无人机网络轻量级安全认证与通信机制研究

作者姓名 孟悦

学校导师姓名、职称 马建峰

企业导师姓名、职称 李亚晖

申请学位类别 工程硕士

万方数据

学校代码 10701　　学　号
分 类 号 TP309　　密　级 公开

西安电子科技大学

硕士学位论文

无人机网络轻量级安全认证与通信机制研究

作者姓名：孟悦

领　　域：计算机技术

学位类别：工程硕士

学校导师姓名、职称：马建峰 教授

企业导师姓名、职称：李亚晖 研究员

学　　院：计算机科学与技术学院

提交日期：2019 年 6 月

万方数据

Research on Lightweight Security Authentication and Communication Mechanism of UAV Network

A thesis submitted to

XIDIAN UNIVERSITY

in partial fulfillment of the requirements

for the degree of Master

in Computer Technology

By

Meng Yue

Supervisor: Ma Jianfeng Title: Professor

Supervisor: Li Yahui Title: Research Fellow

June 2019

万方数据

西安电子科技大学
学位论文独创性（或创新性）声明

秉承学校严谨的学风和优良的科学道德，本人声明所呈交的论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果；也不包含为获得西安电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同事对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

学位论文若有不实之处，本人承担一切法律责任。

本人签名：_____　　日　　期：_____

西安电子科技大学
关于论文使用授权的说明

本人完全了解西安电子科技大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权属于西安电子科技大学。学校有权保留送交论文的复印件，允许查阅、借阅论文；学校可以公布论文的全部或部分内容，允许采用影印、缩印或其它复制手段保存论文。同时本人保证，结合学位论文研究成果完成的论文、发明专利等成果，署名单位为西安电子科技大学。

保密的学位论文在___年解密后适用本授权书。

本人签名：_____　　导师签名：_____

日　　期：_____　　日　　期：_____

万方数据

摘要

无人机是利用无线电遥控设备等操纵的不载人飞机，具有体积小、灵活易于操作等优势。利用多架无人机之间的相互通信和协同，可以扩大对环境态势的感知并完成较为复杂的任务，如抢险救灾、紧急救援和遥测遥感等。无人机网络允许网络中的无人机节点通过无线链路进行通信，实现信息的共享，并具有动态拓扑、灵活接入的特点。与此同时，受限于载荷、计算节点物理资源、外部环境等因素的影响，无人机网络通信的质量和安全性也受到极大挑战。无人机网络在进行应急救援、环境检测和协同作战等任务时，会受到伪造攻击、中间人攻击、重放攻击、信息窃听或篡改等攻击威胁。为缓解以上安全威胁，建立有效的身份认证及安全通信机制迫在眉睫。

现有无人机网络的身份认证及安全通信机制存在以下问题。首先，由于无人机网络节点计算和存储资源有限，传统基于 RSA 公钥体制的身份认证方式需要较长密钥和较大运算量，不能满足无人机网络的轻量级认证需求。其次，由于消息传输过程中丢包和环境干扰，可能导致节点间会话密钥计算不一致的问题。第三，无人机网络在外部环境干扰下的高丢包率，导致加密通信过程的健壮性不足，在数据加密传输过程中，存在由丢包所导致的密文无法正常解密问题。

针对以上问题，本文提出了适用于无人机网络的轻量级安全认证方案和通信方案，用以提升无人机网络数据通信的安全性和健壮性。具体包括：

（1）设计并实现了基于椭圆曲线 ECC（Elliptic Curve Cryptography）体制的身份认证方案。使用 ECC 数字证书作为合法无人机的身份证明，使用基于椭圆曲线的 ECDSA（Elliptic Curve Digital Signature Algorithm）签名算法对节点身份进行签名验证，同时使用 ECDH 密钥交换算法生成通信所需要的会话密钥，从而有效减小密钥长度和运算量。对接入节点身份认证后所生成的会话密钥进行密钥一致性检验，解决节点间会话密钥不一致问题。

（2）基于分组密码 SM4 算法的流密码运行模式，设计并改进了 CTR（Counter mode）模式的无人机高效会话加解密，并基于所提出的 CTR 模式加解密方案实现了支持高实时性、容忍密文无序的安全通信方法。

（3）在实际的多节点无人机网络环境下，以 VxWorks6.9 嵌入式开发板作为载荷计算模块，测试所实现的身份认证方案和安全通信方案的性能和安全性。实验结果表明，所实现的轻量级身份认证方案相比当前基于 RSA 数字证书的认证方案，能够以较短密钥和较小计算量实现较高的安全性；所实现的轻量级安全通信方案加解密速度比传统的 SM4_CTR 算法提升了 7.7%，与 ChaCha20 流加密算法相比更能容忍丢包。

万方数据

关 键 词：无人机网络，身份认证，安全通信，椭圆曲线

万方数据

ABSTRACT

The UAV(Unmanned Aerial Vehicle) is a non-manned aircraft that is operated by radio remote control equipment, etc., and has the advantages of small size, flexibility, and easy operation. By using the mutual communication and coordination among multiple UAVs, the perception of the environmental situation can be expanded and more complex tasks such as rescue and disaster relief, emergency rescue and telemetry remote sensing can be completed. The UAV network allows the UAV nodes in the network to communicate over the wireless link, enabling information sharing, and features dynamic topology and flexible access. At the same time, the quality and security of UAV network communication are also greatly challenged due to factors such as load, computing node physical resources, and external environment. UAV networks are subject to attacks such as forgery attacks, man-in-the-middle attacks, replay attacks, information disclosure, or tampering when performing tasks such as emergency rescue, environmental detection, and coordinated operations. In order to alleviate the above security threats, it is extremely urgent to establish an effective identity authentication and secure communication mechanism.

The following problems exist in the identity authentication and secure communication mechanisms of existing UAV networks. Firstly, due to the limited computing and storage resources of the UAV network node, the traditional RSA public key system based authentication method requires a long key and a large amount of computation, which cannot meet the lightweight authentication requirements of the UAV network. Secondly, due to packet loss and environmental interference during message transmission, the problem of inconsistent session key calculation between nodes may be caused. Third, the high packet loss rate of the UAV network under external environment interference leads to insufficient robustness of the encrypted communication process. In the process of data encryption transmission, there is a problem that the ciphertext caused by packet loss cannot be decrypted normally.

In view of the above problems, this thesis proposes a lightweight security authentication scheme and communication scheme suitable for the UAV network to improve the security and robustness of the data communication of the UAV network. Specifically include:

万方数据

(1) Design and implement an identity authentication scheme based on elliptic curve ECC system. Using the ECC digital certificate as the identity proof of the legal UAV, the EDSSA signature algorithm based on the elliptic curve is used to verify the identity of the node, and the ECDH key exchange algorithm is used to generate the session key required for communication, thereby effectively reducing the key. Length and amount of operation. Key consistency check is performed on the session key generated after the identity authentication of the access node, and the problem of inconsistent session key between nodes is solved.

(2) Based on the stream cipher operation mode of block cipher SM4 algorithm, the CTR mode UAV efficient session encryption and decryption is designed and improved, and based on the proposed CTR mode encryption and decryption scheme, it supports high real-time and tolerant ciphertext. Ordered secure communication method.

(3) In the actual multi-node UAV network environment, the VxWorks6.9 embedded development board is used as the load calculation module to test the performance and security of the implemented identity authentication scheme and secure communication scheme. The experimental results show that the implemented lightweight authentication scheme can achieve higher security with shorter keys and smaller calculations than the current RSA digital certificate-based authentication scheme. Lightweight secure communication is realized. The scheme encryption and decryption speed is 7.7% higher than the traditional SM4_CTR algorithm, and it is more tolerant of packet loss than the ChaCha20 stream encryption algorithm.

Keywords: airborne network, identity authentication, secure communication, elliptic curve

万方数据

插图索引

万方数据

万方数据

表格索引

万方数据

万方数据

符号对照表

符号	符号名称
M	明文消息空间
C	密文消息空间
K	加解密密钥
K_i	无人机 i 的加密密钥
E_{k_i}	无人机 i 的加密操作
D_{k_i}	无人机 i 的解密操作
P	椭圆曲线基点
Q	椭圆曲线上一点
O	椭圆曲线零点
Z_p	有限域
$\Im$	签名集合
V	认证结果值域

万方数据

万方数据

缩略语对照表

缩略语	英文全称	中文对照
AES	Advanced Encryption Standard	高级加密标准
CA	Certificate Authority	认证中心
CTR	Counter mode	计数器模式
DL	Discrete logarithm	离散对数
DLP	Discrete Logarithm Problem	离散对数问题
ECC	Elliptic curve cryptography	椭圆曲线密码学
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
ECDH	Elliptic-curve Diffie–Hellman	基于椭圆曲线的 DH 密钥交换算法
EC	Elliptic Curve	椭圆曲线
ECDLP	Elliptic curve Discrete Logarithm Problem	椭圆曲线离散对数问题
GPS	Global Positioning System	全球定位系统
GCM	Galois/Counter Mode	计数器模式
HMAC	Keyed-hash Message Authentication Code	密钥散列消息认证码
IF	Integer Factorization	整数分解
KDC	Key Distribution Center	密钥分配中心
MD5	Message-Digest Algorithm	MD5 消息摘要算法
MAC	Message Authentication Code	消息认证码
PKCS	Public Key Cryptography Standards	公钥加密标准
SSL	Secure Sockets Laye	安全套接字
SHA	Secure Hash Algorithm	安全散列算法
UDP	User Datagram Protocol	用户数据报协议
UAV	Unmanned Aerial Vehicle	无人驾驶飞机

万方数据

万方数据

目录

万方数据

万方数据

第一章　绪论

1.1 研究背景与意义

无人驾驶飞机是利用无线电遥控设备和自备程序控制装置操纵的不载人飞机，简称为“无人机”。由于无人机具有体积小、造价低、使用便利、作战环境要求低、战场生存能力较强、灵活且易于操作、无需承担人身伤害或死亡的风险等优势，在政府、能源、军工、民生等领域具有广泛的应用。随着网络化通信技术的发展，无人机的作战模式也在不断发展，但是单架无人机受到有限探测距离、有限载荷、有限飞行时间等因素的限制，难以完成较为复杂的任务。为了扩大对环境态势的感知与无人机整体效能的发挥，需要多架无人机之间协同作战，彼此之间相互通信，实现信息共享，完成对复杂任务的协同分配，提高无人机的生存能力和整体作战效能[1]。

无人机网络由多个可以相互通信的无人机组成，相较于单个无人机系统，可以满足不同任务的作战需求。无人机网络内每个无人机节点既可以执行不同类型的任务，也可以一起执行相同的任务，并可以针对不同的任务需求部署不同的网络拓扑结构来应对目标的变化，从而扩大任务执行的覆盖面积。无人机之间通过相互通信来保持联系并进行灵活配置，这就是无人机网络的优势所在。无人机网络具有动态拓扑、灵活接入和机动性大等特点，在一些通信基础设施受限的环境下具有良好的应用前景，包括民用、军用、商业和政府部门有关领域的应用[2][3][4][5][6]，特别是民用和军事领域[7]，具体的应用包括了紧急救援[8]、环境监控[9]、协同作战[10]、抢险救灾、遥测遥感、交通巡捡、军事国防等。

