面向无人机通信的认证和密钥协商协议

蹇奇芮，陈泽茂，武晓康

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220200098

面向无人机通信的认证和密钥协商协议

蹇奇芮[1,2]　**陈泽茂**[1,2]　**武晓康**[3]
1 空天信息安全与可信计算教育部重点实验室　武汉 430072
2 武汉大学国家网络安全学院　武汉 430072
3 海军工程大学电气工程学院　武汉 430033
(jianqirui@whu.edu.cn)

摘　要　针对无人机通信中密钥配置的安全性和轻量化需求,面向不同计算性能的无人机系统分别提出了基于椭圆曲线密码算法的认证和密钥协商协议 DroneSec,以及基于对称密码算法的认证和密钥协商协议 DroneSec-lite。所提协议实现了无人机和地面站之间的双向身份认证和通信密钥配置功能,其中 DroneSec 协议通过结合使用 ECDH(Elliptic-Curve Diffie-Hellman)和消息认证码,在保证前向安全性的情况下减小了计算开销,适用于较高性能的计算平台;DroneSec-lite 协议仅使用了对称密码算法,因而计算开销极低,适用于低性能平台。使用安全协议形式化验证工具 ProVerif 验证了协议在加强的 Dolve-Yao 威胁模型下进行双向认证和密钥配置的安全性,并通过仿真环境实验对协议的性能进行了对比测试和分析。结果显示,协议的计算、通信开销和安全性优于已有协议。

关键词:无人机;双向认证;密钥协商;通信安全;安全协议;形式化验证
中图法分类号　TP309

Authentication and Key Agreement Protocol for UAV Communication

JIAN Qi-rui[1,2],CHEN Ze-mao[1,2] and WU Xiao-kang[3]
1 Key Laboratory of Aerospace Information Security and Trusted Computing,Ministry of Education,Wuhan 430072,China
2 School of Cyber Science and Engineering,Wuhan University,Wuhan 430072,China
3 School of Electrical Engineering,Naval University of Engineering,Wuhan 430033,China

Abstract　In order to achieve the requirement for security and lightweight in unmanned aerial vehicle(UAV)communication,two authentication and key agreement protocols targeted for UAVs with different computational performance are proposed,including an ECC based protocol,DroneSec,and a symmetric cipher based protocol,DroneSec-lite. The two protocols achieve secure mutual authentication and key configuration between ground stations and UAVs. DroneSec protocol achieves relatively low computational overhead while ensuring forward secrecy through combining ECDH and MAC,which is suitable for relatively high-performance platforms. DroneSec-lite protocol achieves extremely low computational overhead through using only symmetric ciphers,which is suitable for low-performance platforms. The security of the proposed protocols under the enhanced Dolve-Yao model is verified using ProVerif,a formal protocol verification tool,and the performance of the protocols is analyzed in the simulation environment. The results show that it is superior to existing protocols in terms of computation overhead,communication overhead and security.

Keywords　Unmanned aerial vehicle,Mutual authentication,Key agreement,Communication security,Security protocol,Formal verification

1　引言

近年来,随着技术的成熟和制造成本的逐渐降低,无人机(Unmanned Aerial Vehicle,UAV)在军用和民用领域都得到了越来越广泛的使用。如今,无人机已经被广泛应用于地理测绘、安防巡逻、电力油气巡检、应急救援等各个领域[1]。

由于无人机同地面站(Ground Station)之间的通信主要使用无线信道,而无线信道是一种广播式的信道,在没有充分保护的情况下,攻击者可以轻易窃听、篡改和伪造无线信道上传输的数据,从而窃取重要隐私数据甚至劫持执行各种关键

到稿日期:2022-02-18　返修日期:2022-03-08
基金项目:国家自然科学基金面上项目(61872430);国家优秀青年科学基金(42122025);湖北省杰出青年科学基金(2019CFA086)
This work was supported by the National Natural Science Foundation of China(61872430),National Science Foundation for Outstanding Young Scholars(42122025) and Natural Science Foundation for Distinguished Young Scholars of Hubei Province,China(2019CFA086).
通信作者:陈泽茂(chenzemao@163.com)

任务的无人机[2-5]，造成不可估量的损失。为了实现无人机和地面站之间的安全通信，必须首先保证无人机和地面站通信密钥配置的安全性，即实现无人机和地面站的双向身份认证以及密钥协商。传统互联网中适用的 DTLS（Datagram Transport Layer Security）协议[6]、TLS（Transport Layer Security）协议[7]以及部分现有的无人机密钥协商协议存在性能开销过大或者安全性不足的问题。针对这些问题，本文的主要研究工作如下：

（1）设计了用于较高计算性能的无人机系统的认证和密钥协商协议 DroneSec，在保证安全性的前提下显著减少了椭圆曲线上的点乘运算次数，计算开销小；使用无证书认证显著减小了通信和存储开销。

