无人机自组网的密钥协商技术综述

张仕明[1] 马舒凡[1] 缪炜星[1] 祝 涛[1]
ZHANG Shiming MA Shufan MIAO Weixing ZHU Tao

摘 要 无人机广泛应用于农业、地质、救援、战争等诸多领域。其中，无人机自组网在任务执行能力、通信能力、抗干扰与抗摧毁能力以及智能化程度等方面相较于单一无人机具有显著优势，因此在许多复杂和需要高度协同的任务中表现出色。然而，无人机通常依赖于安全性较低的无线信道完成相互通信，这使得无人机自组网面临多种安全威胁。为了应对这些威胁，密钥协商技术被用来确保无人机之间建立安全加密的会话信道。首先，指出无人机自组网中密钥协商技术所面临的问题；其次，介绍该技术底层所使用的密码学算法；然后，通过文献分析基于群组密钥和基于对密钥的无人机身份认证与密钥协商研究现状，归纳各种方案的应用场景及其优缺点；最后，对无人机自组网中的密钥协商技术进行总结与展望。

关键词 无人机；密码学；密钥协商；安全通信

doi：10.3969/j.issn.1672-9528.2024.08.048

0 引言

无人机具有覆盖范围广和感知能力强等显著特点，这使它们在军事侦察和灾害监测等应用中备受青睐。相对于多无人机而言，单一无人机具有简单易用、成本低廉以及灵活性等优点。然而，其覆盖范围有限，容易受单点故障影响，且在大范围任务中效率较低。相比之下，多无人机可以实现更广泛的覆盖，提高任务效率，但需要更复杂的协调和管理方式。多无人机组成的网络系统即无人机自组网，主要由地面控制站和资源有限的无人机组成，具有无线多跳路由、节点高速移动性、网络拓扑结构高动态变化性、节点网络结构的异构性、非集中和自组织性、抗毁伤及抗干扰以及智能性强等特性。

无人机自组网中常见的通信场景主要包括无人机与地面控制站之间的通信，以及无人机与无人机之间的通信。本文主要关注无人机与无人机之间的通信。然而，无人机之间的通信存在着许多潜在安全问题亟待解决。首先，无人机自组网可能用于传输敏感信息，如军事情报、安全监测数据等，而无人机之间使用的通信链路是公开的。恶意攻击者可以监听无人机之间的通信内容。因此，保障通信安全可以防止这些信息被未授权的人员获取，保护国家利益和个人隐私；其次，在网络通信过程中，数据可能会受到篡改或修改，导致信息的准确性和完整性受到损害。通过加密和身份认证等技术保障通信的完整性，可以防止数据被篡改；最后，无人机自组织网络可能面临各种网络攻击，如拒绝服务攻击、中间人攻击等。通过安全通信机制，可以提高网络的抵御能力，保障网络稳定运行。总体而言，在缺乏足够的安全和隐私保护的情况下，恶意攻击者可以修改、删除、重放、监控和窃听交换的无人机信息[1]，为了确保无人机自组网的通信安全与数据隐私，无人机自组网需要相应的身份认证、密钥协商等协议。

目前，许多关于物联网密钥协商综述都集中在无线传感器网络和车辆自组网领域，而涉及无人机自组网的研究综述较少。无人机具有移动性和动态性，其通信环境特殊，具有如高速移动、无线信号干扰等特点，传统的密钥协商方案可能无法直接适用于无人机自组网。因此，本文将调研最近的一些密钥协商方案，重点介绍密钥协商在无人机自组网的应用，对于保障无人机自组网的安全通信具有重要意义。

1 基础密码学算法

认证密钥协商协议（authenticated key agreement，AKA）在构建网络安全协议中占据核心地位。AKA 不仅能实现双方的身份验证，还能生成共享的会话密钥。为实现这一目标，它通常结合数字签名算法以确保身份的真实性，并利用密钥交换协议来建立共享的密钥。在本节中，将概述在设计 AKA 时所涉及的密码学基本原理，包括但不限于对称与非对称加