尽管无人机网络在现实生活中具有如此广泛的应用，为生活中的方方面面都提供了应用支持。在带来便利性的同时，针对无人机网络的攻击也越来越多，如伪造、模仿、操纵和拦截等。2011 年，伊朗部队俘获了一架无人驾驶的美国 RQ-170 飞行器引起了无人机网络中针对无人机的安全问题[11]。2016 年，Nils Rodday 利用专业无人机的漏洞来破坏系统并成功控制了无人机系统[12]。同样在民用领域，一些不法分子利用无人机走私毒品[13][14]。由以上案例可知，针对无人机网络所进行的网络攻击，将会造成不可估量的危害。因此，在有效利用无人机网络之前还有许多安全问题需要解决。

一方面，无人机远程接入无人机网络时，保证所接入网络无人机身份的合法性与安全性具有关键的意义。当完成一项较为复杂的任务时，需要多个无人机组成无人机通信系统协同地执行任务，而无人机网络在地面指挥中心控制下，彼此通过无线链路进行通信。这时每一个无人机可以被看作网络内的一个节点，此时的无人机网络是高度变化的，将持续有无人机加入或退出通信网络。因此，无人机网络具有动态变化的

万方数据

拓扑结构[15]。当新的节点加入时，必须保证所加入网络的节点身份合法真实。若不使用任何安全机制攻击者便可以轻松攻击无人机网络中的任何节点，为了提高网络节点的安全性，必须提供一种机制来保证无人机网络接入的安全性，对所有接入无人机网络的设备身份进行验证，这也是保护无人机网络数据真实性的关键措施，是许多安全服务的前提。

另一方面，通信安全对于无人机任务执行至关重要。2009 年，伊拉克武装分子使用 26 美元的 COTS 软件成功拦截了美国“捕食者”无人机的实时视频信号，为他们提供了逃避或监视美国军事行动所需的信息[16]。同年，恐怖组织使用 SkyGrabber[17]捕获了一架未加密的无人机视频，从美国无人机传输到美国军用卫星。由于无人机网络在军事以及民用领域的应用，通常会携带对手可能试图掌握的敏感信息，遭受各类安全攻击，如通过发起 GPS 欺骗攻击或 WiFi 攻击捕获有针对性的无人机并获取其需要的信息。此外，由于无人机网络具有动态拓扑和灵活接入的特点，极易受到恶劣天气等外部环境干扰和通信链路不稳定等因素的影响，造成因传输信息丢包而无法正常解析的安全缺陷。

因此，在身份认证的基础上，为了保证通信双方通信链路的健壮性和传输信息的安全性，必须开展安全通信技术研究。基于传统 RSA 算法的认证方案[18]和基于传统加密算法的通信方案，受到无人机网络中设备物理资源和计算能力[19][20][21]的限制，不能满足无人机网络的轻量级需求。同时无人机网络中存在着因外部环境干扰导致网络丢包而造成密文无法正常解析的问题。如何针对这些问题提出更有效的身份认证和安全通信方案，是当前无人机网络安全领域要解决的核心问题。

1.2 国内外研究现状

无人机网络在紧急救援、环境监控、抢险救灾、交通巡捡、遥测遥感、军事国防等方面具有深远的应用前景，已吸引越来越多学术界和工业界的研究关注。针对无人机网络设备间身份认证和通信中存在的安全问题，相关研究人员已经进行了相关的研究。

1.2.1 无人机网络身份认证

无人机网络具有物联网的一些特性，远程授权用户可以访问可靠的传感器节点以获得数据，甚至允许向网络中的节点发送命令。因此，在关注无人机网络的安全接入时，需要考虑到两个方面的问题，一方面只有合法的无人机才能接入网络来获取数据；另一方面，加入到网络中的各个无人机身份必须经过安全验证。为了实现上述安全接入要求，无人机网络节点间的相互安全认证协议必须被实现。

万方数据

Watro 等人[22]提出了一种基于难处理数学问题的 RSA 算法和 Diffie-Hellman 密钥交换算法计算来加密密钥的用户认证协议，但是该协议却非常容易遭受到传感器节点的影响，因此对任意伪装成传感器的用户来说是毫无抵抗力的。之后，Wang 等人首先提出一种基于散列的用户认证方案[23]，这种方案比较简单、轻量级和动态。但 Das[24]和 Tseng 等人[25]指出 Watro 和 Wong 的用户身份验证方法都容易受到盗窃-验证、重放和伪造攻击，因此 Das 提出了一种双因素用户认证方法，此方法旨在防止上述被盗验证器、重放和伪造攻击。Tseng 等进一步指出，Wong 的方法容易被盗密码，并且 Wong 的方法阻止了用户自由地改变密码。因此，Tseng 等提出了一种增强的用户认证方法，旨在防止各种攻击，减少密码被盗的漏洞。Khan 等[26][27]和 Chen 等[28]发现 Das 的双因素方法需要增加额外的安全措施。因而 Chen 等提出了一种更安全和更健壮的双因素用户身份验证。不幸的是，我们发现陈等人的提案未能提供用于更新用户密码的安全方法，并且易受内部攻击问题的影响。Yeh[29]等人提出一种基于椭圆曲线(ECC)算法的用户认证方案和密钥管理协议。Xu[30]和 Song[31]等人基于用户之间的相互认证提出了 Deffie–Hellman 密钥交换算法。

因为现有已经被提出的身份认证协议在具体实现时需要耗费较大的系统资源，将会导致无人机网络通信质量的下降，造成传输信息不能够及时送达甚至产生丢包问题，这些问题将会在执行一些紧急任务时产生严重的后果。同时，网络中相互通信的双方无人机还存在着会话密钥不一致性的问题。考虑到无人机网络计算节点物理资源有限的特点，提出一种轻量级的身份认证方案对于无人机网络的安全应用具有重要的意义。

1.2.2 无人机网络数据通信

无人机网络中节点通信在各个方向上广播，因此网络范围内的任何接收器都能够收集通信，为了防止发现战术信息，加密是必要的安全需求。由于信息捕获的简易性和通信的开放性，群体特别容易受到攻击，如果没有安全机制，黑客可以轻松捕获用户的私人或敏感个人信息。因此，在身份认证的基础上，为了保证通信双方通信链路的健壮性和传输信息的安全，必须开展安全通信技术研究。Gupta[32]等人为无人机网络引入了一系列通信和网络要求，这些要求包括诸如动态联网、无线通信质量、飞行控制等特征。更具体地说，要考虑动态网络要求，2010 年 Li 等人[33]提出了一种使用小型无人机通信的协作通信系统。

无人机网络的主要安全机制侧重于通过密码学保障无人机网络节点间通信过程中的隐私性、机密性和数据完整性。按照密钥的特征不同，加密方法可以分为基于对称密码的加解密和基于非对称密码的加解密。非对称加密，就是使用已经公开的密钥进行加密并使用秘密的密钥进行解密的方法，即使用不同的密钥进行加密和解密运算，这将在每个节点之间创建不同的通信信道。对称加密更快，适用于当前的无人机网络

万方数据

架构，在该架构中，每个通信节点将预加载相同的钥匙，并使用相同的密钥加密和解密。而按照加密方式的不同，加密方法又可以分为流加密和分组加密，目前常见的对称加密算法都属于分组加密，如 AES（Advanced Encryption Standard）、DES（Data Encryption Standard）和 SM4 等。

AES 和 SM4 是两个非常典型的对称加密算法[34]，众所周知，AES 用途广泛[35]，具有四种不同的模式适用于不同场景下的加密操作。近年来，随着计算机技术的发展，AES 的安全性已不能满足无人机网络对于通信的安全需求。SM4 算法是国密分组算法，是为低功耗芯片应用领域所设计的加密算法。该算法对于分组和密钥的长度都有具体的要求，均为 128 比特。SM4 算法的加密和解密算法结构一致，在实现时只需要实现加密算法。SM4 算法的优势在于其算法设计简单，结构有特点，安全并且高效，符合轻量级安全通信机制的要求。

用于加密的 ChaCha20 流加密算法和用于加密的 Poly1305 身份验证已成为业界的热门选择[36]。2014 年，谷歌在其 Android 手机上用 ChaCha20-Poly1305 取代了 GCM，认为它更安全，并且显示它在软件实现方面要快得多[37]。ChaCha20-Poly1305 通过最小化硬件密集型操作（如矩阵乘法），在通用计算机体系结构上快速设计软件[38][38]。虽然 ChaCha20-Poly1305 的速度比较快，但是对于高动态战场中通信断续的数据传输导致的丢包问题，这种方法的效果却很差，不能解决无人机网络中丢包的问题。

针对无人机网络，现有的安全通信加解密算法并不能满足无人机网络中轻量级的性能和安全需求。一方面，如果加解密的时间过长，会造成系统或网络实时性能的下降，造成无人机来不及接收信息而导致严重的后果。另一方面，若所设计的通信方案不能够容忍网络丢包，会造成密文无法正常解析，从而无法获得正确的明文信息。因此，开展支持传输健壮性的轻量级安全通信技术研究对于无人机网络的通信安全具有重大的意义。

1.3 本文研究内容及创新点

无人机网络是一种开放式的网络系统，具有动态拓扑、灵活接入和网络节点计算和物理资源有限的特点，极易受到恶劣天气等外部环境干扰和通信链路不稳定等因素的影响。在以上特点约束下，传统身份认证机制和安全通信机制存在以下局限性：（1）为了实现认证过程的高安全性，传统身份认证方案的开销大，如基于 RSA 公钥体制和 Diffie-Hellman 密钥协商的用户认证协议，对于无人机网络来说会消耗网络较多计算和存储资源。（2）由于消息传输过程中丢包或计算错误等问题可能造成无人机间会话密钥不一致问题，目前没有较好的解决方法。（3）无人机通信网络的高丢包率对密文传输质量和传输效率造成严重影响，可能造成接收端密文无法解密。

万方数据

针对以上问题，本文提出并实现了：

（1）基于椭圆曲线 ECC 算法的无人机网络身份认证方案。使用 ECC 数字证书作为合法无人机的身份证明，使用计算量和资源消耗更小的基于椭圆曲线的 ECDSA 签名算法对节点身份进行签名验证，并使用 ECDH 密钥交换算法生成通信所需要的会话密钥。对接入的无人机节点身份认证通过后生成的会话密钥进行了密钥一致性检验，解决节点间会话密钥不一致问题。

（2）基于对称分组密码 SM4 算法的流密码运行模式（CTR 模式），设计并改进了 CTR 模式的无人机高效会话加密传输，并基于所提出的 CTR 模式设计和实现了支持高实时性、容忍密文无序的安全通信方法。同时使用 HMAC（Hash-based Message Authentication Code）算法保证传输消息的完整性。

本文所提出的无人机网络身份认证和安全通信方案，其创新性主要包括：

（1）实现的基于 ECC 算法的身份认证方案实现了无人机节点间的高效双向身份认证，与当前主要使用 RSA 数字证书的无人机身份认证方法相比，能够以较短的密钥长度和较小的计算量，实现较高的安全性。

