航空科学技术
Aeronautical Science & Technology
Sept. 25 2023 Vol. 34 No.09 110-120

无人机网络中数控分离的安全传输机制

马诗雨[1]，张俊伟[1]，张兴隆[2]，卢笛[1]，马建峰[1]
1.西安电子科技大学，陕西 西安 710071
2.航空工业自控所 飞行器控制一体化技术国防科技重点实验室，陕西 西安 710065

摘 要：数据和飞控指令的安全性是无人机网络安全性的一个重要方面。针对现有的无人机网络安全机制中的不足，本文提出了一种数控分离的安全传输机制。针对无人机向地面站发送的数据采用基于高级加密标准的计数器和密文分组链接消息认证码（AES-CCM）认证加密机制的数据安全传输协议，保证数据的机密性和完整性，针对地面站向无人机发送的飞控指令设计了基于一次签名的飞控广播认证协议，保证飞控指令的完整性。通过安全性分析，证明所提出的方案能够保护数据的机密性和完整性，以及飞控指令的完整性。最后，通过仿真试验分析了所提出方案的性能，结果表明，所提出的数据安全传输协议发送100B和1KB的消息时，平均每个消息的认证加密时间和解密验证时间均不超过1ms；所提出的飞控广播认证协议在使用不同的哈希函数时，对1MB的飞控指令生成签名和验证签名的时间为1~2.7ms，在实际应用中具有高效性。

关键词：无人机网络；认证加密；广播认证；一次签名；网络安全

中图分类号：TP393 **文献标识码：**A DOI：10.19452/j.issn1007-5453.2023.09.013

在无人机网络中，无人机通过数据通信链路传输飞行数据给地面站，用于进一步分析。地面站通过数据通信链路将飞控指令发送给无人机，以便执行任务轨迹更新、飞行姿态调整等操作。因此，数据通信链路通常需要完整的通信协议，以便无人机和地面站进行消息报文的解析和封装。然而，无人机的消息传输常采用广播网络，其开放性也使得系统安全性遭到严重威胁，如指令伪造、数据重放、信号劫持等攻击，因此，无人机组网下的安全问题备受关注。

在无人机场景下，一方面，无人机将自身的数据发送给地面站，以供后续分析，这些数据与无人机自身的行为及其所处的环境特征相关，因此需要保证这些数据的机密性，为保证无人机所传输的数据被正确地发送给地面站，需要保证这些数据的完整性；另一方面，地面站将飞控指令发送给无人机，无人机需要验证该指令是否被篡改或破坏，以及该指令是否来自合法的地面站，即需要保证飞控指令的完整性。

目前，无人机系统的安全通信机制主要有两种思路：一是在物理层使用轨迹优化方法来抵抗窃听攻击，从而保护无人机所传输的数据的机密性[1-2]；二是使用加密和数字签名等密码学的方法保护数据的机密性和完整性[3-11]。然而，相关研究仅提出了数据安全保护机制，没有针对飞控指令的安全性问题提出解决方案。

目前，针对无人机飞行控制的相关研究主要关注无人机的位姿测量[12]、自主降落[13]以及抗干扰控制[14]等方面。然而，现有研究未关注飞控指令的完整性保护需求，因此未针对数据和飞控指令分别设计相应的保护机制。

本文针对无人机网络中数据传输和飞控指令传递的不同安全需求，提出了数控分离的安全传输机制。针对数据传输的机密性和完整性需求，在接入认证、群组安全管理、多域异构融合的基础上，基于协商的会话密钥，建立基于分

收稿日期：2023-05-16；退修日期：2023-06-09；录用日期：2023-07-20
基金项目：航空科学基金（20185881014）；陕西省自然科学基础研究计划项目（2023-JC-JQ-49，2022JZ-33）；中央高校基本科研业务费专项资金资助（YJSJ23007）
引用格式：Ma Shiyu，Zhang Junwei，Zhang Xinglong，et al.A data-control-separated secure transmission mechanism for UAV networks[J]. Aeronautical Science & Technology，2023，34(09)：110-120. 马诗雨，张俊伟，张兴隆，等. 无人机网络中数控分离的安全传输机制[J].航空科学技术，2023，34(09)：110-120.

组加密和消息认证码的安全传输通道，保障数据传输的机密性和完整性；针对飞控指令完整性的安全需求，基于哈希函数和哈希链构造飞控指令的可靠传输机制，在保证生成飞控指令的设备真实性同时，实现对控制信令完整性的验证，提出基于AES-CCM加密模式的数据安全通信协议以及基于一次签名的飞控广播认证协议。

1 研究现状

随着国内外学者对无人机网络的安全问题的日益关注，目前已经出现了一系列针对无人机网络的安全通信机制的研究。而无人机经常采用广播网络进行消息传输，因此，可使用广播认证协议实现无人机系统中高效的消息认证。

1.1 无人机网络安全通信机制

目前，针对无人机网络中的安全通信，已经存在一系列研究[15]。其中，许多研究旨在保护无人机系统中消息的机密性和完整性。

一些方法使用无人机轨迹优化的方式来抵御非法信道上的窃听攻击，从而保护无人机数据的机密性。徐煜轩等[1]针对无人机网络中信息在物理层的机密性保护问题，提出了一种基于概率视距信道模型的安全通信优化方法。Zhang等[2]提出了一种物理层的安全方法，通过无人机主动优化轨迹来提高合法信道的增益或削弱非法信道，从而抵御窃听攻击。

另一些工作通过密码学手段保护无人机数据的机密性和完整性。郭晶晶等[3]提出了一种无人机自组网中的拓扑消息完整性保护方案，该方案通过数字签名和区块链技术保护网络拓扑建立过程中消息的完整性。张凌浩等[4]提出了一种基于MAVLink协议的无人机系统安全通信方案，该方案基于对称密钥协商完成对地面站的身份认证和加密通信。张敏等[5]提出了一种基于安全概略算法的多因子认证密钥协商协议，能够抵抗密钥窃取、会话密钥泄露攻击、无人机伪装攻击和由第三方服务器发起的合谋攻击。贺蕾等[6]提出了一种面向无人机网络的属性代理签名方案，能够保护指挥机构向无人机发送的命令的完整性，提供认证，并保护签名者的隐私。王宇晨等[7]提出了一种基于区块链和智能合约的无人机数据安全共享和协同决策方法，能够保证数据的机密性、完整性和可用性。Li等[8]提出了一种针对无人机网络的高效节能的安全传输方法，该方法基于SM4轻量级对称国密算法和密钥协商机制保护通信内容的机密性，基于改进的聚合BLS签名和默克尔哈希树保护数据的完整性和真实性。Alladi等[9]提出了一种基于物理不可克隆函数的无人机身份认证机制，能够抵抗伪装、中间人攻击重放攻击等攻击手段。针对地面窃听者破坏数据机密性的攻击，Yang等[10]提出了一种基于零信任的无人机认证方式，实现了无人机群在数据交换和共享中的快速认证，保证消息的可靠性。Kim等[11]针对无人机数据窃听和非法获取控制权等攻击，提出了一种保护无人机通信数据和存储信息的模块，保护数据的机密性和完整性。