（2）设计了用于低性能无人机系统的认证和密钥协商协议 DroneSec-lite，仅使用对称密码算法实现了极低的性能开销。

（3）使用安全协议形式化验证工具 ProVerif[8] 验证了两种协议在加强的 Dolve-Yao 威胁模型[9]下进行双向身份认证以及密钥协商的安全性。

（4）在仿真实验环境中对协议的性能进行了测试分析。

2 相关工作

目前针对无人机无线通信保护的研究主要分为基于物理信道的保护方案和基于密码学算法的保护方案两大类。文献[10-12]提出了基于物理信道的保护方案，此类方案能够较好地抵抗信道阻塞攻击，然而仅能保证一定的秘密性，难以实现完整性保护、身份认证等功能，因此无法单独用于实现高安全性要求的无线通信保护。基于密码学算法的保护方案则是通过结合多种密码算法来实现身份认证以及通信数据的加密、认证等功能。在传统互联网中广泛使用的通信保护协议 TLS 和 DTLS 能够满足安全需求，但其计算开销、通信开销以及存储开销均很大，且依赖于 TCP/IP 协议栈，难以满足性能较低以及广泛使用串口等通信方式的无人机系统。文献[13]提出了一种基于 FPGA（Field-Programmable Gate Array）的无人机通信数据加密方案，其使用 AES 和 CBC-MAC（Cipher Block Chaining-Message Authentication Code）算法来保证通信数据的秘密性和完整性，但方案带宽开销过大，并且加密密钥依靠人工在每次起飞前通过安全的信道注入无人机，操作较为繁琐，难以适用于多架无人机的场景。文献[14]提出了一种基于预共享的密钥表的认证和信道加密方案，但仅能实现无人机对地面站的单向认证，并且需要预先存储大量用于认证的密钥表，存储开销很大。文献[15]提出了一种无人机密钥管理和认证协议，实现了无人机和地面站双向身份认证和密钥协商，但该协议需要在无人机每次起飞前通过安全信道进行无人机私钥配置，操作较为复杂，不适用于无人机数量较多的场景。文献[16]提出了一种基于 MAVLink 的通信加密协议，测试和分析了使用多种不同的加密算法加密 MAVLink 协议的载荷部分的计算性能开销，但该协议仅实现了数据加密，缺少认证、密钥配置、完整性校验等功能。文献[17]提出了一种基于 MAVLink 的通信保护方案，该方案使用 Diffice-Hellman 密钥交换协议进行密钥协商，并利用协商的密钥对 MAVLink 的 payload 字段进行加密，但该方案没有完整性检测和重放检测机制，并且其密钥协商部分缺乏身份认证机制，易受中间人攻击。文献[18]提出了一种无人机通信保护方案，包括基于椭圆曲线的身份认证和密钥协商协议以及基于 MAVLink 的通信加密协议，但其身份认证协议存在缺陷，仅能实现单向身份认证；其通信加密协议仅使用简单的密钥哈希进行完整性校验而非安全的消息认证码算法，因此会受到消息扩展攻击影响[19]。文献[20]提出了一种基于 PUF（Physical Unclonable Function）的无人机身份认证和密钥协商协议，其利用 PUF 的特性避免了复杂的密码学运算，因此计算性能开销极低，但基于 PUF 的方案存在配置复杂且需要特定的 PUF 硬件等缺点。文献[21]提出了一种基于数字水印的无人机通信数据认证方案，相比消息认证码方案，所提方案的计算开销更低，但同时安全性也相对较差。文献[22]提出了一种用于地面站对无人机的飞行任务的合法性进行认证的协议，该协议基于椭圆曲线数字签名和公钥加密算法来实现无人机和地面站的双向身份认证和密钥协商，相比 TLS，所提协议显著减小了通信开销，但计算开销仍然较大；该文献还给出了该协议的安全性证明，但仅证明了单向认证的安全性，经过分析，该协议存在认证缺陷，攻击者可以伪装合法无人机同地面站完成协议。文献[23]提出了一种基于 ECDSA（Elliptic Curve Digital Signature Algorithm）和 ECDH 的无人机身份认证和密钥协商协议，该协议能够抵抗来自无人机网络外部非法节点的中间人攻击，实现双向认证，但会受到无人机网络内部节点的中间人攻击。文献[24]提出了一种基于 ECDSA 和 ECDH 的无人机身份认证和密钥协商方案，该方案使用了 HMAC（Hash-based Message Authentication Code）和 ECDSA 进行双重校验，保证了双向身份认证的安全性，同时一定程度地缓解了拒绝服务攻击，使用 ECDH 进行密钥协商，保证了前向安全性；但该方案使用了大量数字签名运算，且存在证书交换和验证过程，总体计算开销和通信开销较大。

3 网络模型和攻击者模型

3.1 网络模型

本文的协议面向图 1 所示的无人机通信网络模型。在该网络中，地面站通过无线链路同多架无人机建立连接，实现对多架无人机的控制以及状态监测。无人机仅同地面站进行通信，无人机之间不进行通信。

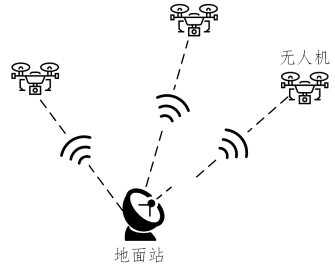

图 1 无人机通信网络模型

Fig. 1 UAV communication network model

3.2 攻击者模型

上述无人机网络模型中可能存在两类攻击者（见图 2），第一类攻击者来自网络外部，其无法获取到任何合法节点中

用于身份认证和安全通信的密钥；第二类攻击者来自网络内部，其能够获取到部分合法节点中用于身份认证和安全通信的密钥。

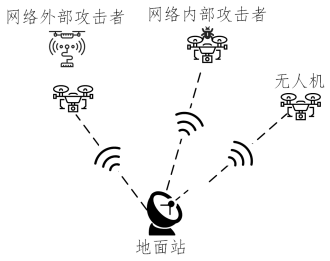

图 2 包含恶意节点的网络模型

Fig. 2 Network model with malicious nodes

本文提出的协议针对 Dolev-Yao 威胁模型中的网络攻击者进行防护，Dolev-Yao 威胁模型是对安全协议进行安全分析常用的威胁模型，其定义的攻击者具有完全监控整个网络通信的能力，与上述网络外部攻击者能力相符。此外，本文还假设攻击者能够控制部分合法无人机节点，即存在内部攻击者，但内部攻击者不包括合法的地面站节点。具体来说，攻击者具备以下能力：