（2）实现的无人机会话密钥一致性检验方法，解决了因密钥计算错误或消息传输过程中丢包造成的协商密钥不一致问题。

（3）实现的无人机网络节点间高健壮性安全通信方法，能够容忍因为环境干扰导致的密文无序、非实时数据丢失导致的密文无法正常解密，与传统的 SM4_CTR 算法相比加解密速度提升了 7.7%，与 ChaCha20 流加密算法相比更能容忍丢包。

1.4 论文的组织结构

全文分为五个章节，首先详细介绍了无人机网络的安全需求，主要从安全身份认证和安全通信两个方面来展开。其次，详细介绍了所设计的轻量级身份认证和通信方案。最后对本文进行了总结和展望。

第一章：介绍了本文的研究背景和研究意义，对国内外相关的研究现状进行分析和总结，并提出本文创新点，介绍论文的组织结构。

第二章：与本文相关的认证和通信安全机制及理论知识进行了详细介绍，并研究分析了现有机制的不足之处。

第三章：介绍了无人机网络身份认证的安全需求和攻击者模型，并提出使用基于 ECC 算法的认证方案对无人机身份进行验证；同时，介绍了实验测试时的硬件环境；最后对所提出的认证方案进行了安全性分析，对认证方案进行了功能和性能方面的测试，，并对实验测试结果进行了分析。

第四章：介绍了无人机网络通信的安全需求和攻击者模型，并阐述了针对这些需

万方数据

求所设计和实现的轻量级安全通信方案；同时对所设计的通信方案进行了安全性分析，并在实际实验环境下对通信方案进行了功能和性能方面的测试，对实验测试的结果进行了分析。

第五章：总结本文针对无人机网络所提出的安全身份认证和安全通信机制方案的主要内容，并展望未来工作方向。

万方数据

第二章 相关安全机制与技术

2.1 密码体制

密码体制是指任何一个需要安全机制的网络或系统所需要的基本工作方式，通常其包含了不同的加解密算法以及用于加解密所需的密钥。加密和解密的算法是公开的，只有加解密所使用的密钥是非公开的。因此，可以说密码体制的安全性是取决于密钥保存的私密性。

通常一个保密系统包括$(M,C,K_1,K_2,E_{K1},D_{K2})$六个元素，其中：

M 是明文消息空间。

C 是密文消息空间。

K_1 和 K_2 是密钥空间，在单钥体制下 $K_1=K_2=K$，此时密钥 $k\in K$ 需要经过安全的密钥信道由发送方传送给接收方。

$E_{k1}\in E$， $m\to c=E_{k1}(m)$，其中 $k_1\in K_1$， $m\in M$， $c\in C$，由加密器完成。

$D_{k2}\in D$， $c\to m=D_{k2}(c)$，其中 $k_2\in K_2$， $\mathrm{m}\in M$， $c\in C$，由解密器完成。

因此，若按照加密密钥是否可以公开，可以把密码体制分为对称密码体制和非对称密码体制两大类。对称加密体制相比较于非对称加密而言速度更快、计算开销更低，但安全性却不如非对称加密高。

2.1.1 非对称密码体制

1976 年[39]提出的非对称密码体制，其原理是使用不同的加解密密钥进行加密和解密运算，即每个人都将公钥公开，并将私钥保存，这是第一个在不使用事先共享密钥的情况下，在未受保护的信道上建立共享密钥的实用方法。该密码体制的优势在于不怕通信线路被窃听，即便公钥丢失也不会产生严重的后果。基本原理如图 2.1 所示。

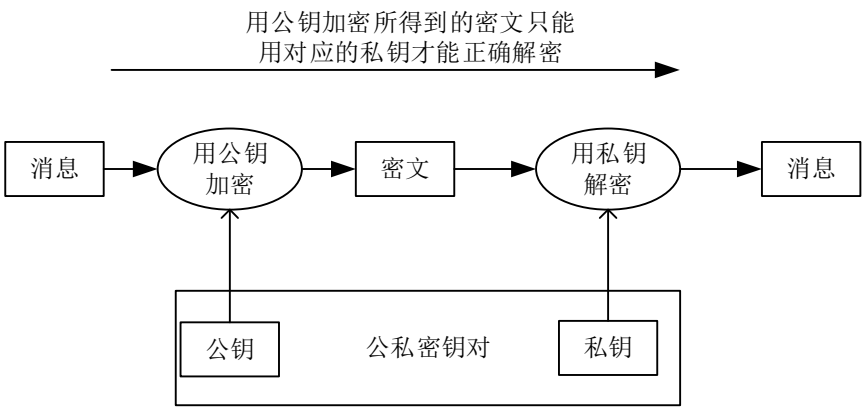

图2.1 公钥密码体制加解密原理

万方数据

今天使用的公钥密码体制可以根据为其安全性提供基础的硬性基础数学问题进行分类：

（1）IF（Integer Factorization）整数分解方案，它们的安全性基于整数分解问题的难处理性。若已知大素数 p 和 q，求 $n = p*q$ 是非常容易计算的，但若根据 n 求 p 和 q，却需要花大量的时间。基于该数学难题的加密算法包括 RSA[40]和 Rabin[41]等。

（2）DL（Discrete Logarithm）离散对数方案，其安全性基于有限域中离散对数问题的难处理性。这些例子包括 ElGamal[42]，Schnorr[43]，DSA[44]和 Nyberg-Rueppel[45][46]。

（3）EC（Elliptic Curve）椭圆曲线方案，它们的安全性是基于椭圆曲线离散对数问题的难处理性。

由于 ECDLP（Elliptic curve Discrete Logarithm Problem）椭圆曲线离散对数问题似乎比 DLP（Discrete Logarithm Problem）离散对数问题明显更难，基于椭圆曲线的密钥每比特所支持的安全性比传统基于其他数学难题的密钥更高。因此，与旧离散对数密码系统相比，ECC 算法能够以较小参数优势包括更快的计算速度、更短的密钥长度和证书实现相同的安全级别，而这些优势在处理能力、存储空间、带宽或功耗受到限制的环境中尤为重要。

2.1.2 椭圆曲线加密体制

椭圆曲线密码系统是基于椭圆曲线离散对数问题（ECDLP）的，其具体原理是，已知椭圆曲线 $E\left(F_q\right)$、阶为 n 的点 $P \in E\left(F_q\right)$ 及 $Q \in \langle P \rangle$（基点 P 生成的循环群），椭圆曲线离散对数问题是指指定 $l \in [0, n-1]$，使得 $Q = [l]P$ 成立的数学问题。

椭圆曲线离散对数问题关系到椭圆曲线密码系统的安全，因此为了确保其安全性，必须选择安全的椭圆曲线。通常，椭圆曲线可以用以下的方程表示：

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{2-1}$$

其中 a，b，c，d，e 为定义在有限域上的方程组系数。在密码学中用到的椭圆曲线方程一般限定为:

$$y^2 = x^3 + ax^2 + b \tag{2-2}$$

其中 $4a^3 + 27b^2 \neq 0$，也即这里的二次项系数为 0。在这里取曲线参数 $a = -4$, $b = 16$，绘制 $y^2 = x^3 - 4x^2 + 16$ 这条椭圆曲线的图像，如图 2.2 所示。

万方数据

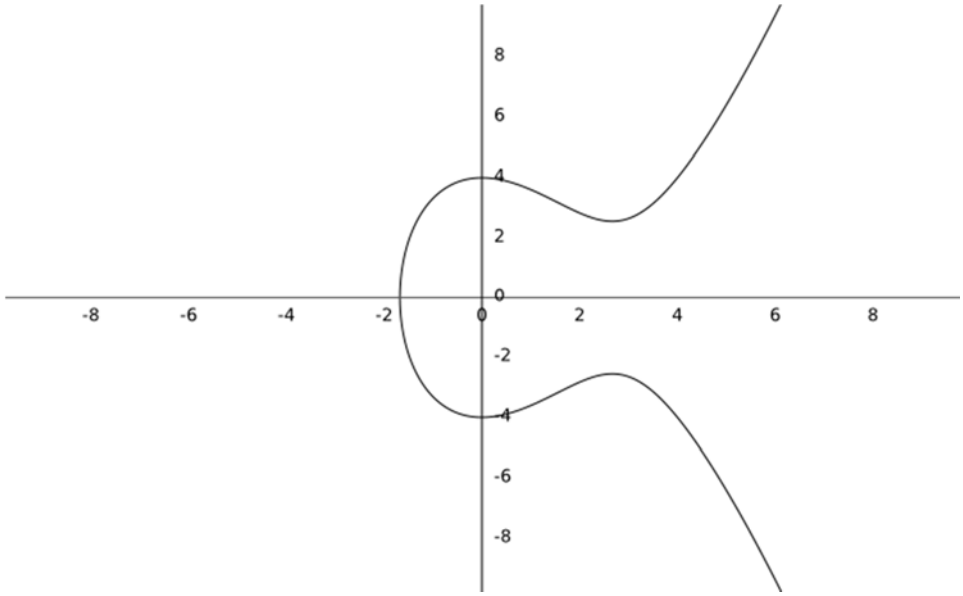

图2.2 $y^2 = x^3 - 4x^2 + 16$ 的椭圆曲线图像

对椭圆曲线上的点进行基本的加法运算，对于任意两个椭圆曲线上的点 P 和 Q，可以定义完整的椭圆曲线上进行加法的方法规则，其中 O 表示零点，也就是无穷远点：

（1）$O+O=O$，对任意的 P，有 $P+O=P$；

（2）$P=(x,y)$ 的对称点 $-P=(x,-y)$，则 $P+(-P)=O$。

（3）计算两个点 P 和 Q 的和，首先需要将 P 和 Q 连接，画出通过其位置的一条直线，此时，这条直线将与曲线交于另外一点，也即这条直线上出 P 和 Q 点之外的第三个点，这个点关于 X 轴的对称点就是就可以作为 P 和 Q 两点的和。

（4）计算 $P(P \neq O)$ 点的两倍时，首先需要做该点的切线，该切线将与曲线相交在 S 点，而相交点 S 关于 X 轴的对称点-S 就是 P 点的两倍，也即是 $2P=P+P=-S$。

椭圆曲线的点乘运算就是多次进行的加法运算。

密码学中普遍采用的是有限域上的椭圆曲线，使用模素数 p 的有限域 Z_p，将模运算引入到椭圆曲线算术中，变量和系数从集合 $0,1,...,p-1$ 取值而不是在实数上取值。此时讨论的椭圆曲线形式如下:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \tag{2-3}$$

其中，$4a^3 + 27b^2 \bmod p \neq 0$，变量和系数均在 Z_p 中取值。将满足上式的所有非负整数对和 O 点记为集合 $E_p(a,b)$，这是一个有限的离散点集。此可知集合中的点分布在 $(0,0)$ 到 $(p-1,p-1)$ 的象限中，集合中的点有可能刚好也在椭圆曲线上，更多的可能是在椭圆曲线外。$E_p(a,b)$ 上的加法规则和实数域上的加法基本一致，只是多加了模运算。但是模 p 的加法没有显而易见的几何解释，只有代数描述。

万方数据

通常，使用 ECC 算法生成的公钥和私钥都具有其固有的结构，具体定义如下：

```
Struct ec_key_st
{
    int                 version;
    EC_GROUP       *group;
    EC_POINT     *pub_key;
    BIGNUM       *priv_key;
}
```