然而，上述的无人机网络安全通信机制相关研究仅仅关注无人机系统中数据的安全需求，没有重点关注飞控指令的完整性需求，因此没有针对无人机数据和飞控指令的不同安全需求分别设计安全通信机制。

1.2 广播认证协议

广播认证协议能够使发送者将认证的消息广播给整个网络，敌手无法篡改广播的消息。对于很多应用，如路由树的建立、软件升级、时间同步等，广播认证都是一个基本且十分重要的安全服务。

基于一次签名的广播认证具有效率高、即时认证、不需要时间同步、不可否认性的优点。Lamport[16]首先提出了一次签名的概念，随后一些一次签名方案也陆续被提出。Bos等[17]以及Bleichenbacher等[18]研究了基于非循环图的一次签名的问题。Even等[19]将公钥签名和一次签名结合提出了在线/离线签名。Hevia等[20]提出了可证安全的基于图论的一次签名。以上方案的计算量和通信开销都较大，不适合资源受限的网络。Perrig[21]首次提出了一个高效的一次签名方案，即BiBa。随后，Mitzenmacher等[22]改进了BiBa[21]并提出了Powerball签名。然而，BiBa[21]和Powerball[22]仅能在随机预言机(RO)模型下证明是安全的。HORS[23]是一个高效的一次签名方案，其安全性基于单向函数和子集弹性哈希函数。由于子集弹性哈希函数是一个较强的安全假设，针对HORS[23]出现了一些基于较弱安全假设的改进方案，如Pieprzyk等[24]设计了一个基于单向函数和非覆盖族可证安全的一次签名方案，但其通信开销和密钥长度都比HORS[23]大很多，不适合低能量设备。

广播认证协议被广泛应用于无线网络中。蒋毅等[25]提出了一种基于默克尔树的广播认证策略，支持无线传感器网络中存在大规模广播发送节点的情况。姚宣霞等[26]提出了一种基于Nyberg快速单向累加器的广播认证算法，并将其应用于无线传感器网络中。Hsiao等[27]提出了快速认证和选择性认证两种广播认证方案，该方案能够应对车联网场景下的签名泛洪导致无法在截止时间前验证签名的问

题。Maidhili等[28]提出了一种基于椭圆曲线公钥密码的广播认证机制，在无线传感器网络中可以实现低能耗的通信。

2 基本理论

本文所提出的数据安全传输协议使用计数器和密文分组链接消息认证码(CCM)模式的认证加密和高级加密标准(AES)分组加密模式，所提出的飞控广播认证协议使用基于哈希函数的一次签名算法。因此本节分别对AES分组加密算法、哈希函数和一次签名进行介绍。

2.1 AES分组加密算法

AES分组加密算法主要由4种运算组成：字节代换层(SubBytes)、行移位层(ShiftRows)、列混淆层(MixColumns)和轮密钥加层(AddRoundKey)。本文采用分组大小与密钥长度均为128位的AES算法，因此明密文块和密钥均由16个字节组成，按照从上到下、从左到右的顺序排列成一个4×4的矩阵，加密轮数为10轮，除了第10轮执行的操作外，其余9轮执行相同的四步运算。每轮加密后更新矩阵，直到得到密文。

2.2 哈希函数

哈希函数$H:\{0,1\}^{*}\rightarrow\{0,1\}^{v}$具有如下性质：

(1)单向性

对于任意概率多项式时间的敌手A，存在一个可忽略的概率v_{A}使得对于足够大的k，满足式(1)

$$\Pr\left(z\leftarrow \mathrm{A}\left(1^{k},y\right):x\rightarrow^{\mathrm{R}}\{0,1\}^{k};y\leftarrow H(x);H(z)=y\right)\leqslant v_{\mathrm{A}}(k) \tag{1}$$

(2)抗碰撞性

对于任意概率多项式时间的敌手A，存在一个可忽略概率v_{A}，使得对于足够大的k，满足式(2)

$$\Pr\left((x,x')\leftarrow \mathrm{A}\left(1^{k}\right):(x\neq x')\wedge\left(H(x)=H(x')\right)\right)\leqslant v_{\mathrm{A}}(\mathrm{k}) \tag{2}$$

2.3 一次签名

一次签名算法是指使用一个公私钥对仅能对一条消息进行签名的签名算法。一个一次签名算法Σ由三个子算法组成，即$\Sigma=(\mathrm{Gen},\mathrm{Sig},\mathrm{Ver})$，其中Gen为密钥生成算法，Sig为签名生成算法，Ver为签名验证算法。其算法描述如下：$\mathrm{Gen}\left(1^{\kappa}\right)$：密钥生成算法输入安全参数$\kappa$，输出公私钥对$(pk,sk)$。$\mathrm{Sig}(m,sk)$：签名算法输入消息$m$和私钥$sk$，输出消息$m$的一次签名$\sigma$。$\mathrm{Ver}(m,\sigma,pk)$：签名验证算法输入消息$m$，签名$\sigma$和公钥$pk$，输出验证结果。若验证结果正确，则输出1，否则输出0。

3 系统结构与设计目标

本节首先给出所提方案考虑的无人机网络的系统模型，之后对敌手的行为作出假设，提出敌手模型，最后提出本文的设计目标。

3.1 系统模型

本文所考虑的无人机网络由一个地面站和一个由若干无人机组成的无人机群所组成，系统模型如图1所示。一方面，地面站将飞控指令发送给无人机，无人机随后验证该指令的完整性以及其是否真正来自合法的地面站；另一方面，无人机执行地面基站发送的指令，并将各项机体信息和监测数据传输给地面站，以供后续分析。

本文所提出的方案适用于由数量不限的无人机组成的无人机群。在数据传输方面，在仅有一架无人机的情况下，该无人机使用其与地面站之间的对称密钥执行数据安全传输协议；在有多架无人机的情况下，所有无人机组成一个集群，使用预共享的群组密钥，以群组整体的形式执行数据安全传输协议，因此，无人机群向地面站发送的数据量独立于无人机的数量。在飞控指令传输方面，地面站以广播认证的方式向无人机群发送飞控指令，即地面站仅需广播一个飞控指令，即可控制多架无人机，因此，地面站发送飞控指令的数据量独立于无人机的数量。综上所述，所提出的方案不受无人机集群规模的限制，因此适用于任意规模的无人机群。