1. 中航（成都）无人机系统股份有限公司 四川成都 611743
[基金项目] 工业和信息化部制造业高质量发展专项资助（TC220A04X-2）

密算法、数字签名技术、Diffie-Hellman 密钥协商协议等。

（1）对称密钥加密算法也称为共享密钥加密算法。在此机制下，发送者与接收者持有同一把密钥，这把密钥同时参与加密与解密的过程。这种加密算法具有自认证的特性，即密钥本身就能证明其有效性，但必须通过安全通信进行共享。对称密钥加密算法在计算资源有限的环境下仍能实现高效的加密和解密运算，因此在实际应用中得到了广泛的推广和使用。

（2）非对称密码也被称为公钥密码算法，其特点在于加密密钥与解密密钥是相互独立的。在此类算法中，每个参与运算的实体均会生成并持有一对密钥，即公钥与私钥。公钥是可以自由公开的，其公开并不会对私钥的安全性构成威胁。发送方可利用接收方的公钥对数据进行加密；而私钥则需由接收方严格保密，并专门用于解密通过公钥加密的消息。

（3）椭圆曲线密码算法是公钥密码体系中的一种。公钥密码体系的安全性，是以其背后的计算复杂性难题为支撑的。当这些难题的解答难度增加时，为达到相同安全级别，所需要的密钥长度会相应减少。椭圆曲线密码算法的安全性建立在椭圆曲线离散对数问题的复杂性之上，而此问题的求解极具挑战性。因此，相较于其他算法，椭圆曲线密码算法在实现同等安全性时，所需的密钥长度要短得多。此外，该算法运算效率更高、能耗更低，特别适用于资源有限且对实时性要求严苛的网络环境，因为它能大幅降低资源消耗并提升处理速度。

（4）数字签名技术涵盖了两个核心算法：签名生成算法与签名验证算法。利用发送者的私钥，可以通过签名生成算法得出对应的数字签名；而接收者则可以利用签名验证算法，结合发送者的公钥，来核实数字签名的有效性。数字签名算法在身份确认方案中扮演着至关重要的角色。在公钥密码体系中，某个实体的数字签名可以证实其公钥的真实性。然而，要确认签名者的身份，还需通过证书认证，或者采用预先共享签名者公钥的方法来实现。

（5）Diffie-Hellman 密钥协商协议基于离散对数问题的数学难题，这使得它在目前已知的计算能力下具有很高的安全性。协议的核心思想是通过两个通信方各自生成部分秘密信息，并通过交换信息来计算出共享的秘密密钥。协议具体步骤如下。

步骤 1：公共参数选择：选择一个大素数 p 和一个生成元 g。

步骤 2：密钥生成：假设参与双方为 Alice 和 Bob，Alice 生成一个私钥 a，Bob 生成一个私钥 b。

步骤 3：公共值计算和交换：Alice 根据私钥 a 计算出公共值 $A = g^a \bmod p$，Bob 根据私钥 b 计算出公共值 $B = g^b \bmod p$。Alice 将 A 发送给 Bob，Bob 将 B 发送给 Alice。

步骤 4：共享密钥计算：Alice 使用 Bob 发送的 B 计算共享密钥 $s = B^a \bmod p$，Bob 使用 Alice 发送的 A 计算共享密钥 $s = A^b \bmod p$，至此，双方协商出共享密钥 $s = g^{ab} \bmod p$。

2 无人机自组网模型和威胁模型

无人机网络采用无线通信网络作为数据传输手段，其通信链路具有开放性和不稳定性。在无人机网络中，主要包含两类实体：一类是资源有限、能源受限的无人机节点，另一类是计算能力较强的地面控制站节点，具体如图 1 所示。