ECC 算法基础原理基于公式$Q = kP$，其中 P 就是结构体中的 EC_POINT，私钥 k 就是结构体中的 BIGNUM。其数学困难性在于由两个乘数因子去计算最后的积是容易实现的，而对于给定的积和任意一个乘数因子而去求另外一个乘数因子而的计算是相当困难的。正因为其几乎不可能被破译，因此，可以使用两个点的乘积作为公钥去公开，而其中的一个乘数因子作为私钥秘密保存。就目前的计算机水平，对于选定的一条安全的椭圆曲线，要解决基于这条曲线的离散对数难题几乎是不可能实现的。

2.1.3 OpenSSL 密码库

OpenSSL（Open Secure Sockets Layer）是基于 SSL（Secure Sockets Layer）的开源算法库，使用 C 语言进行开发，这使得 OpenSSL 具有优秀的跨平台特性。OpenSSL 不但实现了 SSL 的一些接口，它所涵盖的内容从底层对称、非对称加密算法的到建立在其上的 PKCS(Public Key Infrastrature)的接口(包括 X509 证书、PKCS 标准、ASN.1 等)一应俱全。

OpenSSL 所实现的接口包括 2000 多个，主要支持的功能包括：

（1）使用数字证书对通信双方的身份进行认证以保证身份的合法性；

（2）使用加密算法对传输的数据进行加密以保证信息的安全性；

（3）使用 MAC 算法对数据进行完整性检验以保证数据没有被篡改；

（4）辅助功能的实现；

其中，所实现的对称加密算法一共有 8 种、非对称加密算法共 4 种、信息摘要算法共 5 种。

对于密钥和证书的管理功能，OpenSSL 也提供了多种可支持的标准，包括了：对 ASN.1 证书的相关标准和 X.509 证书的标准。实际上，OpenSSL 提供了一个小型的证书管理中心（CA），实现了证书签发的整个流程和证书管理的大部分机制，包括密钥生成、请求产生、证书签发、吊销和验证等功能。

GmSSL 是 OpenSSL 项目的分支，与 OpenSSL 保持接口兼容。GmSSL 也是一个开源的密码工具箱，支持 SM2/SM3/SM4/SM9/ZUC 等国密(国家商用密码)算法。其中

万方数据

“SM”代表“商密”，即用于商用的、不涉及国家秘密的密码技术。其中 SM2 为基于椭圆曲线密码的公钥密码算法标准，包含数字签名、密钥交换和公钥加密，用于替换 RSA/Diffie-Hellman/ECDSA/ECDH 等国际算法。SM3 为密码哈希算法，用于替代 MD5/SHA-1/SHA-256 等国际算法。SM4 为分组密码，用于替代 DES/AES 等国际算法，并且由于 SM4 设计时的预计应用领域为低功耗芯片(即 WAPI 芯片)。SM9 为基于身份的密码算法，可以替代基于数字证书的 PKI/CA（Public Key Infrastructure/Certificate Authority）体系。通过部署国密算法，可以降低由弱密码和错误实现带来的安全风险和部署 PKI/CA 带来的开销。

从功能上来讲，OpenSSL 应该算是关于信息安全知识最全的一套接口，对于各种各样具有不同用途的用户来说，都能够满足其开发需求。

2.2 认证技术

保密的目的是防止攻击者非法获取系统或网络中的机密信息；认证（Authentication）则是为了防止攻击者主动地去伪装合法用户的身份或者恶意地对所传输的消息进行篡改或重发等。

2.2.1 认证与认证系统

认证系统就是能够使通信的接收者或者不在通信链路上的第三方对发送者的身份或所传输的信息进行鉴别和认证，同时能够对此类如伪装合法用户身份、修改、删除或对数据进行篡改的一系列问题进行预防的一种可以具备验证能力的一类密码系统[47]。

通常认证可以具体分为实体认证和数据源认证两类。实体认证可以对信息的发送者进行身份的验证，以判定发送方是否受到了攻击者的攻击而造成了其身份被伪造的情况。数据源认证被称为消息认证，可以验证所接收到的消息是否遭受了攻击者的攻击而造成信息被修改或延迟重放等[48]。身份认证通常基于实体所提供的证据来验证实体的身份，在相互通信的过程中，进行消息传输的两方需要分别提供证明自己身份的证据，并使用相应的安全机制来验证证据和实体身份的对应关系。在具有较高安全等级的系统或应用中，有时需要借助第三方可信机构提供安全认证相关的服务。

公钥加密和其他密码学系统最主要的一个问题是需要确认接收到的消息的发送者实际上是消息中指定的人。一种已知的利用”数字签名”的认证技术允许用户使用其密钥“签署消息”，接收方或第三方可以使用发送方的公钥进行验证。用户可以在发送消息之前使用其公钥对所要发送的消息或消息摘要进行签名，而接受方可以使用发送方已经公开的公钥解密消息或消息摘要来验证发送方的身份，从而实现对于身份的认

万方数据

证功能。

2.2.2 数字证书技术

公钥密码系统在保证指定公钥是由指定个人实际创建的情况下仍然存在严重的问题，如对于公钥不合理的管理，可能会导致严重的安全漏洞。解决这个问题的一种已知技术是依靠一些可信任的权威，例如政府机构，来确保每个公钥都与声称是真正作者的人相关联。受信任机构创建一个数字消息，其中包含申请人的公钥和申请人的姓名，并且使用受信任机构自己的数字签名该数字消息。这种数字信息，通常称为证书。

数字证书主要提供了一种在网络上进行身份验证的方式，借助了 PKI 技术，即公开密钥基础架构技术来管理公钥。数字证书中包含着签名所使用的算法，因此，使用的签名算法不同，数字证书的类型也不同如使用 ECDSA 算法进行签名时所生成的证书就是 ECC 证书。通常，可以从证书中提取设备的公钥信息并且可以查看证书的颁发机构[49]。

使用数字证书进行双向身份认证时的通信过程如图 2.3 所示。首先通信双方想第三方的可信任机构（CA）申请数字证书，CA 在核实过申请者的身份之后，分发数字证书给申请者，此时，相互通信的双方唯一拥有属于自己的数字证书。此后，通信双方使用数字签名技术来验证对方的身份，发送使用其自身私钥签名的认证请求消息至对方，接收方根据 CA 公钥和双方证书对认证请求消息进行验证，因为只有发送方才能拥有他的私钥，从而验证了发送方身份的真实性和合法性。在通信双方身份认证都通过后，使用密钥交换算法生成后续会话密钥。

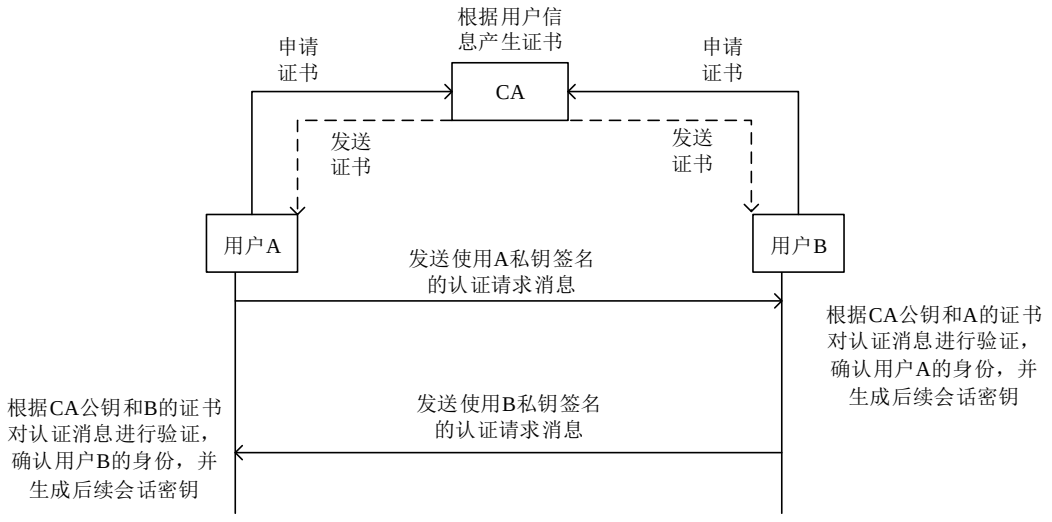

图2.3 PKI/CA 身份认证框架

万方数据

2.2.3 密钥交换算法

1976 年，两位数学家 Whitfield Diffie 和 Martin Hellman[50]发表了一片关于密钥传输方法的文章，解决了通信的双方不用见面就能生成共享会话密钥的问题。这种算法实现的原理是在双方通信之前，相互通信的双方首先需要各自生成密钥的一部分，然后彼此通过通信链路交换这部分信息，最后基于此生成最终的密钥。

用于密钥协商的另外一个算法，即 ECDH 密钥交换算法，其原理是将 ECC 算法和 DH 密钥交换算法结合在一起。具体地，ECDH 的运算是把 DH 中模幂运算替换成了点乘运算，速度更快，可逆更难。交换双方可以在不共享任何秘密的情况下协商出一个密钥。使用 ECDH 密钥协商算法进行密钥磋商的过程如图 2.4 所示：

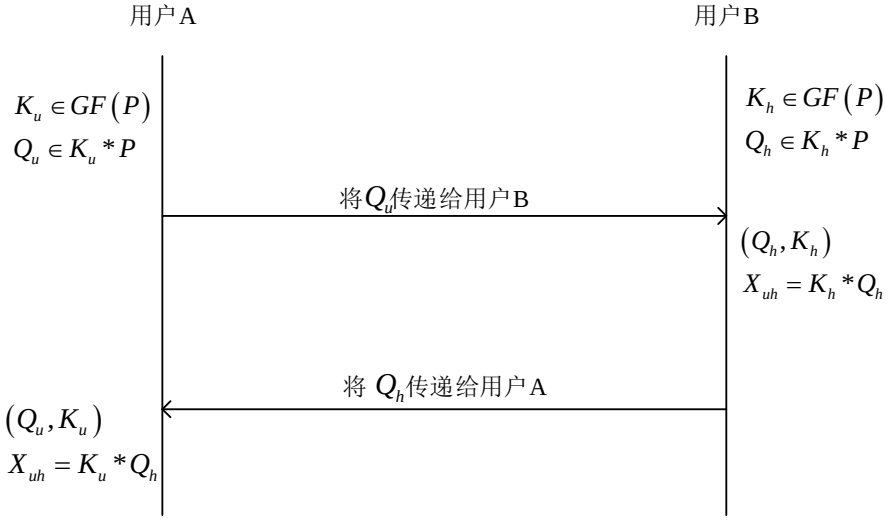

图2.4 ECDH 密钥交换过程

首先密钥分配中心 KDC（Key Distribution Center）在有限域 GF(p)上随机选取特定的椭圆曲线 E，其中 p 是素数并且使基点 P 具有较大的阶 q（其中 q 也是素数）。通信双方共享该曲线参数。

然后 KDC 生成随机数 $K_i \in GF(p)$ 作为设备 i 的私钥，并生成相应的公钥 $Q_i = K_i \times P$。密钥对 $\{Q_i, K_i\}$ 被给予设备 i。随着设备数量的增加，KDC 可以为任意数量的设备生成基于基点 P 的 ECC 密钥对。