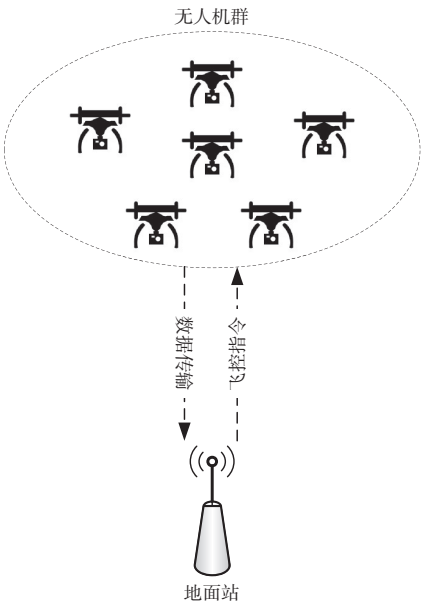

图1 无人机网络系统模型

Fig.1 System model of UAV network

3.2 敌手模型

以下定义敌手的行为，并限制了敌手在资源受限的无人机网络中的能力：(1)敌手可以监听网络上任意一条消息；(2)敌手可以是该方案中的任意一个合法参与方，能够与任意一方建立协议通信，发送消息，或接收任意一方发送的消息；(3)敌手可以伪装成协议中任何一个参与方，向其他任意的参与方发送消息；(4)敌手在计算上的能力受限，其破解哈希函数的概率是可忽略的。

针对上述对敌手行为的假设，定义以下三类敌手：(1)敌手A_1：试图获得无人机发送的数据；(2)敌手A_2：试图篡改无人机发送的数据，或伪装为合法的无人机，向地面站发送虚假数据；(3)敌手A_3：试图篡改地面站发送的飞控指令，或伪装为合法的地面站，向无人机发送飞控指令。

3.3 设计目标

针对无人机网络面临的以上安全威胁，本文拟设计一种针对无人机网络的数控分离的安全传输机制，达到以下设计目标：(1)数据的机密性，即无人机向地面站传输的数据无法被敌手获得；(2)数据的完整性，即无人机向地面站传输的数据无法被敌手篡改或伪造；(3)飞控指令的完整性，即地面站向无人机发送的飞控指令无法被敌手篡改或伪造；(4)高效性，即本文所提出的方案在性能上应具有较高的运行效率。

4 数控分离的安全传输机制

基于第一节对无人机网络中数据和飞控指令安全需求的分析，本文针对二者不同的安全需求，提出了数控分离的安全传输机制。针对无人机向地面站发送的数据，本文提出了一种基于AES-CCM的数据安全传输协议；针对地面站向无人机发送的飞控指令，本文提出了一种基于一次签名的飞控广播认证协议。

4.1 整体设计

本文所提出的数控分离的安全传输机制的系统流程如图2所示。针对无人机到地面站的数据传输，本文采用了基于AES-CCM认证加密机制的数据安全传输协议，其中，使用计数器(CTR)模式的AES-128分组加密生成密文数据，使用CBC-MAC和AES-128分组加密生成消息认证码。针对地面站向无人机发送的飞控指令，本文设计了基于一次签名的广播认证协议。

4.2 基于AES-CCM的数据安全传输协议

针对无人机向地面站发送的数据，本文设计了基于AES-CCM认证加密机制的数据安全传输协议，对数据提供机密性和完整性保证。该协议的过程如算法1所示。

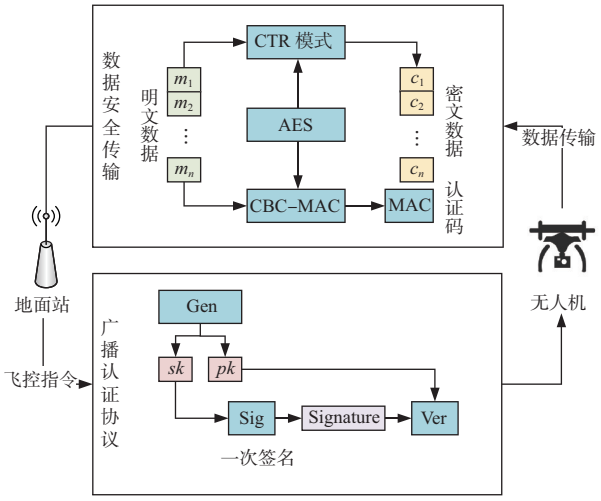

图2 本文的系统流程

Fig.2 Workflow of this paper

在基于AES-CCM的认证加密机制中，每架无人机和地面站共享一个AES的对称密钥K。无人机首先使用随机数Nonce和计数器生成的序列$ct_0, ct_2, \cdots, ct_{n-1}$，通过CTR模式的AES分组加密对消息$m$加密，生成密文$c_1, c_2, \cdots, c_n$，其过程如图3所示；之后使用基于CBC-MAC和AES分组密码的消息认证码机制生成消息认证码MAC，其过程如图4所示。无人机将密文$c_1, c_2, \cdots, c_n$和消息认证码MAC发送给地面站。地面站接收上述消息后，使用CTR模式的AES解密算法解密消息，并使用基于CBC-MAC和AES分组密码的消息认证码机制生成消息认证码MAC′。之后，比较MAC和MAC′，若二者相等，则消息认证码验证通过，接收无人机发送的消息m；否则，拒绝接收无人机发送的消息。

4.3 基于一次签名的飞控广播认证协议

针对地面站发送给无人机的飞控指令，本文提出了一种基于一次签名的飞控广播认证协议，用于保护飞控指令的完整性。该协议包含三个算法：密钥生成算法Gen、签名算法Sig和签名验证算法Ver，具体协议如算法2所示。

算法2中，基于一次签名的广播认证协议使用了哈希链，其构造方法如图5所示。其中，在密钥生成阶段Gen，地面站利用哈希函数f生成d层的单向链，选取链尾的$s_{0,0}, s_{1,0}, \cdots, s_{t-1,0}$作为初始公钥$v$，并将其上一层$s_{0,1}, s_{1,1}, \cdots, s_{t-1,1}$作为初始私钥$s$。在签名阶段Sig，地面站使用哈希函数$F$和$H$对消息$m$进行转换，并将带有签名$\sigma$和飞控指令$m$的消息发送给相应的无人机，之后进行密钥更新，更新过程如图6所示。地面站将签名值中使用过的公钥中