(1)攻击者能够捕获所有无人机和地面站之间通过无线链路传输的数据。

(2)攻击者能够通过无线链路向任何无人机和地面站发送任意数据。

(3)攻击者可以获取到部分无人机中用于安全通信的密钥。

但攻击者不具备控制地面站的能力，不具备猜测随机数的能力，不具备破解密码学原语的能力，即无法在密钥未知的情况下从密文获取明文，无法在密钥未知的情况下为消息生成合法的消息认证码以及无法解决椭圆曲线上的离散对数问题。

4 协议设计

基于上述网络模型和攻击者模型，本文提出的协议旨在达成以下安全目标：

(1)合法的地面站和无人机节点能够实现双向认证，任何外部攻击者无法通过合法节点的认证，任何内部攻击者无法伪装成未被控制的合法节点通过认证。

(2)通过双向认证的合法地面站和无人机节点能够协商出一致的密钥，该密钥不能被完成双向认证的节点之外的攻击者获取。

本文提出的协议分为基于椭圆曲线密码算法的协议 DroneSec 和基于对称密码算法的协议 DroneSec-lite。前者适用于性能较高的平台，其结合了基于椭圆曲线的密码算法和消息认证码算法，在保证相对较低的性能开销的同时保证了前向安全性，同时减少了地面站需要保密存储的密钥数量；后者适用于低性能平台，其仅使用消息认证码算法以及对称加密算法，以保证最低的通信开销和计算开销，但不保证前向安全性。

考虑到多架无人机场景中单播通信和广播通信的需要，协议允许在配置密钥时指定密钥类型，例如通过密钥类型指定配置一对一通信的单播密钥或者配置多对多通信的广播密钥。

协议描述中使用的符号如表 1 所列。

表 1 协议描述使用的符号

Table 1 Notations used in protocol description

符号	含义描述
$\|$	数据连接(将两个数据连接构成一个数据)
G	有限域上椭圆曲线的基点
d_g	地面站私钥(大整数)
P_g	地面站公钥(椭圆曲线点)
d_u	无人机私钥(大整数)
P_u	无人机公钥(椭圆曲线点)
id_u	无人机身份标识
id_g	地面站身份标识
r_g	地面站 ECDH 临时私钥
R_g	地面站 ECDH 临时公钥
r_u	无人机 ECDH 临时私钥
R_u	无人机 ECDH 临时公钥
msg_g	地面站发送的消息
msg_u	无人机发送的消息
ch_u	无人机端生成的用于身份认证的随机字节
$rand()$	生成一个随机数据
$getkey()$	读取一个密钥
$enc()$	$enc(key,data)$表示使用密钥 key 对 $data$ 进行对称加密的加密结果
$dec()$	$dec(key,data)$表示使用密钥 key 对 $data$ 进行解密得到的解密结果
$hmac()$	$hmac(key,data)$表示使用密钥 key 计算 $data$ 的哈希消息认证码的结果

4.1 基于椭圆曲线密码算法的协议

4.1.1 参数初始化

在无人机和地面站设备出厂时需要配置系统的初始化参数，初始化参数包括：

(1) 椭圆曲线运算参数，即选取合适的椭圆曲线群。

(2)无人机身份标识 id_u，无人机私钥 d_u，无人机公钥 $P_u=d_u*G$。

(3)地面站身份标识 id_g，地面站私钥 d_g，地面站公钥 $P_g=d_g*G$。

其中，无人机需要存储自身的身份标识 id_u、公私钥对 d_u 和 P_u，以及其归属的地面站的身份标识 id_g 和公钥 P_g。地面站需要存储自身的身份标识 id_g、公私钥对 d_g 和 P_g，以及其控制的所有无人机的身份标识和公钥。

4.1.2 协议执行流程

该协议流程由地面站发起，整个协议共分为 5 个阶段，协议流程如图 3 所示。

阶段 1 地面站执行如下步骤，发起一次密钥配置。

(1)读取需要配置密钥的无人机的公钥 P_u 以及身份标识 id_u，生成随机数 r_g 并将其作为本次密钥配置使用的 ECDH 临时私钥。

(2)计算 $R_g=r_g*G$，并将其作为 ECDH 临时公钥。

(3)计算认证密钥 $vk=R_g+d_g*P_u$。

(4)生成消息认证码 $mac_g=hmac(vk,id_g\|R_g)$。

(5) 将 $msg_{g1}=(id_g,R_g,mac_g)$ 发送给需要设置密钥的无人机。

阶段 2 无人机接收到 msg_{g1} 后，执行如下步骤：

(1)计算认证密钥 $vk=R_g+d_u*P_g$。

(2)验证 msg_{g1} 中的 id 是否为自身保存的地面站 id，并使用认证密钥 vk 验证 mac_g 的合法性，若验证失败则继续等待合法的 msg_{g1}，等待超时则终止协议执行。

(3)生成随机数 r_u 作为 ECDH 临时私钥。

(4)计算 $R_u=r_u*G$ 作为 ECDH 临时公钥。

(5)计算 $tmpkey=r_u*R_g$。

(6)计算消息认证码 $mac_g=hmac(vk,id_u\|R_u)$。

(7)将 $msg_{u1}=(id_u,R_u,mac_u)$发送给地面站。

阶段 3 地面站接收到 msg_{u1}后,执行如下步骤:

(1)验证 msg_{u1}中的 id 是否为本次会话的无人机 id,并使用 vk 验证消息认证码 mac_u的合法性,若验证失败则续等待 msg_{u1},若等待超时则终止协议执行;通过验证后,地面站已经完成对无人机的身份认证。