最后，相互通信的设备将其公钥发送至对方，双方基于自己私密的参数和对方已公开的参数计算得到后续通信所需的协商密钥。任何第三方都无法访问每个设备的私有详细信息，无法从可用的已知信息中计算出私密的共享密钥。

由于 ECC 算法具有更小的密钥和更低的计算开销，因此，将 ECC 算法与 DH 算法结合的 ECDH 对称密钥交换协议，更加适用于资源受限的系统。

万方数据

2.3 消息完整性技术

实现数据的安全传输，仅用加密算法是不够的。攻击者虽难以破译加密数据，但可以试图篡改或破坏，使接收者无法收到正确的信息。为了能够使接收者辨别其所接收到的信息是否是发送者所传输过来的原始数据，需要一种安全机制来解决所存在的这种问题。具体的功能是在存储数据或传输数据的过程中，若数据遭受到未经授权的攻击者篡改或修改时，能够快速地被发现，常把这种机制称为消息完整性机制。

为了验证所传输的消息是否完整，通常使用消息摘要，也称为散列（hash），来实现这种功能。1976 年，公钥密码体制概念被提出的同时，散列函数也一同被提出[50]。基于散列函数（hash），它可以将任何数据映射为一个较小长度的固定输出。它具有两个特性：

（1）函数是单向的；

（2）找到两个输入数据生成相同的输出散列值是几乎不可能的。

这样就可以使用它来将报文指纹化，而指纹可用于验证数据的完整性。常用的散列函数可以分为一般杂凑函数和密码散列函数。

一般散列函数，不需要密钥进行控制，任何人都可以使用输入子串进行计算得到哈希值，因此可以说，一般散列函数能够实现的功能只有数据的完整性检验，而不能用于进行身份认证。密码散列函数，相对于一般散列函数，需要密钥进行控制，常以h(k,M)的形式表示。密码散列函数值不仅与输入的子串有关，还需要密钥参与计算得到散列值。因为只有持有密钥的人才能计算出相应的哈希值，因此，密码散列函数不仅可以用于数据完整性检验，还可以对身份进行验证。

消息鉴别码（MAC）是常用的密码散列函数，可以确认消息完整性并进行认证。与消息摘要相似，但 MAC 要求发送方与接受方知道共享对称密钥，用其生成 MAC，即 MAC = h(k||M)。基于散列的消息鉴别码（HMAC）是实现互联网安全协议的重要工具，基本原理如图 2.5 所示。

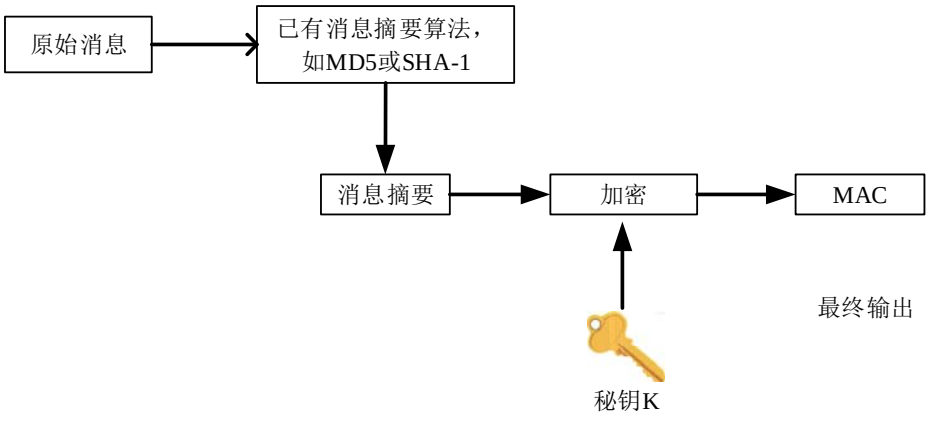

图2.5 HMAC 基本原理

万方数据

使用消息验证码（MAC）对所传输的消息进行完整性检验的过程如下：

（1）发送方 A 把消息发送给接收方 B 前，先把共享密钥发送给接收方 B。

（2）A 把要发送的消息使用共享密钥与 MD5（Message-Digest Algorithm）、SHA-1（Secure Hash Algorithm 1）之类的现有消息摘要算法计算出 MAC 值，然后将消息和 MAC 发送给 B。

（3）B 接收到消息和 MAC 值后，使用共享密钥对接收到的数据进行计算得到新的 MAC 值，并与接收到的 MAC 值比较。

（4）如果比较的结果是两者的 MAC 值相同，则说明在消息传输过程中消息未被篡改，消息是 A 发送的并且消息是完整的。

2.4 数字签名技术

根据 2.3 节的知识可以知道，消息鉴别码可以用来检验消息的完整性，还可以对消息进行认证。但消息鉴别码的缺陷就在于其共享密钥可能会导致抵赖问题的发生。因此，可以使通信双方的密钥不同，从密钥的使用上来区分彼此的身份，数字签名技术便可以解决抵赖问题的发生。

2.4.1 数字签名原理

随着计算机网络和互联网技术的发展，可以使用电子数字签名来代替传统的手书签名方式，这种机制在安全信息系统中被称为数字签名。

数字签名用途广泛，包括对于网站身份的认证、不可否认性、对消息完整性检验、以及代码签名等，尤其在涉及到电子商务系统或其他大型网络安全通信时，数字签名的作用更加明显。作为网络中实现认证的重要工具，数字签名方案通常用作加密协议中的原语，提供其他服务。

一个签名体制可由四元组$(M,\Im,K,V)$组成，其中：

M 是明文空间；

$\Im$ 是签名的集合；

K 是密钥空间；

V 是认证后的结果值域，由真和伪两种结果组成；

签名算法：对任意$m\in M$和$k\in K$，M的签名$S=Sig(m)\in\Im$很容易被计算出来，并且只能由签名人对此签名，因为使用的签名密钥是秘密的，任何其他人是不知道的。

验证算法$Ver_k(M,S)\in\{真，伪\}=\{0,1\}$，已知$M$，$S$易于证明$S$是否为$M$的签名，要验证签名，因此，验证算法应该被公开。

万方数据

$$Ver_k(\mathrm{M},\ S)=\begin{cases}\text{真}, & \text{当 S}=\ Sig_k(\mathrm{M})\\ \text{伪}, & \text{当 S}\neq Sig_k(\mathrm{M})\end{cases} \tag{2-4}$$

使用数字签名技术进行认证的过程如图 2.3 所示。可以看出，数字签名的基本原理似乎与使用公钥密码体制进行加解密的过程是相反的，在公钥密码体制中，公钥用于加密，而在数字签名算法中，公钥用于解密。同理，私钥的作用也刚好相反。

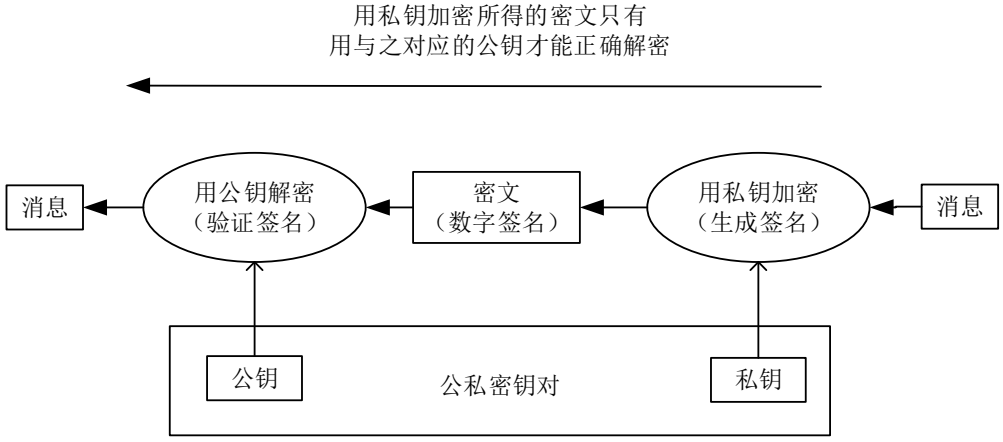

图2.6 数字签名过程

根据图 2.6 可以将数字签名的过程总结为如下三个阶段：

数字签名的生成：对于要传输的消息原文首先使用摘要算法（如 MD5、SHA 等）生成一定长度的消息摘要，并使用发送方的私钥对所生成的消息摘要进行加密操作，形成最后的签名信息。

消息传输阶段：将所生成的数据信息和数字签名发送至对方。

数字签名的验证：接收方接收到数据，首先使用发送方的公钥对摘要信息进行解密，同时对所接收到的数据重新进行哈希计算，比对两份消息摘要结果是否相同。借助公私钥对和签名算法可以证明消息确实是由公钥拥有者发出的。两份摘要的比对结果，可以证明消息在传输的过程中是否被改动。

2.4.2 数字签名算法

数字签名方案可以根据为其安全性提供基础的硬性基础数学问题分为基于大整数分解难题如 RSA 数字签名算法、基于有限域中（普通）离散对数问题的难处理性如 ElGamal 签名算法和基于椭圆曲线上离散对数的难处理性如 ECDSA 签名算法三大类。

RSA 是目前计算机密码中最经典的算法之一，经常被广泛用于各种加密场景中，RSA 的数字签名算法实现原理也和其加解密算法是一样的，也是至今为止使用最为

万方数据

广泛的数字签名算法。

数字签名算法（DSA），被称为数字签名标准（DSS[36]）。和 RSA 签名算法的不同之处在于 DSA 只能用于签名，而不能用于加解密操作。就速度而言 DSA 比 RSA 更快；针对安全性，两者相比差不多。DSA 的安全性是基于Z_p^*的素数子群中离散对数问题的计算难处理性。

ECDSA 用于数字签名的整个过程与 DSA 类似，并且与 DSA 算法数学基础类似。不同之处在于 ECDSA 是对离散对数问题进行椭圆曲线模拟，其将旧离散对数密码系统中有限域上的子组Z_p^*由椭圆曲线上的点组代替。

与 ECDSA 签名算法原理相同，国密算法 SM2 也是基于椭圆曲线公钥算法的数字签名算法，用 SM2 算法进行签名时，需要借助 SM3 密码杂凑函数消息进行杂凑值的计算。正是因为 SM2 算法安全性所基于的理论基础，使用 SM2 算法进行签名与使用 RSA 算法和 DSA 算法进行签名的性能更好。

对于 SSL 数字证书和代码签名证书以及其它非对称加密产品来说，RSA 目前普及度最高。但在不同的应用场景下，应该选择适合的签名算法，如对于资源比较受限的系统或实时性比较高的系统，建议选择基于椭圆曲线的签名算法，因为他们能够以较小参数优势在处理能力、存储空间、带宽或功耗受到限制的环境中发挥更好的性能。