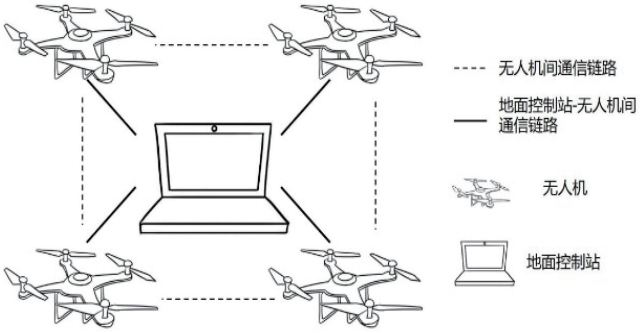

图 1 无人机网络拓扑示意图

构建通信安全防护方案的首要步骤是设计相应的威胁模型。无人机网络作为一种特殊的无线网络形式，其信道的脆弱性带来了多重安全风险。针对安全性较低的无线网络进行威胁模型设计时，Dolev 等人 [2] 提出了一个经典的无线网络威胁模型，该模型假设对手具有极强的能力。在这个威胁模型下，无人机网络可能会面临以下几种类型的攻击。

（1）假冒攻击：攻击者通过使用伪造的身份凭证，冒充系统中的其他成员，意图窃取私密信息。

（2）去同步攻击：在用户和无人机更新其内部存储数据时，可能会受到网络延迟或波动等不可预测因素的影响，从而导致服务器中的数据与其他实体内部存储的信息产生不匹配的现象。攻击手会尝试利用这种信息不匹配的机会来攻击无人机网络系统，通过向服务端提交过时的认证信息，实现对系统的成功攻击。

（3）内部攻击：内部攻击者指的是那些怀有恶意攻击意图并享有内部特权的实体。在本协议框架下，这类攻击者有能力操纵受害用户的智能终端，借助用户的合法身份去控制目标无人机，以实现其攻击意图。

（4）中间人攻击：攻击者在用户和无人机之间分别建立独立的会话，并中转双方接收到的数据。这给用户和无人

机造成一种错觉，即他们正在通过安全的私密通道进行直接通信，然而整个通信会话实际上完全处于攻击者的掌控之下。

（5）物理攻击：与单纯的无人机设备丢失攻击不同，攻击者在获取无人机后，有能力对其内存进行修改和复制。他们可以利用被篡改的内存数据来误导用户，或者通过复制无人机的内存信息来伪装或复制无人机，从而破坏无人机网络系统的完整性和安全性。

3 基于群组密钥的无人机密钥协商研究

在无人机之间，通过公开信道进行两两通信存在诸多安全隐患。例如，恶意攻击者可以监听公开信道，窃取通信数据，甚至利用信息重放、篡改或伪造等手段冒充合法的无人机。为了应对上述挑战，群组密钥是一种用于保障群组通信安全的加密密钥。在网络通信中，群组密钥被用来加密和解密无人机之间的通信内容，确保只有授权的无人机才能访问和解密通信内容，从而保障通信的机密性和安全性。使用群组密钥可以简化无人机自组网通信的管理和操作，提高通信的效率和安全性，因为只需要管理和维护一个密钥，即可保障整个无人机自组网的通信安全。无人机自组网协同工作时需要一个群组密钥保证集群的通信安全，但缺点是当无人机自组网规模变化时，难以动态更改群组密钥。此外，无人机通常被认为是资源有限的移动设备，需要保证无人机通信的安全，并尽可能减少无人机侧的计算开销和通信成本。