(2)计算 $tmpkey=r_g*R_u$。

(3)读取或者生成需要配置给无人机的密钥 key。

(4) 将 key 使用 $tmpkey$ 加密得到 $ekey$。

(5)使用 $tmpkey$ 生成消息认证码 $mac_{g2}=hmac(tmpkey,id_g\|ktype\|ekey)$,其中 $ktype$ 为密钥类型描述信息。

(6) 将 $msg_{g2}=(id_g,ekey,ktype,mac_{g2})$发送给无人机。

阶段 4 无人机接收到 msg_{g2}后,执行如下步骤:

(1)验证 msg_{g2}中的 id 是否为自身保存的地面站 id,并使用 $tmpkey$ 验证消息认证码 mac_{g2}的合法性,若验证失败则继续等待 msg_{g2},若等待超时则终止协议执行;通过验证后,无人机已经完成对地面站的身份认证。

(2)使用 $tmpkey$ 解密 $ekey$ 得到地面站传递的密钥 key,将密钥 key 保存以供后续安全通信使用。

(3)计算 $mac_{u2}=hmac(tmpkey,id_u\|key)$。

(4) 将 $msg_{u2}=(id_u,mac_{u2})$发送给地面站。

阶段 5 地面站接收到 msg_{u2}后,验证其中的 id 是否为本次会话的无人机 id,并使用 $tmpkey$ 验证消息认证码 mac_{u2}的合法性,若验证失败则继续等待 msg_{u2},若等待超时则表示密钥配置可能存在问题;若验证通过则表示协议执行成功。

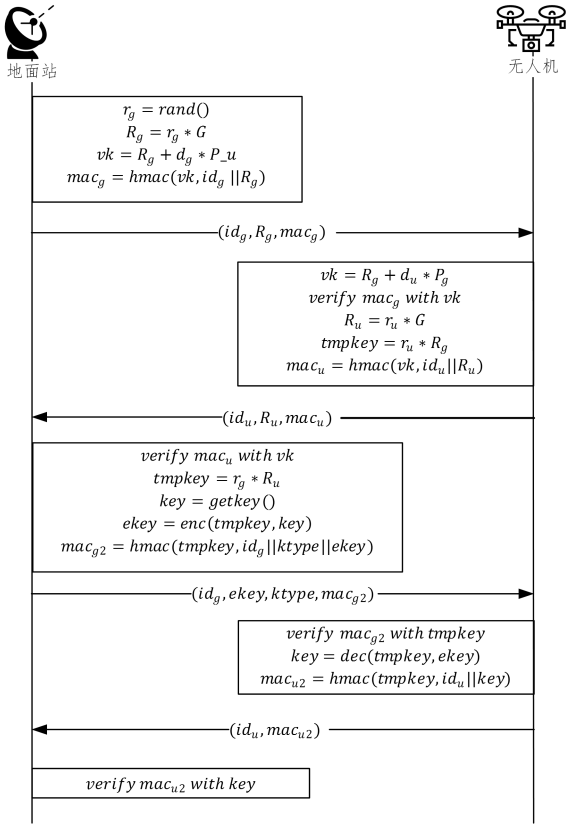

图 3 DroneSec 协议

Fig. 3 DroneSec protocol

4.1.3 无人机和地面站归属关系变更

当一架无人机 U 需要从归属于地面站 A 改为归属于地面站 B 时,地面站 A 需要从其数据库中移除无人机 U 的身份标识以及对应的公钥,地面站 B 需要将无人机 U 的身份标识以及对应的公钥加入到自身数据库中。同时无人机 U 需要将自身存储的地面站 A 的公钥替换为地面站 B 的公钥。

4.2 基于对称密码算法的协议

4.2.1 参数初始化

在无人机和地面站设备出厂时需要配置系统的初始化参数,初始化参数包括:

(1)无人机身份标识 id_u,无人机认证密钥 K;

(2)地面站身份标识 id_g。

每架无人机需要设置不同的身份标识和认证密钥 K。无人机需要存储自身的身份标识 id_u、无人机认证密钥 K 以及其归属的地面站的身份标识 id_g。地面站需要存储自身的身份标识 id_g以及所有归属于自身的无人机的身份标识以及对应的认证密钥。

4.2.2 协议执行流程

该协议流程由地面站发起,整个协议共分为 5 个阶段,协议流程如图 4 所示。

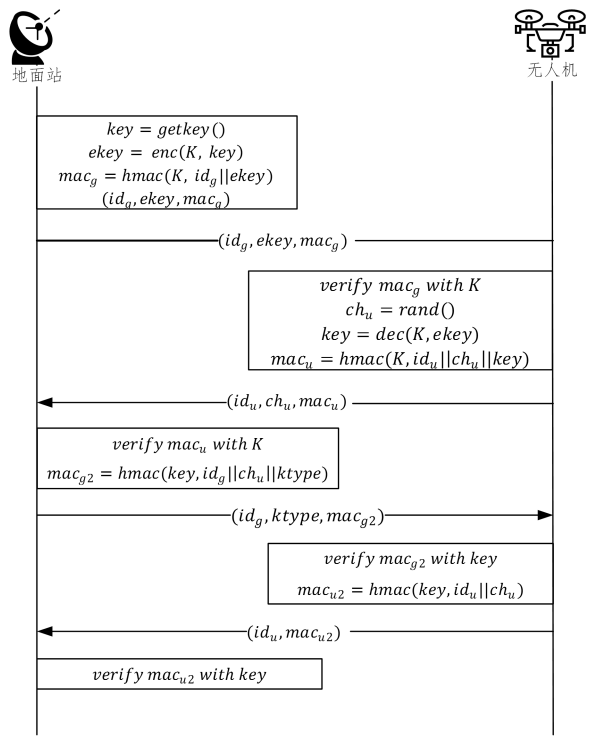

图 4 DroneSec-lite 协议

Fig. 4 DroneSec-lite protocol

阶段 1 地面站执行如下步骤,发起一次密钥配置。

(1)读取或者生成需要配置给无人机的密钥 key,读取需要配置密钥的无人机的认证密钥 K。

(2)使用 K 加密 key 得到 $ekey$。

(3)使用 K 生成消息认证码 $mac_g=hmac(K,id_g\|ekey)$。

(4) 将 $msg_{g1}=(id_g,ekey,mac_g)$发送给目标无人机。

阶段 2 无人机接收到 msg_{g1}后,执行如下步骤:

(1)验证 msg_{g1}中的 id 是否同自身存储的地面站的 id

相同，并使用自身的认证密钥 K 验证消息认证码 mac_g 的合法性，若验证失败则继续等待 msg_{g1}，若等待超时则终止协议执行。

(2)生成随机数 ch_u，长度至少 16 字节。

(3)使用密钥 K 解密 $ekey$ 得到密钥 key。

(4)使用密钥 K 计算消息认证码 $mac_{u1}=hmac(K, id_u \| ch_u \| key)$。

(5)将 $msg_{u1}=(id_u, ch_u, mac_u)$ 发送给地面站。

阶段 3 地面站接收到 msg_{u1} 后，执行如下步骤：

(1)验证 msg_{u1} 中的 id 是否为目标无人机的 id，并使用目标无人机的认证密钥 K 验证消息认证码 mac_u 的合法性，若验证失败则继续等待 msg_{u1}，若等待超时则终止协议执行；通过验证后，地面站已经完成对无人机的身份认证。

(2)使用密钥 key 生成消息认证码 $mac_{g2}=hmac(key, id_u \| ch_u \| ktype)$。

(3)将 $msg_{g2}=(id_g, ktype, mac_{g2})$ 发送给无人机。

阶段 4 无人机接收到 msg_{g2} 后，执行如下步骤：

(1)验证 msg_{g2} 中的 id 是否同自身存储的地面站的 id 相同，并使用密钥 key 验证消息认证码 mac_{g2} 的合法性，若验证失败则继续等待 msg_{g2}，若等待超时则终止协议执行；通过验证后，无人机已经完成对地面站的身份认证。

(2)使用密钥 key 生成消息认证码 $mac_{u2}=hmac(key, id_u \| ch_u)$，保存 key 以供后续安全通信使用。

(3)将 $msg_{u2}=(id_u, mac_{u2})$ 发送给地面站。

阶段 5 地面站接收到 msg_{u2} 后，验证消息中的 id 是否为本次会话的无人机 id，并使用密钥 key 验证消息认证码 mac_{u2} 的合法性，若验证失败则继续等待 msg_{g2}，若等待超时则表示密钥配置可能存在问题，若验证通过则表示协议执行成功。

在具体的协议实现中，Dronesec 和 DroneSec-lite 协议执行流程的各个阶段均需要根据网络情况在因超时而造成协议终止之前进行一定次数的重传(重传当前节点上一阶段的消息)，以应对网络中偶然丢包的影响。

4.2.3 无人机和地面站归属关系变更

当一架无人机 U 需要从归属于地面站 A 改为归属于地面站 B 时，地面站 A 需要从其数据库中移除无人机 U 的身份标识以及对应认证密钥 K。同时，无人机 U 需要生成新的认证密钥 K_{new} 以替换旧的认证密钥 K，并将 K_{new} 和无人机 U 的身份标识存储到地面站 B 的数据库中。

5 安全性分析

协议安全性分析使用了形式化分析工具 ProVerif 来进行。ProVerif 能够验证协议在 Dolev-Yao 威胁模型下的安全性。

ProVerif 采用基于事件的方式来实现对协议正确性和双向身份认证安全性的验证，因此首先需要定义协议关键节点事件，如表 2 所列。accept_drone 事件表示无人机完成对地面站的身份认证，即将发送最后的回复消息；accept_station 事件表示地面站完成对无人机的身份认证，即将发送最后的回复消息；termi_drone 事件表示无人机端协议执行完成；termi_station 事件表示地面站端协议执行完成。

表 2 ProVerif 事件定义

Table 2 Event definition of ProVerif

```
(*参数说明:密钥,密钥类型,是否被劫持*)
event accept_drone(key,bitstring,bool)
event accept_station(key,bitstring,bool)
event termi_drone(key,bitstring,bool)
event termi_station(key,bitstring,bool)
```

根据上述事件定义，使用 ProVerif 的形式化描述语言对第 4 节给出的安全目标进行形式化描述，如表 3 所列，其中每一条 query 语句表示一个需要验证的安全属性。前两条 query 语句验证协议活性(即协议能够正常执行完成)，第三条 query 语句验证无人机对地面站进行身份认证的安全性(即每次无人机完成协议流程时，必定是同合法的地面站完成协议)，第四条 query 语句验证地面站对无人机进行身份认证的安全性(即每次地面站完成协议流程时，必定是同合法的无人机完成协议)。使用 inj-event 描述事件表示要求两个事件是一对一的关系，用于验证协议在面临重放攻击时的安全性。最后一条 query 语句验证地面站配置给无人机的密钥的秘密性。