算法1 基于AES-CCM的数据安全传输协议

输入：消息m；
密钥K；
计数器发生器；
随机数Nonce；
初始化矢量$\boldsymbol{IV}$；
//无人机基于CTR分组加密模式生成密文
1. 对明文m进行填充并分组：$m_1, m_2, \cdots, m_n$；
2. 计数器生成序列$ct_0, ct_2, \cdots, ct_{n-1}$；
3. for i = 1 to n
//使用AES-128分组加密
4. 加密密钥$k_i \leftarrow \mathrm{Enc}\left(\left(ct_{i-1}, Nonce\right), K\right)$；
5. $c_i = m_i \oplus k_i$；
6. end for
//无人机生成密文分组链接消息认证码(CBC-MAC)
7. $T_1 = m_1 \oplus \boldsymbol{IV}$；
8. $b_1 = \mathrm{Enc}\left(T_1, K\right)$；
//使用AES-128分组加密
9. for i = 2 to n
10. $T_i = m_i \oplus b_{i-1}$；
11. $b_i = \mathrm{Enc}\left(T_i, K\right)$；
12. end for
13. MAC = b_n；
14. 无人机将$c_1, c_2, \cdots, c_n$, MAC发送给地面站；
//地面站解密消息并验证消息认证码(MAC)
15. 计数器生成序列$ct_0, ct_2, \cdots, ct_{n-1}$；
16. for i = 1 to n
//使用AES-128进行解密
17. 解密密钥$k_i \leftarrow \mathrm{Enc}\left(\left(ct_{i-1}, \mathrm{Nonce}\right), K\right)$；
18. $m_i = c_i \oplus k_i$；
19. end for
20. $m = m_1 \| m_2 \| \cdots \| m_n$；
21. 执行第7~13行的步骤，计算MAC′；
22. if MAC′ = MAC
23. return $(m, 1)$；
24. else
25. return 0；
26. end if

的$s_{i_j,r}$用其对应的私钥$s_{i_j,r+1}$进行替换，并将更新后的公钥上层的值$s_{i_j,r+2}$作为新的私钥，在验证阶段Ver，无人机首先使用当前的公钥验证收到的签名，即验证签名σ中的每个$s_j^{'}$是否满足$f\left(s_j^{'}\right) = v_{i_j}$，若满足，则签名通过验证，再按照如图6所示的方式对公钥进行更新。

5 安全性分析

本节基于第三节中所提出的敌手模型和相关假设，分别对所提出的数据安全传输协议和飞控广播认证协议进行安全性分析。

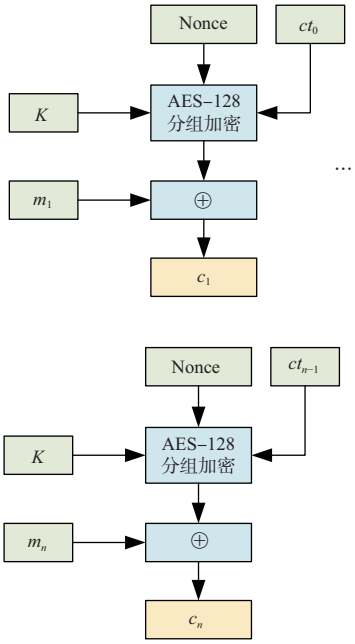

图3 CTR模式的AES-128

Fig.3 AES-128 in CTR mode

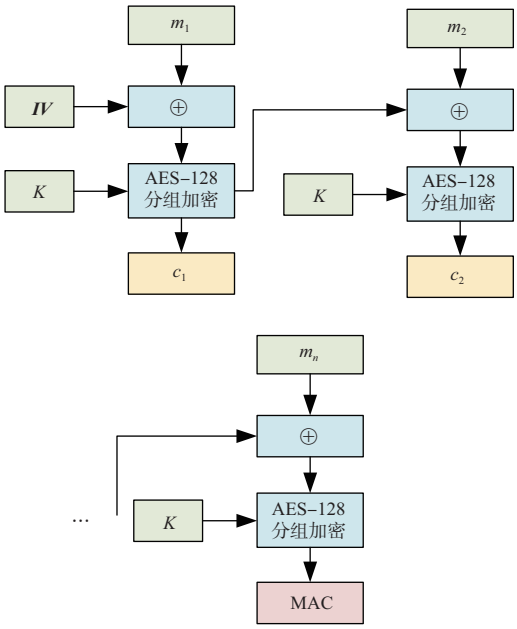

图4 基于AES-128的CBC-MAC

Fig.4 CBC-MAC based on AES-128

5.1 针对数据安全传输协议的安全性分析

对于算法1中的数据安全传输协议，以下分析该协议能够保证数据的机密性和完整性。

5.1.1 数据的机密性

本文所提出的数据安全传输机制能够保证数据的机密

算法2 基于一次签名的飞控广播认证协议

输入：安全参数p, q, l, L, k, t；

哈希函数$F: \{0,1\}^p \to \{0,1\}^q$；

哈希函数$H: \{0,1\}^{p+q} \to \{0,1\}^L$；

$L = k\log_2 t$；

哈希函数$f: \{0,1\}^l \to \{0,1\}^l$；

公开参数$(p, q, l, L, k, t, H, F, f)$，其中$l$ = 80bits；

协议最大消息轮数为d。

//密钥生成阶段(Gen)

地面站执行：

1. 地面站随机选择t个长度为l的比特串$s_{0,d}, s_{1,d}, \cdots, s_{t-1,d}$；
2. 计算矩阵

$\boldsymbol{S} = \left\{ s_{i,j} \middle| s_{i,j} = f\left(s_{i,j+1}\right), 0 \leqslant i < t-1, 0 \leqslant j \leqslant d-1 \right\}$；

3. 令$v_0 = s_{0,0}, s_{1,0}, \cdots, s_{t-1,0}, s = s_{0,1}, s_{1,1}, \cdots, s_{t-1,1}$，将$s$当作私钥，$v = v_0$作为公钥，公开$v$。

//地面站对消息m签名(Sig)

4. 地面站计算$n = \mathrm{F}(m)$, $h = \mathrm{H}(m \| n)$；
5. 令$h_1 \| h_2 \| \cdots \| h_k = h$, $i_j = h_j$，其中$\left|h_j\right| = \log_2 t$, $1 \leqslant j \leqslant k$；
6. 令私钥$s = s_0, s_1, \cdots, s_{t-1}$；
7. 令$\sigma = \left(s_{i_1}, s_{i_2}, \cdots, s_{i_k}\right)$为签名；
8. 用矩阵$\boldsymbol{S}$中的$s_{i_j, r+1}$替换公钥v中的$s_{i_j, r}$，用矩阵$\boldsymbol{S}$中的$s_{i_j, r+2}$替换私钥s中的$s_{i_j, r+1}$，$1 \leqslant j \leqslant k$；
10. 将(m, σ)发送给无人机。

//无人机验证签名(Ver)