最近，许多研究者针对基于无人机网络的无人机应用场景，提出了许多轻量级认证密钥协商方案。例如，Wazid 等人[3]设计了一种适用于无人机网络环境的三因素安全和高效的认证密钥协商方案。在该方案中，用户可以直接从无人机访问数据，前提是用户被授权访问该无人机的数据。然而，该方案并不能保证身份信息的独立性和后向安全。针对这些缺陷，Srinivas 等人[4]设计了一个无人机网络环境下基于时间凭据的匿名轻量级三因素认证密钥协商方案，然而该方案很容易受到身份检验器被盗攻击和假冒攻击，而且也不能提供用户身份的可追溯性。Ali 等人[5]提出了一种基于无人机网络的智能城市环境的增强认证密钥协商方案，解决 Srinivas 等人所提方案的安全漏洞。但是，该方案在伪造、会话密钥泄露和服务器欺诈攻击方面仍然很脆弱。由于无人机自组网固有的不稳定性和动态拓扑结构，Won 等人[6]提出了用于中型空中无人机的基于无证书签名加密的协议。该协议通过消除证书来减少通信开销，但需要多次求幂，因此会带来巨大的开销，这对于资源有限的小型无人机来说可能不实用。Tanveer 等人[7]利用用户密码、移动设备和生物识别信息的三因素安全方案设计了一种新颖的无人机环境互联网轻量级认证密钥协商协议，但该方案无法提供匿名性和容易受到去同步攻击。Semal 等人[8]提出了一种使用无证书组认证密钥协议（CL-GAKA）方案来解决不信任方之间的安全通信问题，其目的是实现无人机与无人机通信的保密性、信息完整性和真实性，这为不受信任的无人机网络提供了可信通信，将为进一步的研究和应用提供基础。施荣华等人[9]提出了一种密钥管理方案。该方案基于分层思想，通过群密钥对数据双重加密以及在节点之间进行密钥交换提高通信的安全性，并且针对网络拓扑结构变化带来的群结构维护复杂的问题进行讨论，然后给出解决方案。不足的是，节点加入和退出网络造成的开销较大。本文将基于群组密钥的密钥协商方案进行了总结性对比，如表 1 所示。

表 1 基于群组密钥的无人机认证密钥协商方案总结对比

方案	密码原语	描述	缺陷
Wazid 等人	模糊提取 Hash 运算	基于无人机网络的轻量双向认证协议	无后向安全 无匿名性
Srinivas 等人	模糊提取 Hash 运算	无人机网络环境下基于时间凭证的轻量级认证协议	无法抵抗身份检验器被盗攻击 无法抵抗假冒攻击
Ali 等人	对称加密 Hash 运算	基于无人机网络的轻量级双向认证协议	无法抵抗伪造攻击 无法抵抗欺骗攻击
Tanveer 等人	对称加密 Hash 运算	利用用户密码、移动设备和生物识别信息的三因素安全方案	无匿名性 无法抵抗去同步攻击
Semal 等人	双线性对加密	用于不可信无人机网络中安全通信的无证书组认证密钥协商协议	高计算成本

4 基于对密钥的无人机密钥协商研究

对密钥方案是一种仅在通信双方之间协商密钥的方案。这种方案相比组密钥方案来说，没有组网规模变化带来的密钥更新问题。对密钥方案最常采用的实现方法是使用非对称密码算法实现密钥协商。

最近，基于公钥密码的对密钥协商方案大量涌现，用以适应无人机网络环境下的应用场景。例如，Ozmen 等人[10]提出了一种基于公钥基础设施的无人机网络框架，将轻量级对称密码原语集成到框架中。该框架通过利用特殊的预计算方法和优化的椭圆曲线提供节能技术。但其没有考虑密钥撤销，攻击者仍然可能会利用算法的实现缺陷破译密钥。Munivel 等人[11]提出了一种基于公钥证书密钥协商方案，该方案有一个认证机构作为公钥证书的签发机构进行公钥证

