 应用程序，以连接 ROS 系统。超宽带节点经过编程，用于验证身份标识并定位无人机。

位置数据。 我们使用一套配备 16 台 Optitrack 摄像机的外部动作捕捉（MOCAP）系统，确定无人机和着陆平台的精确位置数据，并将其用作地面真实值参考系统。

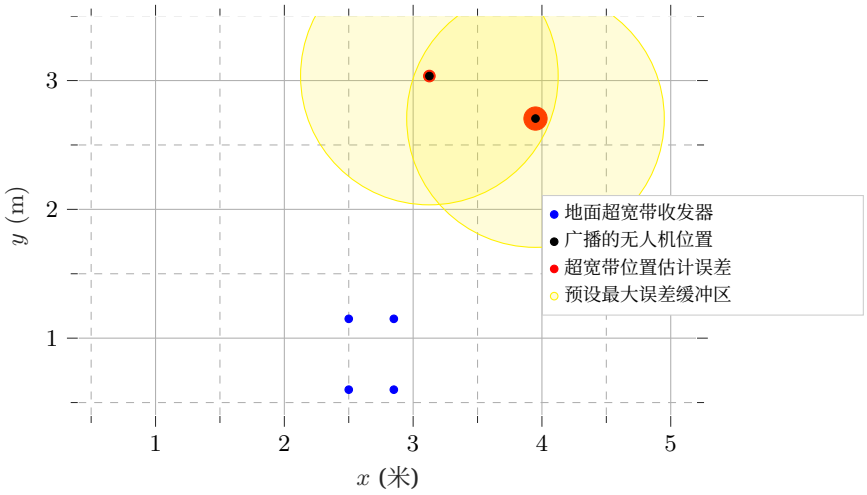

图 5：无人机移动时，在短距离内使用两种不同测量值进行远程识别的首次实验。安全的短距离定位有助于精确着陆系统。

5.5 实验结果

本小节报告了基于上述实现的概念验证实验结果。为验证位置证明系统，

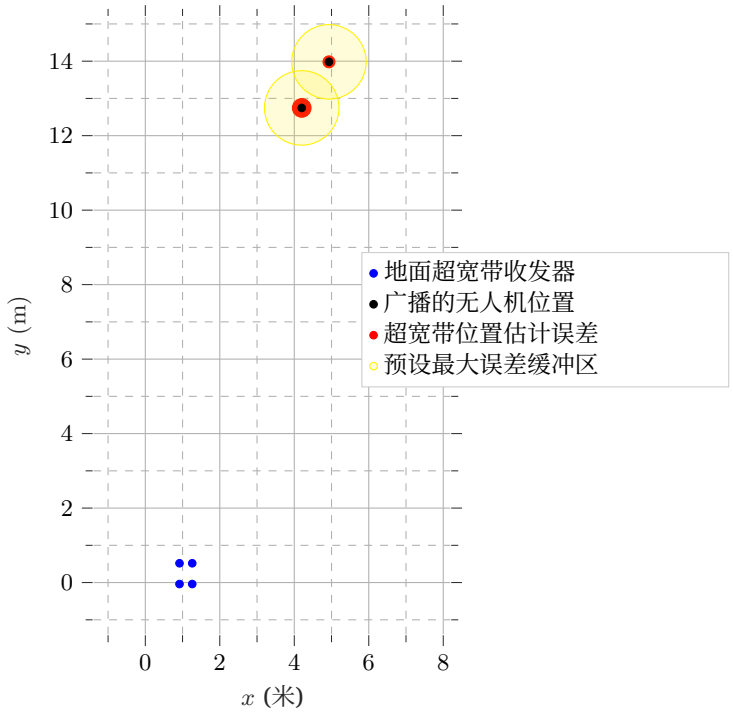

图 6：无人机移动时，在较远距离下使用两种不同测量值进行远程识别的第二次实验。

我们进行了短距离和长距离实验。图 5 展示了地面站中的超宽带收发器（位置固定且已知）以及无人机（待验证位置）的位置。这些位置由动作捕捉系统获取，用于模拟实际室外飞行中的全球导航卫星系统位置。为了验证无人机通过 Fabric 区块链中的智能合约提供的位置，我们预先设定了一个最大误差缓冲区，其半径为 1 米，并在图中以黄色显示。

图 5 和图 6 的结果均表明，无人机的位置在四种不同情况下都得到了有效验证。虽然在较大距离实验中，根据超宽带测量值估算的位置误差更接近预先设定的最大误差缓冲区，但我们认为，1 米的缓冲区相当保守，因为单星座接收机的全球导航卫星系统误差很容易达到数米，尤其是在城市区域。无论如何，位置证明智能合约的输出可以调整为直接表示误差本身，或表示无人机实际处于其所声称位置的可能性。