11. 令$\sigma = \left(s'_1, s'_2, \cdots, s'_k\right), v = \left(v_0, v_1, \cdots, v_{t-1}\right)$；
12. 计算$n = F(m), h = H(m \| n)$；
13. 令$h_1 \| h_2 \| \cdots \| h_k = h$, $i_j = h_j$，其中$\left|h_j\right| = \log_2 t$, $1 \leqslant j \leqslant k$；
14. counter = 0；
15. for j = 1 to k
16. if $f\left(s'_j\right) = v_{i_j}$
17. counter + +；
18. end if
19. end for
20. if counter = k
21. 用$s_{i_j, r+1}$替换公钥v中的$s_{i_j, r}$, $1 \leqslant j \leqslant k$；
22. return 1；
23. else
24. return 0；
25. end if

性。在算法1中，无人机通过CTR模式的AES-128分组加密，使用和地面站共享的对称密钥K对消息m进行加密。由于AES-128的安全性和密钥的安全性，敌手A_1根据密文$c_1, c_2, \cdots c_n$获得明文m的概率可以忽略，即满足式(3)

$$\Pr\left(m' \leftarrow c_1, c_2, \cdots, c_n, m' = m\right) < \mathrm{negl} \tag{3}$$

因此，算法1的数据安全传输机制能够保护无人机数据的机密性。

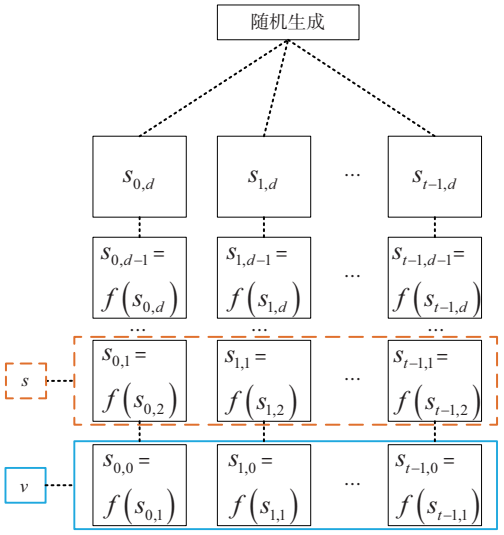

图5 基于哈希链的一次签名构造

Fig.5 Construction of one-time signature based on Hash chains

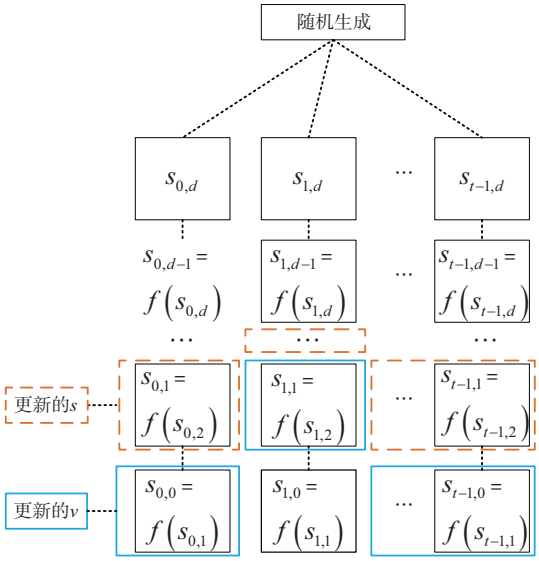

图6 密钥更新过程

Fig.6 Key updating procedure

5.1.2 数据的完整性

本文所提出的数据安全传输机制能够保证数据的完整性。在算法1中，无人机通过CBC-MAC和AES-128分组加密机制生成对消息m的消息认证码MAC。一方面，由于AES-128的安全性和CBC分组加密体制对错误的传播性质，敌手A_2针对伪造的消息$m'(m' \neq m)$，生成消息认证码MAC′，使得MAC′ = MAC的概率可以忽略，即满足式(4)

$$Pr(\mathrm{MAC} \leftarrow m, \mathrm{MAC}' \leftarrow m', m \neq m', \mathrm{MAC} = \mathrm{MAC}') < \mathrm{negl} \tag{4}$$

另一方面，由于密钥K仅由无人机和地面站共享，AES-128密钥空间为2^{128}，敌手A_2猜测密钥K，进而伪装成合法的无人机发送数据的概率为$1/2^{128}$，这一数值可以忽略。因此，本文所提出的数据安全传输机制能够保证无人机数据的完整性。

综上所述，本文所提出的数据安全传输机制能够保证无人机数据的机密性和完整性。

5.2 针对飞控广播认证协议的安全性分析

本文所提出的飞控广播认证协议能够保护地面站发送的飞控指令的完整性。

（1）在密钥生成阶段，地面站基于哈希函数f生成矩阵S，并将最低一层的v作为公钥，将其上一层的s作为私钥。由于哈希函数f具有单向性，则敌手A_3根据公钥v成功推断私钥s的概率是可以忽略的，即满足式(5)

$$\Pr\left(A_3:s' \leftarrow v, s' = s\right) < \mathrm{negl} \tag{5}$$

（2）在签名阶段，地面站首先会生成消息m的哈希函数值$n=F(m)$。由于哈希函数F具有抗碰撞性，敌手A_3对一个伪造的消息$m'(m' \neq m)$生成一个哈希函数值n'，使得$n' = n$的概率是可以忽略的，即满足式(6)

$$\Pr\left(m' \neq m, n = F(m), n' = F(m'), n' = n\right) < \mathrm{negl} \tag{6}$$

（3）在签名阶段，地面站计算$h=H\left(m \| n\right)$。由于哈希函数H具有抗碰撞性，敌手A_3对一个伪造的消息m'生成$h' = H\left(m' \| n\right)$，使得$h' = h$的概率是可忽略的，即满足式(7)

$$\begin{aligned}&\Pr\left(m' \neq m, n = F(m), h = H\left(m \| n\right),\right.\\&\left.h' = H\left(m' \| n\right), h = h'\right) < \mathrm{negl}\end{aligned} \tag{7}$$

（4）在签名阶段，地面站输出消息m及其签名$\sigma = \left(s_{i_1}, s_{i_2}, \cdots, s_{i_k}\right)$。敌手$A_3$试图对伪造的消息$m'$生成签名$\sigma'$，使得$\sigma' = \sigma$。由于$s_{i_j}$的长度为$l$，则敌手$A_3$伪造$\sigma' = \left(s_{i_1}^{'}, s_{i_2}^{'}, \cdots, s_{i_k}^{'}\right)$，使得$\sigma' = \sigma$的概率可由式(8)表示

$$\Pr\left(s_{i_1} = s_{i_1}^{'}, s_{i_2} = s_{i_2}^{'}, \cdots, s_{i_k} = s_{i_k}^{'}\right) = \left(2^{-l}\right)^k = 2^{-lk} \tag{8}$$