表 3 安全属性的定义

Table 3 Security attribute definition

```
(*无人机没有被攻击者控制时协议能够正确执行完成*)
query sk:key,ktype:bitstring;event(termi_drone(sk,ktype,false))
query sk:key,ktype:bitstring;event(termi_station(sk,ktype,false))
(*当无人机没有被攻击者控制时,双方能够完成相互认证,就秘钥k达成一致*)
query sk:key,ktype:bitstring;inj-event(termi_drone(sk,ktype,false))==> inj-event(accept_station(sk,ktype,false))
querysk:key,ktype:bitstring;inj-event(termi_station(sk,ktype,false))==> inj-event(accept_drone(sk,ktype,false))
(*攻击者无法获取到秘钥k*)
query attacker(secrecy)
```

为了验证部分无人机被攻击者控制时，攻击者无法伪装成未被控制的无人机或者地面站通过认证，在协议开始前将被控制无人机的私钥输出到公共信道上，并在协议的描述中设置 3 个并行实体，包括地面站、未被控制的无人机以及已被攻击者控制的无人机。表 4 列出了增加了被攻击者控制的无人机节点时 DroneSec 协议的验证主过程，DroneSec-lite 协议的验证主过程与此类似，区别在于 DroneSec-lite 协议的验证过程中公开了被攻击者控制的无人机使用的对称密钥而不是私钥。

表 4 ProVerif 主流程

Table 4 Main process of ProVerif

```
process
    new id_g:bitstring;
    new id_u1:bitstring;
    new id_u2:bitstring;
    let P_g=pk(gs_skey) in
    let P_u1=pk(safe_skey) in
    out(c,P_g);
    out(c,P_u1);
(*公开被控制无人机的私钥 *)
    out(c,compromised_skey);
    (* 正常无人机和被攻击者控制的无人机均能参与协议 *)
    ((! choose_drone)
    |(! station(id_g,gs_skey))
    (* 参数 false 表示未被攻击者控制 *)
    |(! drone(id_u1,safe_skey,P_g,false))
    (* 参数 true 表示被攻击者控制 *)
    |(! drone(id_u2,compromised_skey,P_g,true)))
```

DroneSec 协议的安全性验证结果如表 5 所列。第一条

和第二条安全属性验证结果表示 term_drone 和 term_station 事件能够正常触发,即协议能够正常完成执行,实现身份认证和密钥配置功能,即具备活性;第三条安全属性验证结果表示无人机对地面站的身份认证是安全的,无人机完成协议时能够确认对方是合法地面站,且对方的密钥和密钥类型同自己一致;第四条安全属性的验证结果表示地面站对无人机的身份认证是安全的,地面站完成协议时能够确认对方是合法的无人机,且对方的密钥和密钥类型同自己一致;第五条安全属性的验证结果表示攻击者无法获取协议中双方共享的密钥。

表 5 DroneSec 协议安全性验证结果

Table 5 Security verification result of DroneSec

RESULT not event(termi_drone(sk_3,ktype_3,false)) is false
RESULT not event(termi_station(sk_3,ktype_3,false)) is false
RESULT inj-event(termi_drone(sk_3,ktype_3,false)) ==> inj-event(accept_station(sk_3,ktype_3,false)) is true
RESULT inj-event(termi_station(sk_3,ktype_3,false)) ==> inj-event(accept_drone(sk_3,ktype_3,false)) is true
RESULT not attacker(secrecy[]) is true

DroneSec-lite 协议安全性验证结果如表 6 所列,同与上述 DroneSec 协议验证结果一致,满足安全目标。

表 6 DroneSec-lite 协议安全性验证结果

Table 6 Security verification result of DroneSec-lite

RESULT not event(termi_drone(sk_3,ktype_3,false)) is false
RESULT not event(termi_station(sk_3,ktype_3,false)) is false
RESULT inj-event(termi_drone(sk_3,ktype_3,false)) ==> inj-event(accept_station(sk_3,ktype_3,false)) is true
RESULT inj-event(termi_station(sk_3,ktype_3,false)) ==> inj-event(accept_drone(sk_3,ktype_3,false)) is true
RESULT not attacker(secrecy[]) is true

完整的形式化协议描述和验证过程已开源到 gitee 代码托管平台[1)]。

6 仿真实验和性能分析

本文分别在两种硬件平台下对 DroneSec,DoneSec-lite 进行了仿真实验分析,并使用了 DTLS 协议作为性能基准,实验硬件环境如表 7 和表 8 所列。

表 7 硬件平台 1

Table 7 Hardware platform No. 1

	硬件平台	CPU 平台
地面站端	PC	Intel(R) Core(TM) i5-1035G1
无人机端	PC	Intel(R) Core(TM) i5-1035G1

协议的实现选择了 256 位素域椭圆曲线 secp256r1[25] 用于椭圆曲线运算,选择了 128 位 AES 作为对称加密算法,选择了基于 SHA256 的 HMAC 作为消息认证码算法。协议数据包的发送和接收使用了 UDP 协议。

表 8 硬件平台 2

Table 8 Hardware platform No. 2

	硬件平台	CPU 平台
地面站端	PC	Intel(R) Core(TM) i5-1035G1
无人机端	Raspberry Pi 3B	Quad Core 1.2 GHz Broadcom BCM2837 64bit CPU

DTLS 协议实现使用 TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256 密码套件并启用了双向身份认证功能,其中的椭圆曲线同样使用了 256 位素域椭圆曲线 secp256r1。

图 5 和图 6 分别给出了 3 种协议在两种不同硬件环境下完成一次密钥配置所需的时间(从协议开始执行到协议完成的耗时)。因为密钥配置由地面站发起,所以地面站耗时为整个过程的总耗时。从实验结果可以得出,在高性能计算平台中 DroneSec 协议和 DroneSec-lite 协议的时间开销分别为 DTLS 协议的时间开销的 28.65%和 7%;在较低性能平台中 DroneSec 协议和 DroneSec-lite 协议时间开销分别为 DTLS 协议时间开销的 42.53%和 4.6%。