6 结论与未来工作

我们提出了一种新方法，通过与地面站进行定位通信，证明空中机器人或自主航空系统的位置。本文提出的方法依托 UWB 测距测量和 Hyperledger Fabric 区块链网络，在已知固定地面基础设施位置的前提下，验证与其通信的无人机的身份标识和位置。通过概念验证实现，我们展示了该方案的可行性，并提供了此类系统所需的 Fabric 智能合约和应用程序示例。实验还表明，基于UWB-Fabric的位置证明可实时执行，并具有可扩展性潜力。

未来的工作中，我们将把所提出的解决方案与 ROS 2 和 PX4自动驾驶仪项目集成，以提供一种更通用、开箱即用的解决方案。

致谢

本研究得到芬兰科学院 AeroPolis项目（资助编号：348480、348481）以及由安全系统研究中心（SSRC）、技术创新研究院（TII）资助的 R3Swarms项目的支持。

参考文献

1. Al-Sa'd, M.F., Al-Ali, A., Mohamed, A., Khattab, T., Erbad, A.: 基于射频的无人机探测与识别：采用深度学习方法，推动建立大型开放式无人机数据库。《未来一代计算机系统》**100**, 86–97 (2019) 2. Amoretti, M., Brambilla, G., Medioli, F., Zanichelli, F.: 基于区块链的位置证明。载于：2018 IEEE软件质量、可靠性与安全国际会议伴会（QRS-C）。第146–153页。IEEE（2018）3. Batuwangala, E., Silva, J., Wild, G.: 适航组织安全管理系统监管框架。《航空航天》**5**(4), 117 (2018) 4. Belwafi, K., Alkadi, R., Alameri, S.A., Al Hamadi, H., Shoufan, A.: 无人驾驶航空器的远程识别：教程与综述。《IEEE Access》**10**, 87577–87601 (2022) 5. Bithas, P.S., Michailidis, E.T., Nomikos, N., Vouyioukas, D., Kanatas, A.G.: 基于无人机的通信中机器学习技术综述。《传感器》**19**(23), 5170 (2019) 6. Chamola, V., Kotesh, P., Agarwal, A., Gupta, N., Guizani, M., et al.: 无人驾驶飞行器攻击及其消除技术综合综述。《自组网络》**111**, 102324 (2021) 7. Fu, L., Salimi, S., Pe¯na Queralta, J., Westerlund, T.: 事件驱动的Fabric区块链与ROS 2接口：迈向移动机器人的安全、可审计远程操作。arXiv（2023）

8. Hashem, Y., Zildzic, E., Gurtov, A.: 基于Hyperledger Iroha的安全无人机识别。载于：第11届ACM智能车联网设计与分析研讨会论文集。第11–18页（2021）9. Javali, C., Revadigar, G., Rasmussen, K.B., Hu, W., Jha, S.: 我是Alice，我曾身处仙境：安全位置证明生成与验证协议。载于：2016年IEEE第41届本地计算机网络会议（LCN）。第477–485页。IEEE（2016）10. Kakaletsis, E., Symeonidis, C., Tzelepi, M., Mademlis, I., Tefas, A., Nikolaidis, N., Pitas, I.: 自主无人机飞行安全的计算机视觉：概述及基于视觉的安全着陆流程示例。ACM计算调查（CSUR）**54**(9), 1–37 (2021) 11. Khan, M.A., Menouar, H., Eldeeb, A., Abu-Dayya, A., Salim, F.D.: 未经授权的无人机探测：技术与未来展望综述。《IEEE传感器期刊》（2022）12. Khan, R., Zawoad, S., Haque, M.M., Hasan, R.: “谁、何时、何地？”移动设备的位置证明声明。载于：数据与应用安全和隐私第28届会议：第28届IFIP WG 11.3工作会议，DBSec 2014，奥地利维也纳，2014年7月14–16日。论文集28。第146–162页。施普林格（2014）13. Liang, W.Y., Yuan, Y., Lin, H.J.: Zenoh、MQTT、Kafka与DDS的吞吐量和延迟性能研究。arXiv预印本 arXiv:2303.09419（2023）14. Meng, L., Yang, L., Yang, W., Zhang, L.: 全球导航卫星系统欺骗与反欺骗技术综述。《遥感》**14**(19), 4826 (2022) 15. Mohsan, S.A.H., Khan, M.A., Noor, F., Ullah, I., Alsharif, M.H.: 无人驾驶航空器（UAV）：综合综述。《无人机》**6**(6), 147 (2022) 16. Mor´on, P.T., Queralta, J.P., Westerlund, T.: 面向动态超宽带角色分配的多机器人系统大规模相对定位。载于：2022年第7届国际机器人与自动化工程会议（ICRAE）。第239–246页（2022）。https://doi.org/10.1109/ICRAE.2022.10054614 17. Osco, L.P., Junior, J.M., Ramos, A.P.M., de Castro Jorge, L.A., Fatholahi, S.N., de Andrade Silva, J., Matsubara, E.T., Pistori, H., Gon˙calves, W.N., Li, J.: 无人机遥感中的深度学习综述。《国际应用地球观测与地理信息学杂志》**102**, 102456 (2021) 18. Outay, F., Mengash, H.A., Adnan, M.: 无人机在道路安全、交通和公路基础设施管理中的应用：最新进展与挑战。《交通研究A辑：政策与实践》**141**, 116–129 (2020) 19. Pe˜na Queralta, J., Qingqing, L., Schiano, F., Westerlund, T.: 基于视觉惯性里程计与超宽带的协同定位及异构多机器人系统中的稠密场景重建。载于：IEEE先进机器人与机电一体化国际会议。IEEE（2022）20. Salimi, S., Mor´on, P.T., Pe˜na Queralta, J., Westerlund, T.: 基于Hyperledger Fabric区块链的安全异构多机器人协作与对接。载于：IEEE第8届物联网世界论坛。IEEE（2022）21. Salimi, S., Pe˜na Queralta, J., Westerlund, T.: 面向自主移动机器人的Hyperledger Fabric区块链与ROS 2集成。载于：IEEE/SICE SII。IEEE（2023）22. Sim, S.W., Kwan, B.H., Yap, W.S., Ng, D.W.K.: 工厂类环境中基于ROS 2的自动导引车多机器人仿真开发。电子信息通信学会论文集系列**69**(SS2-5)（2022）23. Singh, M., Leu, P., Abdou, A., Capkun, S.: 超宽带距离扩大型攻击检测。《IACR密码学电子印刷档案》**2019**, 1349 (2019)