通常情况下，$l \geqslant 80$，因此这一概率可以忽略。

综合上述分析，敌手A_3伪装为地面站发送飞控指令，或篡改地面站的飞控指令，使得签名可以通过无人机的验证的概率是可忽略的，因此，本文所提出的基于一次签名的飞控广播认证协议能够保护飞控指令的完整性。

6 性能测试

6.1 试验设置

本文通过仿真试验来对所提出的方案进行性能测试。目前主流的无人机机载计算机包括树莓派和Jetson等。由于树莓派具有体积小、成本低、可编程和可扩展的特点，在无人机系统的搭建与开发中，经常使用树莓派作为无人机机载计算机，因此，本文使用树莓派模拟无人机的程序执行。无人机地面站通常由计算机、显示器、遥控器和数据链路4类硬件设备组成，其中，计算机需要有足够的运算和存储能力。由于本文重点关注地面站参与执行数据安全传输和飞控广播认证协议的开销，方案中使用了对称加密和哈希函数等计算开销相对较小的密码学技术，因此，本文使用PC模拟地面站的程序执行，能够满足所设计的协议的执行。使用C语言，基于OpenSSL库进行性能测试。

本文对数据安全传输协议和广播认证协议的性能分别进行如下测试：

（1）对于数据安全传输协议，本文评估了方案的加密与消息认证码生成，以及解密与验证过程的运行时间。其中，AES-CCM模式的分组大小和密钥长度为128bits，分别统计了数量N为100、1000、10000和10万的100B和1KB的消息时，执行认证加密模块所需的时间t_{ae}和执行验证解密模块所需的时间t_{vd}，单位为s。其中，消息选取100B和1KB的全0比特串。

（2）对于广播认证协议，本文评估了该协议使用不同的哈希函数的情况下各阶段的运行时间。具体地，本文统计了当分组数量k分别取2、4、8、16、32、64、128和256时，使用MD5、SHA-1、SHA-256和SHA-512的哈希函数时的签名生成时间和签名验证时间，单位为ms。仿真地面站发送一个1MB的飞控指令给无人机。

6.2 试验结果分析

6.2.1 数据安全传输协议性能测试

无人机对100B和1KB的数据执行认证加密模块所需的时间t_{ae}如图7所示。无人机对100B的数据进行100次认证加密耗时0.09s，进行1000次认证加密耗时0.64s，进行10000次认证加密耗时3.74s，进行10^5次认证加密耗时40.9s。无人机对1KB的数据进行100次认证加密耗时0.09s，进行1000次认证加密耗时0.5s，进行10000次认证加密耗时3.79s，进行10^5次认证加密耗时43.02s。

地面站执行验证解密模块所需的时间t_{vd}如图8所示。地面站对100B的数据进行100次验证解密耗时0.06s，进行1000次验证解密耗时0.6s，进行10000次验证解密耗时3.6s，进行10^5次验证解密耗时38.88s。地面站对1KB的数据进行100次验证解密耗时0.06s，进行1000次验证解密耗时0.45s，进行10000次验证解密耗时3.72s，进行10^5次验证

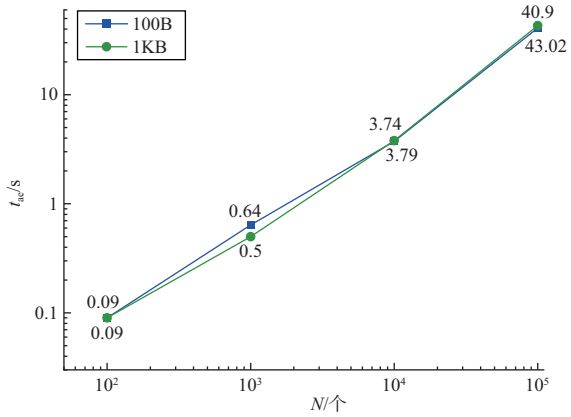

图7 AES-CCM认证加密模块的运行时间

Fig.7 Running time of the authenticated encryption module of AES-CCM

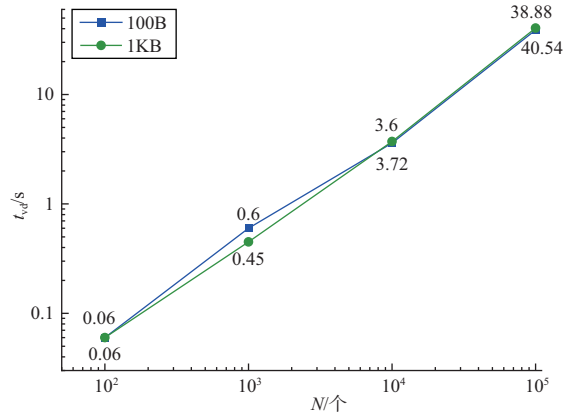

图8 AES-CCM验证解密模块的运行时间

Fig.8 Running time of the verification and decryption module of AES-CCM

解密耗时40.54s。

由上述数据可以分析得出，由于本文所提出的数据安全传输协议基于对称密码体制，发送100B和1KB的消息时，平均每个消息的认证加密时间和解密验证时间均不超过1ms，数据安全传输协议的开销较小。

6.2.2 飞控广播认证协议性能测试

本文所提出的飞控广播认证协议在分组数量k取不同的值和使用不同的哈希函数的情况下，地面站的签名生成时间t_s如图9所示。当哈希函数为MD5，对一个大小为1MB的飞控指令生成一次签名，选取分组数量k为2时，耗时2.6ms；k为4时，耗时2.52ms；k为8时，耗时2.58ms；k为16时，耗时2.54ms；k为32时，耗时2.58ms。当哈希函数为SHA-1，对一个大小为1MB的飞控指令生成一次签名，选取分组数量k为2时，耗时1.03ms；k为4时，耗时1.02ms；k为8时，耗时1.01ms；k为16时，耗时1.02ms；k为32时，耗时1ms。当哈希函数为SHA-256，对一个大小为1MB的飞控指令生成一次签名，选取分组数量k为2时，耗时1.17ms；k为4时，耗时1.18ms；k为8时，耗时1.22ms；k为16时，耗时1.23ms；k为32时，耗时1.19ms；k为64时，耗时1.19ms；k为128时，耗时1.2ms。当哈希函数为SHA-512，对一个大小为1MB的飞控指令生成一次签名，选取分组数量k为2时，耗时2.52ms；k为4时，耗时2.65ms；k为8时，耗时2.49ms；k为16时，耗时2.55ms；k为32时，耗时2.63ms；k为64时，耗时2.59ms；k为128时，耗时2.63ms；k为256时，耗时2.65ms。