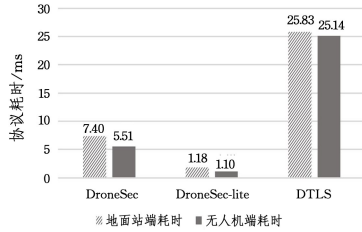

图 5 硬件平台 1 中的时间开销

Fig. 5 Time overhead on hardware platform No. 1

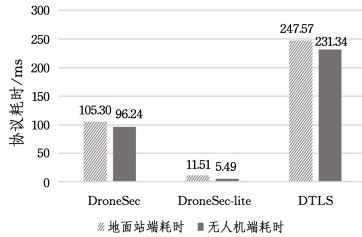

图 6 硬件平台 2 中的时间开销

Fig. 6 Time overhead on hardware platform No. 2

使用 wireshark 捕获协议交互时总的数据发送量,结果如图 7 所示。DroneSec 协议的通信开销为 DTLS 协议通信开销的 7.7%,DroneSec-lite 协议的通信开销为 DTLS 协议通信开销的 4.9%。

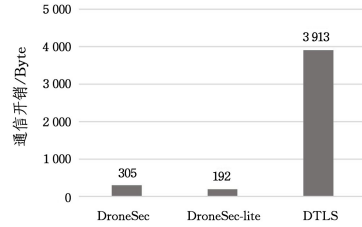

图 7 通信开销

Fig. 7 Communication overhead

本文的协议与现有无人机身份认证和密钥协商的计算性能开销比较通过理论计算的方式进行。本文在 Raspberry Pi 3B 开发板中测试了对协议计算开销有显著影响的运算的典型时间开销,测试方法为执行 1 000 次对应运算取平均值,如表 9 所列。其中,椭圆曲线运算使用了 256 位素域椭圆曲线 secp256r1,对称加密使用了 128 位 AES,消息摘要使用了 SHA256,有限域大整数运算使用长度为 256 位的大整数。

1) https://gitee.com/JanuaryJIAN/drone-sec.git

PUF 时间开销同计算平台的运算性能关系很小，参考了文献[26]中的结果。

表 9 典型密码运算的时间开销

Table 9 Time overhead of typical cryptographic operations

计算类型	描述	典型时间开销/ms
C_{ecmul}	椭圆曲线点乘	4.59
C_{ecadd}	椭圆曲线点加	3.03
C_{enc}	对称加密计算(256 字节)	0.12
C_{hash}	消息摘要计算(256 字节)	0.05
C_{mul}	有限域大整数乘法	0.03
C_{inv}	有限域大整数求逆	0.19
C_{puf}	PUF 计算	0.12

根据表 9 中的结果，表 10 列出了本文提出的协议同现有典型的无人机身份认证和密钥协商协议的计算开销对比，表 11 列出了安全特性对比。DroneSec 协议相比文献[15]、文献[18]以及文献[24]的协议计算开销分别减少了 4.5%，23.14%，69.85%，计算性能有一定的提升；DroneSec-lite 协议相比文献[15]、文献[18]以及文献[24]的协议计算开销分别减少了 98.21%，98.56%，99.44%，计算开销显著降低，更适合低性能计算平台的微型无人机。文献[15]的方案要求在无人机每次起飞前通过安全的信道进行参数配置，以安全管理的复杂性为代价实现了较低的性能开销。本文的协议无须每次起飞前使用安全信道进行参数配置，仅在出厂或者发生密钥泄露后需要使用安全信道进行配置。文献[20]使用了基于 PUF 的认证方案，以数据管理的复杂性以及特殊硬件需求为代价得到了极低的性能开销。本文的协议无须使用 PUF 硬件模块。

表 10 时间开销对比

Table 10 Comparison of time overhead

协议	主要计算开销	时间开销/ms
DroneSec	$6C_{ecmul}+2C_{ecadd}+8C_{hash}+2C_{enc}$	34.24
DroneSec-lite	$8C_{hash}+2C_{enc}$	0.64
文献[15]	$7C_{ecmul}+4C_{hash}+2C_{enc}+C_{ecadd}+C_{inv}+2C_{mul}$	35.86
文献[18]	$7C_{ecmul}+4C_{ecadd}+6C_{hash}$	44.55
文献[20]	$2C_{puf}+6C_{hash}$	0.42
文献[24]	$20C_{ecmul}+6C_{ecadd}+10C_{inv}+22C_{hash}+20C_{mul}$	113.58

表 11 安全特性对比

Table 11 Comparison of security features

协议	双向身份认证	前向安全性	无需安全信道	无需特殊硬件
DroneSec	√	√	√	√
DroneSec-lite	√	×	√	√
文献[15]	√	√	×	√
文献[18]	×	√	√	√
文献[20]	√	×	√	×
文献[24]	√	√	√	√

性能测试代码及仿真实验使用的协议实现已开源到 gitee 代码托管平台。

结束语 现有的无人机认证和密钥协商协议存在安全缺陷或者计算和通信开销大的问题，传统互联网中使用的 DTLS 协议满足无人机网络密钥配置的安全性需求，但性能开销过大且对底层协议有较大依赖。本文设计了针对不同计算性能的无人机系统的轻量、可移植的无人机认证和密钥协商协议 DroneSec 和 DroneSec-lite，实现了安全的双向身份认证和通信密钥配置功能，且不依赖特殊硬件。在保证双向认证和密钥协商的安全性以及密钥管理配置的便利性的情况下，相比现有的无人机认证和密钥协商协议，本文提出的 Dronesec 协议的计算性能开销有一定程度的减小，Dronesec-lite 协议的计算性能开销大幅减小，满足无人机系统通信的安全性和轻量化需求。本文的协议目前仅支持地面站对无人机进行密钥配置，难以处理大规模无人机集群中无人机之间进行相互认证和安全通信的场景。在未来的工作中，将进一步优化和适配无人机集群场景中的通信保护需求。

参 考 文 献

[1] Frost & Sulliva. Chinese Industrial UAV Industry research report[EB/OL]. (2020-02-14) [2021-05-28]. http://www.frostchina.com/?p=16157.