书的生成、分布、验证、更新和撤销。但是无人机网络无可信第三方对密钥进行分发，因此基于公钥证书的方案不适用无人机网络。Capkun 等人 [12] 提出一个完全自组织的公钥管理系统，该系统允许用户生成他们的公私密钥对，颁发证书，并在没有任何集中服务的情况下执行身份验证，而不考虑网络分区。此外，该方法不需要任何可信的权威机构，甚至在系统初始化阶段也不需要，但节点的存储量和计算量都较大，且只能从概率上保证节点间的证书链。朱辉等人 [13] 根据无人机网络通信应用场景的具体特点，设计了面向无人机网络通信场景特化的密钥管理和认证协议。该方案将无人机网络分为有控制站节点和无控制站节点两种情况，并分别设计了在这两种情况下的密钥管理和认证协议。Cheon 等人 [14] 设计了一个基于同态加密的认证密钥协商方案，以在无人机网络环境中提供安全可靠的服务。然而，他们的方案并不能抵抗会话密钥泄露攻击和内部特权攻击。Ever 等人 [15] 提出了一个基于双线性配对的安全和高效的认证密钥协商框架，用于无人机网络环境中使用的移动汇聚节点。然而，该方案既无法抵抗无人机的物理捕获和假冒攻击，又不能提供前向安全。此外，该方案很难在资源受限的无人机网络环境中保证实时服务，因为它使用了双线性配对这种需要较高的计算和通信开销的运算方式。He 等人 [16] 提出了一种基于身份的安全无人机网络通信方案，采用分层广播加密和假名机制分别实现批量加密数据包传输和相互认证。为了保护无人机网络中传输数据的隐私，Khan 等人 [17] 在超椭圆曲线的基础上提出了无证书公钥密码学中的密钥封装方案。他们证明该方案比传统的椭圆曲线密码学更有效。然而，在上述方案中，无人机每次发送消息时，都必须执行非对称算法进行身份验证、加密或两者兼而有之。此外，这些无人机网络环境下基于 PKC 的认证密钥协商方案需要较高的计算开销和通信成本，因此不适用于资源受限的无人机网络环境。本文基于对密钥的认证密钥协商方案进行了总结性对比，如表 2 所示。

表 2 基于对组密钥的无人机认证密钥协商方案总结对比

方案	密码原语	描述	缺陷
Ozmen 等人	椭圆曲线	针对小型无人机量身定制的开源低能耗加密框架	高计算成本
Munivel 等人	非对称加密公钥基础设施	一种基于公钥证书密钥协商方案	无人机网络无可信第三方
Capkun 等人		完全自组织的公钥系统	较高的计算开销和通信成本
朱辉等人	椭圆曲线	向有控制站支持的无人机网络认证方案和面向无控制站支持的无人机网络认证方案	高计算成本
Cheon 等人	同态加密	基于同态加密的认证密钥协商方案，以在无人机网络环境中提供安全可靠的服务	不能抵抗会话密钥泄露攻击和内部特权攻击
Ever 等人	双线性对加密 椭圆曲线	针对无人机网络环境下移动传感器的安全双向认证与密钥协商协议	无前向安全 高计算成本
He 等人	分组密码	基于身份的分层广播加密和假名机制无人机网络安全通信方案	高计算成本
Khan 等人	超椭圆曲线	无证书公钥密码学中的密钥封装方案	较高的计算开销和通信成本

5 总结和展望

在许多应用场景中，无人机收集的数据具有敏感性和私密性，且无人机被部署在开放环境中，无人机之间的通信是通过不安全信道建立的，容易受到多种安全攻击，包括中间人攻击、重放攻击、监听攻击、假冒攻击、物理捕获攻击等，因此对无人机及其网络应用提出了较高的安全性要求，密钥协商是满足这种安全需求的基本技术手段。本文通过分析无人机自组网密钥协商的发展现状，总结归纳了现有方案的特点及存在的不足。密钥协商技术作为网络与信息安全的关键技术，在无人机网络中至关重要。移动网络的自组织和动态拓扑特性，传统的有线网络组通信中的密钥协商手段无法在移动网络中应用，因此在设计协议时，要从健壮性和效率两方面考虑，既要能处理单节点失效或变动的情况，又要能利用无人机有限的带宽完成任务。资源受限的无人机在计算、存储和通信带宽等方面相对有限，因此生成会话密钥的算法需要足够高效和轻量级。传统的方案中使用双线性对或椭圆曲线等能够显著提高会话的安全性，但其相对高昂的计算开销与存储要求并不适合基于无人机网络的轻量级认证密钥协商方案。另一方面，基于多因素（密码、指纹、生物识别等）的认证方案能够阻止敌手利用未知身份验证参数进行攻击，

但因需要存储验证参数在智能卡或者内存中，也无法保证无人机物理安全。综上所述，针对无人机网络中出现的数据安全与隐私保护问题，设计出既能有效保护无人机物理安全，又能实现轻计算开销和低通信成本的认证密钥协商方案，仍然具有重要的研究意义和应用价值。

参考文献：

[1]NYANGARESI V O, PETROVIC N. Efficient PUF based authentication protocol for internet of drones[C]//2021 International Telecommunications Conference (ITC-Egypt). Piscataway: IEEE,2021:1-4.