2.5 本章小结

本章主要针对安全认证和安全通信的相关安全机制和技术进行了介绍。首先介绍了密码学中的加密体系，主要包括了非对称密码体制和椭圆曲线密码体制，并对常用的 OpenSSL 开源密码库进行了简单介绍。接着，给出了认证和认证系统的基本概念，分析了传统认证协议中存在的问题，并对传统的数字证书技术以及密钥交换算法进行了概述。其次，对消息完整性技术进行了简单的介绍。最后，讨论了数字签名技术的原理以及常用的数字签名算法。通过对所有相关安全机制和技术理论的讨论和研究，为下一步无人机网络轻量级安全认证和通信方案的研究提供了有力的理论基础。

万方数据

万方数据

第三章 轻量级身份认证机制

无人机网络身份认证方案需要为参与交互的无人机节点提供相互之间的身份认证和会话密钥协商功能。传统基于用户名/密码、动态口令的的身份认证方式安全性较低，基于 RSA 证书的认证方案需要较长密钥和较大运算量。针对以上问题，本章实现了将 ECC 体制应用于无人机节点间双向身份认证，与当前主流的基于 RSA 数字证书的无人机身份认证方法相比，能够以较短的密钥长度和较小的计算量，实现较高的安全性。同时实现了对无人机会话密钥的一致性检验，解决了因密钥计算错误或消息传输过程中丢包造成的协商密钥不一致问题。

3.1 无人机网络身份认证需求

如果无人机网络不能提供适当的身份验证方案，将会导致各种安全威胁的发生。具体来讲即攻击者可以伪装成合法实体，从而在通信网络中散布虚假的信息或命令。因此，为了能够对无人机身份进行安全认证，无人机网络所提供的安全认证方案应该实现如下的安全目标：

相互认证：所有的其他服务都是建立在确认参与者的身份是真实合法的基础之上。由于多源无人机之间的通信和异构化的网络，攻击者可以充当其他参与者并使用可靠的设备来控制通信。因此，为了获得访问权限，用户可以提供某种形式的凭证，常由某种形式的凭证和追溯到权威的信任链建立，一旦建立了身份（身份验证），用户就会被授予使用网络和访问网络上某些资源的权限（授权）。

会话密钥安全性：一旦会话密钥泄露，攻击者就可以轻松解密传输的消息，从而破坏消息的机密性，因此会话密钥安全性是消息机密性的基础。为了进一步保护通信，符合条件的方案应确保用于加密传输消息的某些参与者之间建立的共享会话密钥是安全的。

不可否认性：不可否认性用于确保节点不能否认已发布某些信息，是一种双面服务。发件人必须确认消息接收者是预定收件人，而收件人必须确认发件人有效并予以确认。与消息完整性不同因为它侧重于发送者和接收的身份而不是消息的内容。此要求加强了对各种操作的管理，从而预防了对已发生行为的否认，目的是为安全问题的出现提供调查的基础或方法。

身份认证方案一方面需要满足以上的安全需求。另一方面无人机的能效也是一个关键的问题，因为无人机和计算设备采用电池供电，同时具有存储空间和计算资源有限的特点。因此，受以上特性的局限，所设计的身份认证方案应以较低的资源开销实

万方数据

现对无人机身份的认证。

3.2 攻击者模型

对于攻击类型的建模有助于理解实际无人机网络的安全威胁，并能够基于此攻击者模型制定相应的安全机制提高无人机通信过程中的安全性。在无人机接入网络时，本文假设攻击者可以发起假冒攻击、信息窃取攻击和重放攻击，攻击示意图如 3.1 所示。

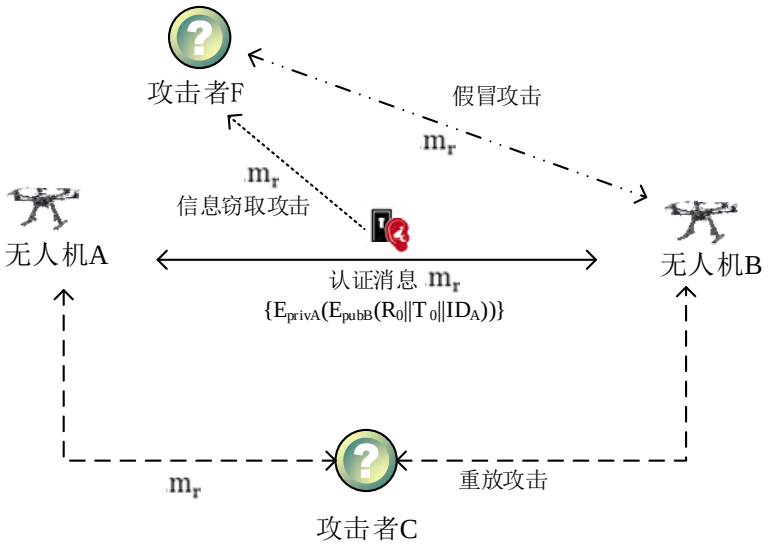

图3.1 攻击示意图

将无人机 i 的设备符号标识为ID_i，该方案中无人机包括四种认证材料，为无人机公钥Pub_i、无人机私钥$Priv_i$、对称密钥K和无人机证书f_i, 并定义加密函数 E 和解密函数 D，用以实现方案中的加解密操作。所传输的认证消息格式定义为:

$$m_r=\{E_{privA}(E_{pubB}(R_0||T_0||ID_A))\} \quad (3\text{-}1)$$

其中||表示连接符，$E_{pubB}(R_0||T_0||ID_A)$表示用无人机 B 的公钥加密无人机 A 标识符 ID_A、随机数 R_0 和时间戳 T_0，$E_{privA}(E_{pubB}(R_0||T_0||ID_A))$表示使用无人机 A 私钥对加密信息进行签名。

本文假设攻击者可发起以下攻击：

（1）信息窃取攻击

攻击者 F 可以利用一些技术或者工具捕获网络中的认证消息m_r，并对消息m_r进行处理分析得到有效信息如无人机身份 ID。窃取信息攻击只能窃取信息中的敏感数据但不对数据进行篡改。

万方数据

（2）假冒攻击

攻击者 F 在无人机网络中，通过截获无人机节点间传输的认证消息m_r，从中获取得到合法无人机的身份信息 ID，攻击者 F 就可以使用这个身份连接到网络中。攻击者通过这种方式伪装成合法无人机 A 来接入无人机网络并与网络内的无人机节点进行通信，对网络内所传输的消息进行监听并发布虚假的消息。

（3）重放攻击

攻击者可以发送一个目的主机已经接收过的数据消息来达到欺骗系统的目的，并利用网络监听或其他方式获取发送方的认证消息m_r，主要用于身份认证过程，破坏认证的正确性。发起攻击的可以是无人机或地面设施，定义为攻击者 C。C 可以截获 A 通过实线发送给 B 的消息m_r，C 伪装成 A 按照虚线所示路径将m_r转发给 B，而 B 会误以为 C 就是 A，就把回应报文发送给 C。虽然消息m_r是加密的，但 C 根本不用破译便可以直接伪装成 A 将消息发送给 B。

3.3 基于椭圆曲线算法的身份认证方案

基于证书的认证方案是传统的基于公钥的多播认证方案，基于传统公钥算法如 RSA 的证书认证方案通常具有较高的计算、通信和存储开销。相比而言，基于 ECC 算法和 ECDH 密钥交换来认证加入网络中各个节点的身份合法性，理论上能够以较短的密钥长度实现较高的安全等级，且计算速度更快、存储开销更小，能够降低身份认证的开销。

本章采用椭圆曲线密码体制来实现对于无人机身份的认证，具体地，使用轻量级 ECC 数字证书作为无人机间身份的凭证，并使用 ECDSA 签名算法和验证签名算法对无人机身份进行签名验证，同时使用 ECDH 密钥交换算法为两无人机协商出通信过程中使用的会话密钥。技术设计方案如图 3.2 所示。

图 3.2 详细地描述了我们所设计的针对无人机网络中节点的轻量级认证方案。为了保证无人机间通信内容的安全性，轻量级远程身份认证技术需要使合法的无人机之间能够互相交换认证信息，在通信双方认证对方身份并成功的基础上，为两无人机协商出相同的加密密钥，并对通信内容进行加密后传输至对方。针对认证过程高安全性的要求，使用数字证书作为合法无人机的身份证明；无人机双方交换数字证书后，通过对对方证书签名的验证，可以确认对方为合法无人机。同时，针对无人机间通信对时延、带宽、功耗要求较高，采用轻量级 ECC 数字证书来降低对系统资源的消耗，并且要保证认证方案的安全性。

具体的，可以简单地把基于 ECC 证书的轻量级认证方案分为认证初始化阶段、身份认证阶段和身份认证三个阶段。

万方数据

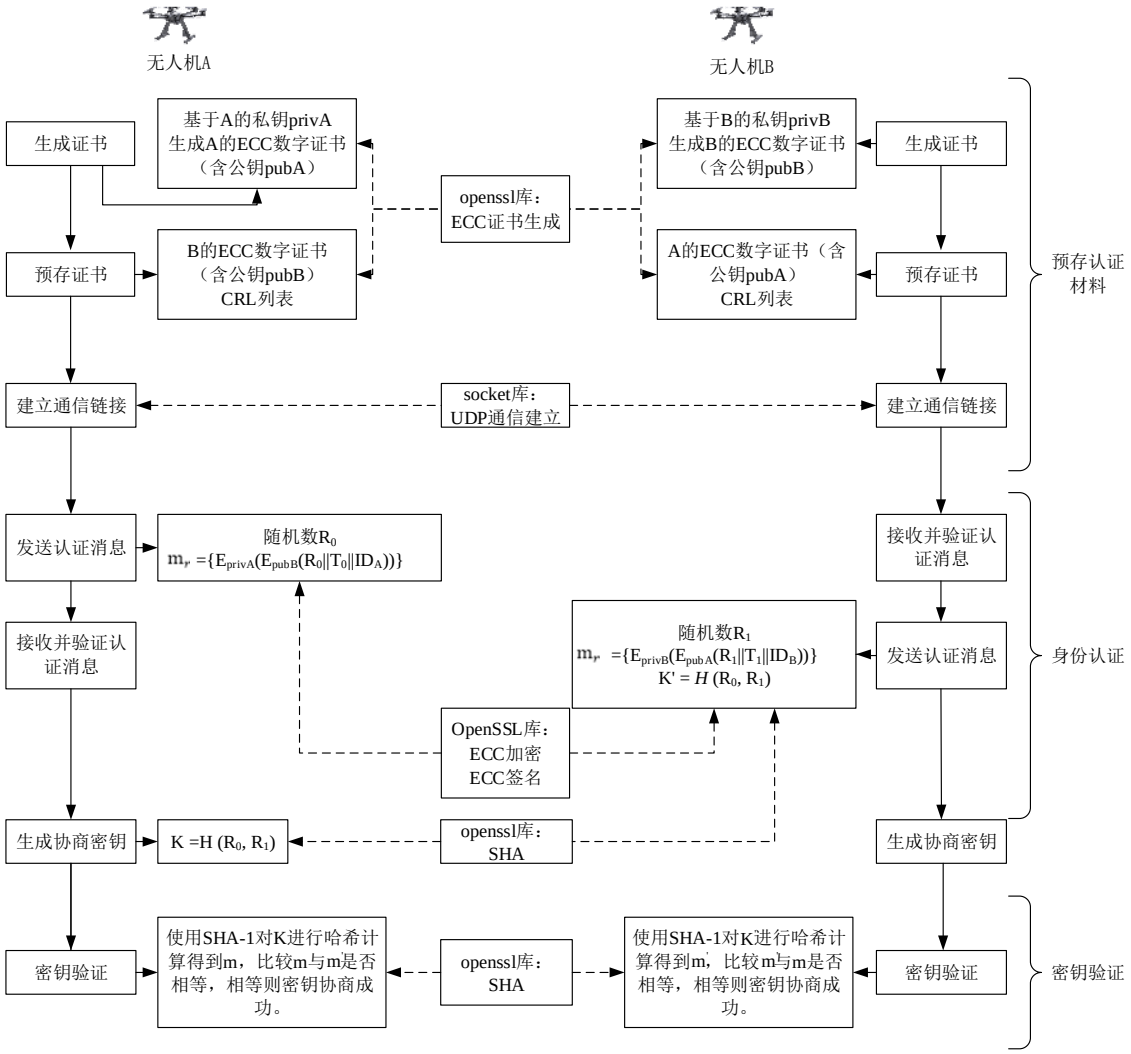

图3.2 基于椭圆曲线的身份认证方案

3.3.1 ECC 证书生成及认证初始化

在对通信双方的无人机进行认证之前，首先需要对认证材料进行初始化操作，并提前预存双方无人机的认证材料。具体地，需要预存的材料包括：

无人机 A 预存认证中心 CA 的公钥、认证中心 CA 签发的无人机 A 的 ECC 数字证书（含公钥）、无人机 A 私钥、无人机 B 的 ECC 数字证书（含公钥）以及认证中心发布的证书撤销列表。