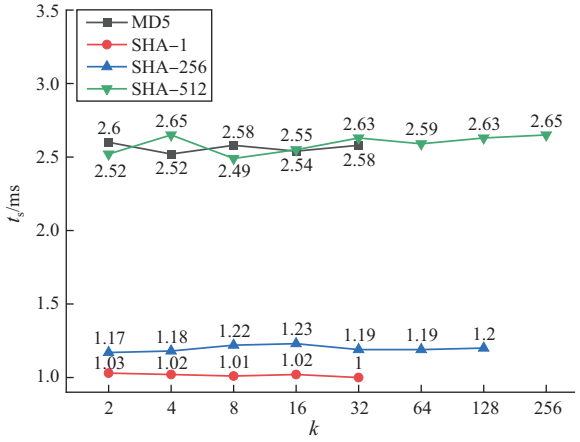

图9 签名生成时间

Fig.9 Running time of signature generation

当k取不同的值，选择不同的哈希函数，无人机的签名验证时间t_v如图10所示。当哈希函数为MD5，对一个大小为1MB的飞控指令进行签名验证，选取分组数量k为2时，耗时2.6ms；k为4时，耗时2.52ms；k为8时，耗时2.58ms；k为16时，耗时2.54ms；k为32时，耗时2.58ms。当哈希函数为SHA-1，对一个大小为1MB的飞控指令进行签名验证，选取分组数量k为2时，耗时1.03ms；k为4时，耗时1.02ms；k为8时，耗时1.01ms；k为16时，耗时1.02ms；k为32时，耗时1ms。当哈希函数为SHA-256，对一个大小为1MB的飞控指令进行签名验证，选取分组数量k为2时，耗时1.17ms；k为4时，耗时1.18ms；k为8时，耗时1.22ms；k为16时，耗时1.23ms；k为32时，耗时1.19ms；k为64时，耗时1.19ms；k为128时，耗时1.2ms。当哈希函数为SHA-512，对一个大小为1MB的飞控指令进行签名验证，选取分组数量k为2时，耗时2.52ms；k为4时，耗时2.65ms；k为8时，耗时2.49ms；k为16时，耗时2.55ms；k为32时，耗时2.65ms；k为64时，耗时2.6ms；k为128时，耗时2.67ms；k为256时，耗时2.7ms。

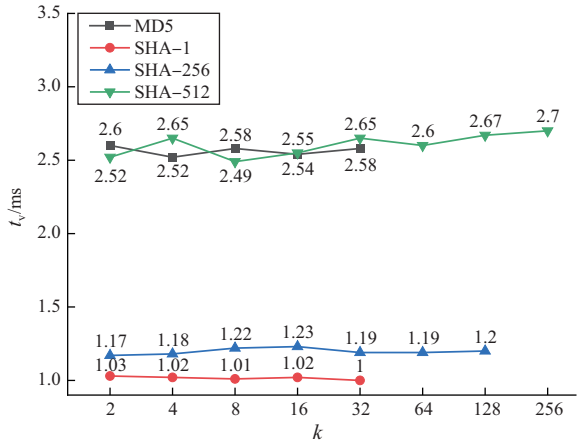

图10 签名验证时间

Fig.10 Running time of signature verification

由上述数据可以分析得出，由于本文中选取的飞控指令的长度较大（1MB），在对其进行签名的生成和验证时，飞控指令的大小对运行时间的影响相对较大，而分组数量k的值对运行时间的影响相对较小。此外，选取不同的哈希函数和分组数量k值，对大小为1MB的飞控指令进行签名生成和验证的时间总体上较小，为1~2.7ms。因此，本文所提出的基于一次签名的飞控广播认证协议具有高效性。

7 结论

本文提出了一种无人机网络中数控分离的安全传输机制，针对无人机网络的数据通信链路提出了一种基于AES-CCM认证加密机制的数据安全传输协议；针对无人机网络的飞控指令提出了一种基于一次签名的飞控广播认证协议；安全性分析结果表明所提出的数据安全传输协议能够保证无人机发送给地面站的数据的机密性和完整性，所提出的飞控广播认证协议能够保证飞控指令的完整性。仿真试验结果表明，所提出的数据安全传输协议在发送100B和1KB的消息时，平均每个消息的认证加密时间和解密验证时间均不超过1ms；所提出的飞控广播认证协议在使用不同的哈希函数时，对1MB的飞控指令生成签名和验证签名的时间约为1~2.7ms，在无人机网络的应用中具有高效性。

AST

参考文献

[1] 徐煜轩, 崔苗, 张广驰, 等. 概率视距空地信道下的无人机安全通信优化设计研究[J]. 计算机应用研究, 2023, 40(2): 554-560.
Xu Yuxuan, Cui Miao, Zhang Guangchi, et al. UAV secure communication optimization design under probabilistic line-of-sight air-ground channels[J]. Application Research of Computers, 2023, 40(2): 554-560.(in Chinese)

[2] Zhang Guangchi, Wu Qingqing, Cui Miao, et al. Securing UAV communications via joint trajectory and power control[J]. IEEE Transactions on Wireless Communications, 2019, 2(18): 1376-1389.

[3] 郭晶晶, 高华敏, 刘志全, 等. 面向无人机自组网的路由消息完整性保护方法[J]. 航空科学技术, 2022, 33(4): 28-38.
Guo Jingjing, Gao Huamin, Liu Zhiquan, et al. Integrity protection method of routing message for UAV ad-hoc networks[J]. Aeronautical Science & Technology, 2022, 33(4): 28-38.(in Chinese)

[4] 张凌浩, 王胜, 周辉, 等. 基于MAVLink协议的无人机系统安全通信方案[J]. 计算机应用, 2020, 40(8): 2286-2292.
Zhang Linghao, Wang Sheng, Zhou Hui, et al. Secure communication scheme of unmanned aerial vehicle system based on MAVLink protocol[J]. Journal of Computer Applications, 2020, 40(8): 2286-2292.(in Chinese)

[5] 张敏, 许春香, 张建华. 无人机网络中基于多因子的认证密钥协商协议研究[J]. 信息网络安全, 2022(9): 21-30.
Zhang Min, Xu Chunxiang, Zhang Jianhua. Research on authentication key agreement protocol based on multi-factor in internet of drones[J]. Netinfo Security, 2022(9): 21-30.(in Chinese)

[6] 贺蕾, 马建峰, 魏大卫. 面向无人机网络的属性代理签名方案[J]. 通信学报, 2021, 42(11): 87-96.
He Lei, Ma Jianfeng, Wei Dawei. Attribute-based proxy signature scheme for unmanned aerial vehicle networks[J]. Journal on Communications, 2021, 42(11): 87-96.(in Chinese)

[7] 王宇晨, 齐文慧, 徐立臻. 基于区块链的无人机集群安全协作[J]. 计算机科学, 2021, 48(z2): 528-532, 546.
Wang Yuchen, Qi Wenhui, Xu Lizhen. Security cooperation of UAV swarm based on blockchain[J]. Computer Science, 2021, 48(z2): 528-532, 546. (in Chinese)

[8] Li Teng, Zhang Jiawei, Mohammad S O, et al. Energy-efficient and secure communication toward UAV networks[J]. IEEE Internet of Things Journal, 2022, 9(12): 10061-10076.