[2] HE D J, DU X, QIAO Y R, et al. A Survey on Cyber Security of Unmanned Aerial Vehicles[J]. Chinese Journal of Computers, 2019, 42(5): 1076-1094.

[3] SCHUMANN J, MOOSBRUGGER P, ROZIER K Y. R2U2: monitoring and diagnosis of security threats for unmanned aerial systems[C]// Runtime Verification. Springer, 2015: 233-249.

[4] HE D, CHAN S, GUIZANI M. Communication security of unmanned aerial vehicles[J]. IEEE Wireless Communications, 2016, 24(4): 134-139.

[5] YAACOUB J P, NOURA H, SALMAN O, et al. Security analysis of drones systems: Attacks, limitations, and recommendations [J/OL]. Internet of Things, 2020, 11. https://doi.org/10.1016/j.iot.2020.100218.

[6] Internet Engineering Task Force(IETF). RFC 6347: Datagram transport layer security version 1.2[EB/OL]. [2021-05-28]. https://datatracker.ietf.org/doc/html/rfc6347.

[7] Internet Engineering Task Force(IETF). The Transport Layer Security(TLS) Protocol Version 1.3 [EB/OL]. [2021-05-28]. https://datatracker.ietf.org/doc/html/rfc8446.

[8] BLANCHET B. Modeling and verifying security protocols with the applied pi calculus and ProVerif[J]. Foundations and Trends in Privacy and Security. 2016, 1(1/2): 1-135.

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

[10] CHOUDHARY G, SHARMA V, YOU I. Sustainable and secure trajectories for the military Internet of Drones(IoD) through an efficient Medium Access Control (MAC) protocol[J/OL]. Computers & Electrical Engineering, 2019, 74: 59-73. https://doi.org/10.1016/j.compeleceng.2019.01.007.

[11] LIU P P. Research on Key Technologies of High Secure Transmission in UAV Communication Networks[D]. Nanchang: Nanchang University, 2020.

[12] SUN X,NG D W,DING Z,et al. Physical layer security in UAV systems:Challenges and opportunities[J]. IEEE Wireless Communications,2019,26(5):40-47.

[13] SHOUFAN A,ALNOON H,BAEK J. Secure communication in civil drones[C]// International Conference on Information Systems Security and Privacy. Springer,2015:177-195.

[14] YOON K,PARK D,YIM Y,et al. Security authentication system using encrypted channel on uav network[C]// 2017 First IEEE International Conference on Robotic Computing(IRC). IEEE,2017:393-398.

[15] ZHU H,ZHANG Y P,YU P,et al. Key Management and Authentication Protocol for UAV Network[J]. Advanced Engineering Sciences,2019,51(3):158-166.

[16] ALLOUCH A,CHEIKHROUHOU O,KOUBÂA A,et al. MAVSec:Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems[C]// 2019 15th International Wireless Communications & Mobile Computing Conference(IWCMC). IEEE,2019:621-628.

[17] ZHANG L H,WANG S,ZHOU H,et al. Secure communication scheme of unmanned aerial vehicle system based on MAVLink protocol[J]. Journal of Computer Applications,2020,40(8):2286-2292.

[18] LI S N. Research on Security of UAV communication Protocol [D]. Beijing:Beijing Jiaotong University,2020.

[19] CORTEZ D M,SISON A M,MEDINA R P. Cryptographic Randomness Test of the Modified Hashing Function of SHA256 to Address Length Extension Attack[C]// Proceedings of the 2020 8th International Conference on Communications and Broadband Networking. 2020:24-28.

[20] ALLADI T,BANSAL G,CHAMOLA V,et al. SecAuthUAV:A Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication[J]. IEEE Transactions on Vehicular Technology,2020,69(12):15068-15077.

[21] SUN J,WANG W,KOU L,et al. A data authentication scheme for UAV ad hoc network communication[J]. The Journal of Supercomputing,2020,76(6):4041-4056.

[22] CHO G,CHO J,HYUN S,et al. SENTINEL:A secure and efficient authentication framework for unmanned aerial vehicles[J/OL]. Applied Sciences,2020,10(9). https://doi.org/10.3390/app10093149.

[23] TENG L,JIANFENG M,PENGBIN F,et al. Lightweight security authentication mechanism towards uav networks[C]// 2019 International Conference on Networking and Network Applications(NaNA). IEEE,2019:379-384.

[24] KO Y,KIM J,DUGUMA D G,et al. Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone [J/OL]. Sensors, 2021, 21(6). https://doi.org/10.3390/s21062057.

[25] Standard curve database. secp256r1 [EB/OL]. [2021-05-28]. https://neuromancer.sk/std/secg/secp256r1.

[26] GOPE P. PMAKE:Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid[J]. Computer Communications,2020,152:338-344.

JIAN Qi-rui, born in 1998, postgraduate. His main research interests include trusted computing for embedded system and security protocol.

CHEN Ze-mao, born in 1975, Ph.D, professor, Ph.D supervisor. His main research interests include cyber physical system security, trusted computing and so on.

(责任编辑:喻藜)