无人机 B 预存认证中心 CA 的公钥、认证中心 CA 签发的无人机 B 的 ECC 数字证书（含公钥）、无人机 B 私钥、无人机 A 的 ECC 数字证书（含公钥）以及认证中心发布的证书撤销列表。

基于 ECC 的数字签名证书在结构上与基于 RSA 的证书相近，都符合 X.509 标准，对 X.509 证书来说，认证者总是 CA 或由 CA 指定的人，并且主要字段包括证书

万方数据

版本号、公钥信息和所使用的签名算法等，签名信息是使用认证中心 CA 的私钥对证书中其他信息的哈希值进行签名所得。ECC 证书结构如图 3.3 所示。

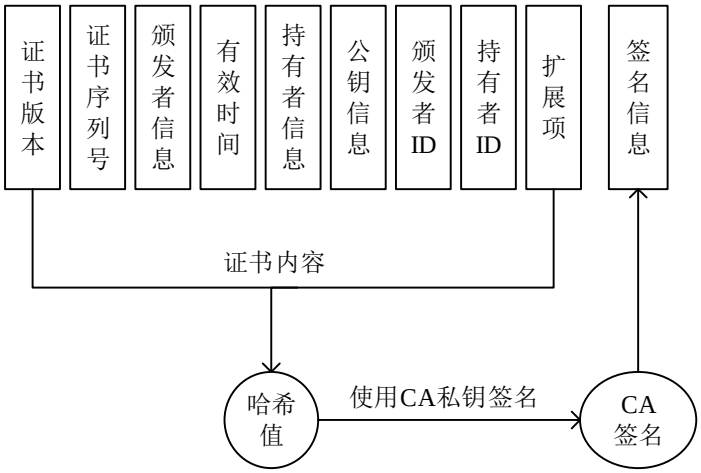

图3.3 基于 ECC 的数字证书结构

ECC 证书和 RSA 证书的不同之处主要在于主体公钥信息和所使用的签名算法。其中 ECC 证书中的公钥信息是基于 ECC 算法生成的，同时该证书采用椭圆曲线签名算法进行签名。而 RSA 证书中的公钥信息是基于 RSA 算法生成。基于 ECC 证书的认证方案能够以较小的密钥长度实现较高的安全性，适用于资源受限的无人机网络。

具体实现时，基于 OpenSSL 开发软件库进行开发，进行证书材料预存的主要步骤如下：

（1)基于 ECC 密钥生成算法生成 CA 私钥、无人机 A 和无人机 B 的 ECC 私钥，并将私钥信息秘密保存在本地密钥管理区。

（2）基于所生成的 CA 私钥，使用 OpenSSL 所提供的自签发证书的功能生成 PEM 格式的 X.509 CA 根证书；

（3）根据无人机 A 和无人机 B 的私钥，生成证书请求文件；

（4）利用 CA 对无人机 A、B 的证书请求文件进行签发，生成无人机 A、BECC 数字证书；

（5）使用 UDP 套接字将证书发送给对方无人机进行预存，以方便之后使用证书信息对无人机身份进行认证。

在实现相同安全等级时所需的 ECC 密钥比 RSA 密钥明显更短，因此在存储 ECC 密钥时所占用的存储空间更小、带宽要求更低，降低了无人机网络的存储开销，增强了无人机系统的可用性。同时更短的密钥所需要的计算开销也更小。当通信双方无人机将认证所需材料预存好之后，便可以基于 ECC 算法的数字签名算法对双方无人机的身份进行签名和验证。

万方数据

3.3.2 身份认证

身份认证阶段主要借助于双方无人机提前预存的证书信息，同 ECC 算法实现原理一致，使用基于椭圆曲线的 ECC 算法实现对于无人机身份的签名和验证签名来验证无人机身份的合法性。同时，使用基于 ECC 算法的 ECDH 密钥交换算法生成后续通话所需的会话密钥。具体流程如图 3.4。

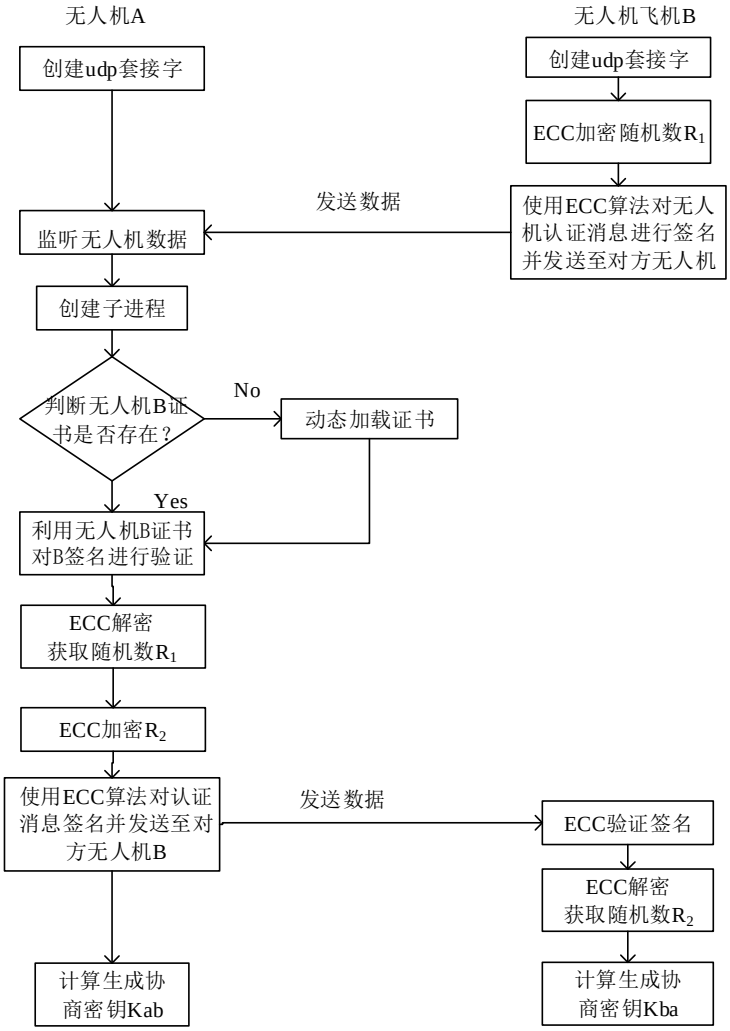

图3.4 身份认证基本流程

当无人机 B 向无人机 A 发送认证请求消息时，无人机 A 对无人机 B 身份认证的基本步骤如图 3.4。同理，当无人机 A 向无人机 B 发送请求消息时，无人机 B 对于无人机 A 的身份认证步骤也同图 3.4。具体地，可将无人机间的双向身份认证步骤总结如下：

a. 无人机 A 使用随机数发生器产生随机数 R_0；发送认证请求消息至无人机 B 进行身份认证，其中，身份认证请求消息包括：

万方数据

i. 使用无人机 B 公钥加密的无人机 A 身份标识符 ID_A、时间戳 T_0 和随机数 R_0

ii. 使用无人机 A 私钥对加密信息 i 的签名；

b. 无人机 B 接收到无人机 A 发送来的认证请求消息，并使用无人机 A 公钥解密得到加密后的无人机 A 的 ID_A、随机数 R_0 和时间戳 T_0，使用无人机 B 的私钥解密得到 ID_A、R_0 和 T_0；

c. 无人机 B 判断随机数 R_0 是否被使用过，若被使用过，则可能存在重放攻击，认证失败；R_0 认证通过后验证时间戳 T_0 是否在时延 ε 范围内，若在 ε 范围内认证成功，继续下一步认证；否则认证失败；

d. 无人机 B 根据预存的 ECC 数字证书来认证无人机 A 的证书，若该证书合法，则认证成功，无人机 B 将自己的认证请求消息发送至无人机 A；否则，认证失败。无人机 B 的身份认证请求消息包括：

i. 使用无人机 A 公钥加密的无人机 B 身份标识符 ID_B、时间戳 T_1 和随机数 R_1

ii. 使用无人机 B 私钥签名的加密信息 i；

e. 当无人机 A 收到 B 发送的认证消息，进行无人机 B 相同的验证操作：判断随机数 R_1 是否被使用过以及 T_1 是否在时延 ε 范围内，并根据预存的 ECC 数字证书判断无人机 B 的证书的合法性。符合以上要求，则认证成功；否则，认证失败。

f. 无人机 A 和 B 双方身份认证都通过后，使用认证请求消息中的随机数 R_0 和 R_1 计算出用于后续通信的协商密钥 K 和 K'。

具体在进行代码开发时，使用无人机私钥加密随机数这一步可以基于 OpenSSL 的签名算法实现。具体使用 ECDSA 签名算法对认证消息进行签名，并使用 UDP 套接字建立通信链路并发送签名信息，接收方使用 ECDSA 验证签名算法对签名消息进行验证来确认对方身份。双方身份均认证通过后，使用基于 ECC 算法的密钥交换算法 ECDH 生成后续通信的会话密钥。

根据以上步骤可以实现通信双方的双向身份认证。在双方身份都认证成功后，生成后续通信所需会话密钥。因为在密钥交换的过程中，协商的密钥可能会因消息传输过程中由于丢包或因为计算错误等问题造成不一致的问题，所以需要对协商后的密钥进行一致性检验。

3.3.3 密钥一致性检验

由于无人机网络是一种开放式的网络系统，极易受到恶劣天气等外部环境干扰和通信链路不稳定等因素的影响，造成因传输信息丢包而无法正常解析的安全缺陷。因此，在密钥交换的过程中，可能会因消息传输过程中由于丢包或因为计算错误等问题造成密钥不一致的问题。由于会话密钥在后续的通信过程中发挥着重要的作用，因此，对双方无人机生成的会话密钥进行一致性检验是非常有意义的。具体密钥一致性检验