[2]DOLEV D, YAO A.On the security of public key protocols[J]. IEEE transactions on information theory,1983,29(2):198-208.

[3]WAZID M, DAS A K, KUMAR N, et al. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment[J].IEEE internet of things journal,2018,6(2):3572-3584.

[4]SRINIVAS J, DAS A K, KUMAR N, et al.TCALAS: temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment[J].IEEE transactions on vehicular technology, 2019, 68(7): 6903-6916.

[5]ALI Z, CHAUDHRY S A, RAMZAN M S, et al.Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles[J].IEEE access,2020,8:43711-43724.

[6]WON J, SEO S H, BERTINO E.Certificateless cryptographic protocols for efficient drone-based smart city applications[J]. IEEE access, 2017,5:3721-3749.

[7]TANVEER M, ZAHID A H, AHMAD M, et al.LAKE-IoD: lightweight authenticated key exchange protocol for the Internet of Drone environment[J].IEEE access, 2020, 8:155645-155659.

[8]SEMAL B, MARKANTONAKIS K, AKRAM R N.A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks[C]//2018 IEEE/AIAA 37th digital avionics systems conference (DASC).Piscataway: IEEE,2018:1-8.

[9] 施荣华 , 袁倩 . 一种安全的多层移动自组网密钥管理方案 [J]. 中南大学学报 (自然科学版), 2010,41(1):201-206.

[10]OZMEN M O, YAVUZ A A.Dronecrypt-an efficient cryptographic framework for small aerial drones[C]//MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM).Piscataway:IEEE,2018:1-6.

[11]MUNIVEL E, AJIT G M. Efficient public key infrastructure implementation in wireless sensor networks[C]//2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC). Piscataway: IEEE, 2010:1-6.

[12]CAPKUN S, BUTTYAN L, HUBAUX J P. Self-organized public-key management for mobile ad HOC networks[J]. IEEE transactions on mobile computing, 2003, 2(1):52-64.

[13] 朱辉 , 张业平 , 于攀 , 等 . 面向无人机网络的密钥管理和认证协议 [J]. 工程科学与技术 ,2019,51(3):158-166.

[14]CHEON J H, HAN K, HONG S M, et al.Toward a secure drone system: flying with real-time homomorphic authenticated encryption[J].IEEE access,2018,6:24325-24339.

[15]EVER Y K.A secure authentication scheme framework for mobile-sinks used in the internet of drones applications[J]. Computer communications, 2020, 155:143-149.

[16]HE S, WU Q, LIU J, et al.Secure communications in unmanned aerial vehicle network[C]//Information Security Practice and Experience: 13th International Conference, ISPEC 2017, Melbourne, VIC, Australia, December 13-15, 2017, Proceedings 13. Beerlin: Springer International Publishing, 2017: 601-620.

[17]KHAN M A, ULLAH I, NISAR S, et al.An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying Ad-hoc network[J]. IEEE access, 2020,8:36807-36828.

【作者简介】

张仕明（1988—），男，四川巴中人，硕士，工程师，研究方向：仪器科学与技术。

马舒凡（2000—），女，新疆阿克苏人，学士，助理工程师，研究方向：指控系统研发。

缪炜星（1988—），男，浙江衢州人，硕士，高级工程师，研究方向：体系对抗。

祝涛（1997—），男，江西南昌人，硕士，助理工程师，研究方向：卫星通信技术。

（收稿日期：2024-05-17）