[9] Alladi T, Naren N, Bansal G, et al. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication[J]. IEEE Transactions on Vehicular Technology, 2020, 12(69): 15068-15077.

[10] Yang Dongyu, Zhao Yue, Wu Kaijun, et al. An efficient authentication scheme based on zero trust for UAV swarm[C]. 2021 International Conference on Networking and Network Applications (NaNA), 2021: 356-360.

[11] Kim K, Kang Y. Drone security module for UAV data encryption[C]. 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020: 1672-1674.

[12] 阎峰, 刘震. 基于立体视觉的无人机位姿测量方法[J]. 航空科学技术, 2023, 34(4): 72-78.
Yan Feng, Liu Zhen. UAV pose measurement method based on stereo vision[J]. Aeronautical Science & Technology, 2023, 34 (4):72-78. (in Chinese)

[13] 刘飞, 单佳瑶, 熊彬宇, 等. 基于多传感器融合的无人机可降落区域识别方法研究[J]. 航空科学技术, 2022, 33(4): 19-27.
Liu Fei, Shan Jiayao, Xiong Binyu, et al. Research on the identification method of UAV landing area based on multi-sensor fusion[J]. Aeronautical Science & Technology, 2022, 33 (4): 19-27. (in Chinese)

[14] Yu Xiang, Zhou Xiaobin, Guo Kexin, et al. Safety flight control for a quadrotor UAV using differential flatness and dual-loop observers[J]. IEEE Transactions on Industrial Electronics, 2022, 12(69): 13326-13336.

[15] Gupta L, Jain R, Vaszkun G. Survey of important issues in UAV communication networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(2):1123-1152.

[16] Lamport L. Constructing digital signatures from a one way function [R]. Technical Report CSL-98, 1979.

[17] Bos J, Chaum D. Provably unforgeable signatures[C]. Annual International Cryptology Conference, 1992.

[18] Bleichenbacher D, Maurer U. Directed acyclic graphs, one-way functions and digital signatures. [C]. Advances in Cryptology-CRYPTO, 1994: 75-82.

[19] Even S, Micali G S. On-line/off-line digital signatures[J]. Journal of Cryptology, 1996, 9(1): 35-67.

[20] Hevia A, Micciancio D. The provable security of graph-based one-time signatures and extensions to algebraic signature schemes[C]. Advances in Cryptology-ASIACRYPT 2002,2002: 379-396.

[21] Perrig A. The BiBa One-time signature and broadcast authentication protocol[C]//Proceedings of the 8th ACM conference on Computer and Communications Security, 2001: 28-37.

[22] Mitzenmacher M, Perrig A. Bounds and improvements for BiBa signature schemes[D]. USA: Harvard University, 2002.

[23] Reyzin L, Reyzin N. Better than BiBa: short one-time signatures with fast signing and verifying[C]. Australian Conference on Information Security & Privacy,2002.

[24] Pieprzyk J, Wang H, Xing C. Multiple-time signature schemes against adaptive chosen message attacks[C]. Selected Areas in Cryptography, 10th Annual International Workshop, 2003.

[25] 蒋毅, 史浩山. 无线传感器网络中基于Merkle树的广播认证策略[J]. 传感技术学报, 2007, 20(7): 1597-1602.
Jiang Yi, Shi Haoshan. Merkle tree based broadcast authentication strategies in wireless sensor networks[J]. Chinese Journal of Sensors and Actuators, 2007, 20(7): 1597-1602.(in Chinese)

[26] 姚宣霞, 郑雪峰, 周贤伟. 适用于无线传感器网络的广播认证算法[J]. 通信学报, 2010, 31(11): 49-55.
Yao Xuanxia, Zheng Xuefeng, Zhou Xianwei. Broadcast authentication algorithm for wireless sensor networks[J]. Journal on Communications, 2010, 31(11): 49-55.(in Chinese)

[27] Hsiao H C, Studer A, Chen Chen, et al. Flooding-resilient broadcast authentication for VANETs[C]//Proceedings of the 17th annual international conference on Mobile computing and networking (MobiCom'11). Association for Computing Machinery, 2011: 193-204.

[28] Maidhili R, Karthik G M. Energy efficient and secure multi-user broadcast authentication scheme in wireless sensor networks[C]. 2018 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 2018: 1-6.

A Data-control-separated Secure Transmission Mechanism for UAV Networks

Ma Shiyu[1], Zhang Junwei[1*], Zhang Xinglong[2], Lu Di[1], Ma Jianfeng[1]

1. Xidian University, Xi'an 710071, China

2. National Key Laboratory of Science and Technology on Integrated Control Technology, AVIC Flight Automatic Control Research Institute, Xi'an 710065, China

Abstract: The security of data and flight control instruction is an important aspect of Unmanned Aerial Vehicle (UAV) network security. In view of the shortcomings of the existing UAV network security mechanisms, this paper proposes a data-control-separated secure transmission mechanism. For the data sent from a UAV to the ground station, this paper adopts a secure data transmission mechanism based on authenticated encryption of Advanced Encryption Standard-Counter with Cipher-Block Chaining Message Authentication Code (AES-CCM) to ensure the confidentiality and integrity of the data. For the flight control instructions sent from ground stations to UAVs, this paper designs a flight control broadcast authentication protocol based on one-time signature to ensure the integrity of flight control instructions. With the security analysis, this paper proves that the proposed scheme can provide confidentiality and integrity for the data, as well as the integrity for the flight control instructions. Finally, this paper analyzes the performance through simulation experiments. The results show that for the secure data transmission protocol, both the average authenticated encryption time and the average verification and decryption time are less than 1 millisecond when sending 100-byte and 1-kilobyte messages. For the flight control broadcast authentication protocol, both the time to generate a signature and the time to verify a signature of a 1MB flight control instruction are between 1 and 2.7 milliseconds, which is efficient in practical applications.

Key Words: UAV networks; authenticated encryption; broadcast authentication; one-time signature; network security

Received: 2023-05-16; **Revised:** 2023-06-29; **Accepted:** 2023-07-20

Foundation item: Aeronautical Science Foundation of China(20185881014); Natural Science Basic Research Program of Shaanxi (2023-JC-JQ-49, 2022JZ-33); The Fundamental Research Funds for the Central Universities(YJSJ23007)