24. Sorbelli, F.B., Conti, M., Pinotti, C.M., Rigoni, G.：无人机路径偏离攻击：综述与研究挑战。载于：2020年IEEE传感、通信与网络国际会议（SECON研讨会）。第1–6页。IEEE（2020）25. St¨ocker, C., Bennett, R., Nex, F., Gerke, M., Zevenbergen, J.：无人机法规现状综述。《遥感》**9**(5), 459（2017）26. Tang, A.C.：城市空中交通网络安全漏洞综述。载于：AIAA SciTech 2021论坛。第0773页（2021）27. Waters, B., Felten, E.：安全、私密的位置证明。计算机科学系，普林斯顿大学，技术报告 TR-667-03（2003）28. Wilson, R., Tse, D., Scholtz, R.A.：信道识别：利用超宽带信道中的互易性进行秘密共享。《IEEE信息取证与安全汇刊》**2**(3), 364–375（2007）29. Xiangmin, G., Renli, L., Hongxia, S., Jun, C.：民用无人航空系统在一体化国家空域系统运行时的安全间隔管理与避碰方法综述。《中国航空学报》**33**(11), 2851–2863（2020）30. Xianjia, Y., Qingqing, L., Pe˜na Queralta, J., Heikkonen, J., Westerlund, T.：超宽带网络与定位在自主机器人和工业系统中的应用。载于：信息物理系统之系统（CPSoS）与物联网（IoT）会议。IEEE（2021）31. Xianjia, Y., Qingqing, L., Pe˜na Queralta, J., Heikkonen, J., Westerlund, T.：地面机器人辅助的、基于超宽带的无人机室外定位与导航协同定位。载于：IEEE自主系统国际会议（IEEE ICAS 2021）。IEEE（2021）32. Yu, X., Mor´on, P.T., Salimpour, S., Pe˜na Queralta, J., Westerlund, T.：用于相对蒙特卡罗多机器人定位的松耦合里程计、超宽带测距与协同空间检测。arXiv（2023）33. Zafar, F., Khan, A., Anjum, A., Maple, C., Shah, M.A.：面向智能物联网的位置证明系统：需求、分类体系与比较分析。《电子学》**9**(11), 1776（2020）34. Zhang, J., Keramat, F., Yu, X., Hern´andez, D.M., Pe˜na Queralta, J., Westerlund, T.：边缘云连续体中的分布式机器人系统与 ROS 2：新型架构及技术成熟度综述。载于：2022年第七届雾计算与移动边缘计算国际会议（FMEC）。第1–8页。IEEE（2022）35. Zhang, Y., Liu, W., Fang, Y., Wu, D.：超宽带传感器网络中的安全定位与身份验证。《IEEE通信选刊》**24**(4), 829–835（2006）