万方数据

方法过程如图 3.5。

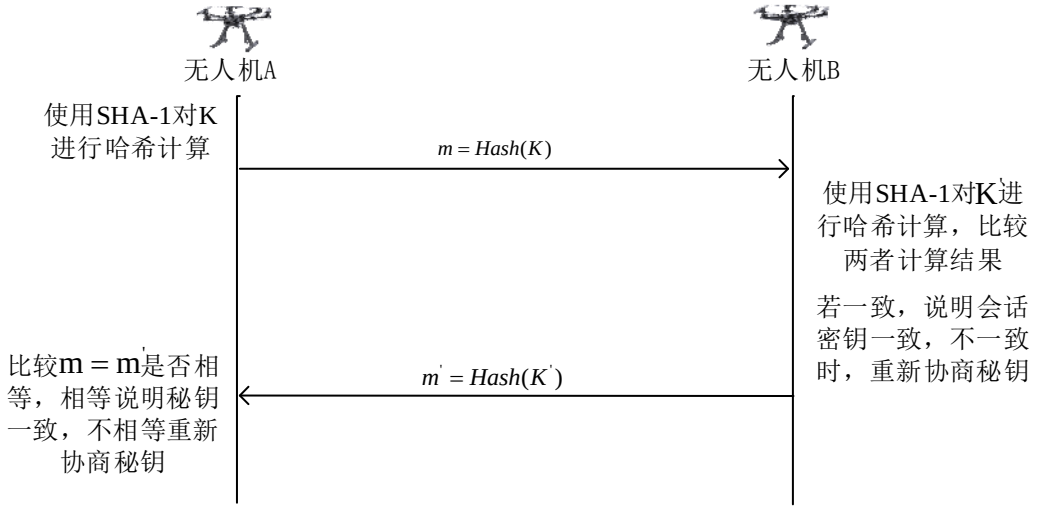

图3.5 密钥一致性检验过程

可以将密钥一致性检验的步骤总结如下：

a.无人机 A 使用其 SHA-1 计算协商密钥 K 的哈希值 m，并将 m 发送至无人机 B；

b.无人机 B 使用其 SHA-1 计算协商密钥 K' 的哈希值 m'，并将 m' 发送至无人机 A。比较 m 和 m' 是否相等，若相等，则说明协商密钥一致；不相等时，跳转至步骤 d；

c.无人机 A 比较接收到的 m' 与其计算所得的 m 是否相等，若相等则说明密钥一致；不相等时，跳转至步骤 d；

d.密钥不一致时，重新根据认证阶段的随机数生成会话密钥，直至双方的会话密钥一致为止。

3.4 实验与分析

3.4.1 网络环境部署

本节根据无人机网络计算机系统的实际环境完成了无人机网络的部署。实际进行测试时的无人机网络环境如图 3.6 所示。其中包括四台无人机，无人机之间可以通过无线链路实现相互通信。

基于 OpenSSL 开发软件包开发的 ECC 认证方案代码。首先需要将所开发的软件移植到 VxWorks6.9 开发板上，并将 LYS-IMX6Q 开发板分别部署到无人机上，模拟无人机网络拓扑环境进行测试。

万方数据

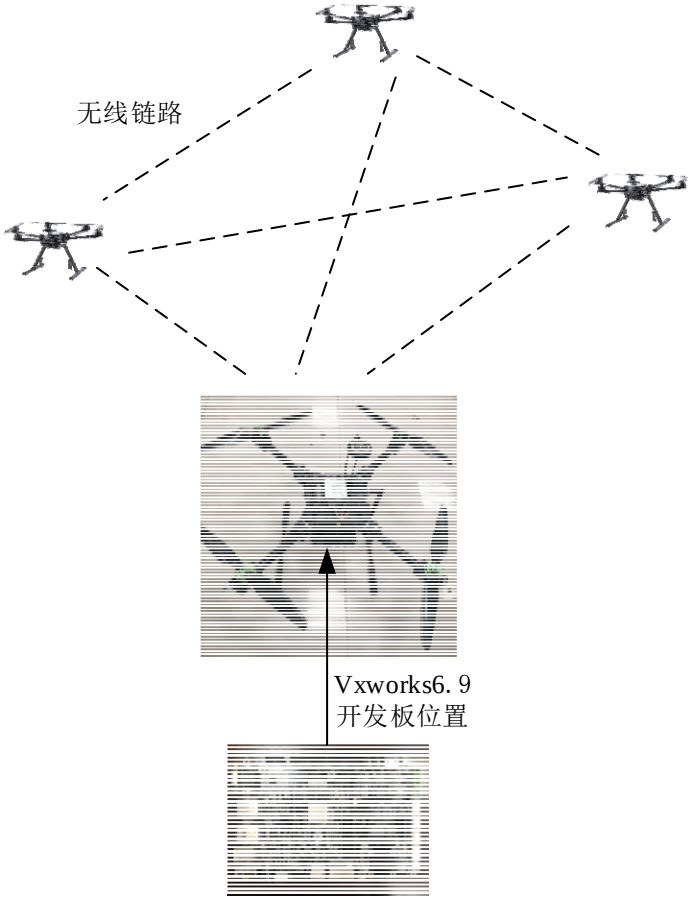

图3.6 实验测试时无人机网络环境

在进行代码移植时，首先需要对 VxWorks6.9 开发板进行配置，具体步骤如下：

（1）初始配置和连接：连接 VxWorks6.9 串口线和电源，其中串口指的 UART4。若无相关驱动，安装 USB 转串口驱动。主机 IP 和板子 IP 一定要设置到同一网段；

（2）BOOT 烧写：打开烧写软件 MfgTool2，按下 RESET 和 BOOT 键。然后先释放 RESET 键，再释放 BOOT 键，进入烧写模式。烧写完成后，在串口终端软件 SecrueCRT 中配置串口参数。

（3）系统安装：在系统更新时，需要通过 ftp 加载系统映象启动系统。首先连接网线，打开 wftp32 软件进入 Boot Sheel 界面，输入@命令进行系统烧写。当系统烧写完成后，可以使用 Shell 命令执行一些基本的系统操作。

当所有的硬件环境准备好之后，需要将所开发的软件部署在 VxWorks6.9 开发环境上，主要利用的运行开发环境为 workbench3.0。具体步骤如下：

（1）配置工程：首先打开 workbench3.0 软件，进入内核配置空间进行系统内核配置，加入常规需要的组件如 C++、数据安全组件、网络组件、操作系统组件、硬件驱动组件等。

万方数据

（2）新建工程：通过 workbench3.0 建立 Downloadable 类型的动态库工程，将基于 ECC 算法的认证代码导入至该工程目录下。

（3）编译软件：选中工程文件，使用编译工具 ARMARCH7gun 编译生成最后的.out 可执行文件。

（4）下载可执行文件：将编译生成的可执行文件下载到开发板，在 VxWorks6.9 开发板终端通过命令执行该可执行文件，并将结果输出至系统终端。

通过以上步骤，可以搭建测试所用的实验硬件环境，并能够将软件部署到该硬件环境下进行功能和性能两方面的测试。

3.4.2 认证方案功能测试

根据无人机网络认证功能的具体要求，对所设计的认证方案进行了功能性测试，首先从理论上分析了 ECC 算法的安全性，并与 RSA 算法实现不同安全级别所需要的密钥长度进行了对比，具体分析如表 3.1[51]所示。

表3.1[51] RSA、ECC 的安全性分析比较

破译所需时间/MIPS 年	RSA 密钥长度	ECC 密钥长度	RSA/ECC 密钥长度之比
10^4	512	106	5:1
10^8	768	132	6:1
10^12	1024	160	7:1
10^20	2048	210	10:1
10^78	21000	600	35:1

同时，在实验环境下对包括使用 ECC 证书进行身份验证的正确性、ECDSA 签名算法的正确性以及使用 ECDH 算法生成会话密钥的正确性和一致性进行了测试。实验结果如表 3.2 所示，具体实验测试界面显示如图 3.7 和 3.8 所示。

实验结果显示，当客户端发送伪造的数字证书时，服务器端对客户端身份验证失败，不能够继续进行协商密钥等后续操作。当客户端发送正确的数字证书时，服务器端可以对客户端的身份进行正确的验证签名操作。身份认证通过后，基于传输的随机数生成协商密钥，双方无人机对生成的协商密钥进行一致性检验，若双方协商密钥一致则输出“Key consistency check passed”；若不一致，则输出“Key consistency check failure”。此处的客户端和服务器端可以为无人机或地面设施。

万方数据

表3.2 无人机网络身份认证功能测试结果

功能	测试项目	测试结果
ECC 证书身份认证的正确性	使用伪造的 ECC 证书进行身份认证 使用正确的 ECC 证书进行身份认证	认证失败 认证成功
数字签名	将基于椭圆曲线的签名算法移植至 VxWorks6.9 系统，并对认证消息进行签名和验证	数字签名和验证签名成功
协商密钥生成	使用 ECDH 密钥交换算法生成双方会话密钥	生成密钥成功并被保存在密钥管理文件夹
密钥一致性检验	检验双方的会话密钥是否一致	一致时，保存密钥 不一致时，重新生成密钥并保存

```
-> server
listening......
connect to client 192.168.0.205!
child created : 2749
verify failure
Negotiation key create failure!
child 2749 terminated!
```

(a) 认证失败时服务器端输出

```
-> client
connect to server!
signature success!
send authentication message to server
client disconnected
```

(b) 认证失败时客户端输出

图3.7 认证失败时结果输出

```
-> server
listening......
connect to client 192.168.0.205!
child created : 2749
verify success
Negotiation key create success!
--------------------
signature success!
send authentication message to client!
Key consistency check passed !
child 2749 terminated!
```

(a) 认证成功时服务器端输出

```
-> client
connect to server!
signature success!
send authentication message to server
--------------------
verify success
Negotiation key create success!
Key consistency check passed !
client disconnected
```

(b) 认证成功时客户端输出

图3.8 认证成功时结果输出

从功能测试结果可以看出我们所设计的基于 ECC 证书的身份认证方案，能够在无人机网络实际环境下借助椭圆曲线签名算法完成对于无人机身份的安全认证，满足无人机网络认证的基本功能需求。在认证成功后，使用 ECDH 密钥交换算法生成后续通信所使用的会话密钥，并能够对无人机双方的会话密钥进行一致性检验，确保在后续通信过程中双方使用一致的密钥对传输消息进行加解密。

万方数据

3.4.3 安全性分析

本文提出的基于椭圆曲线的身份认证方案，利用 ECC 数字证书和 ECDSA 签名算法以及 ECDH 密钥交换算法完成了无人机间的双向身份认证，可抵御重放攻击、中间人攻击。同时，采用基于椭圆曲线的认证方案，计算量较少，满足了无人机网络安全认证的轻量级需求。具体对无人机网络认证方案的安全分析如下：

（1）身份认证性

无人机接入网络时，需要提供证明其身份合法性的证书f_i并对所传输的认证消息m_r进行签名，使用 ECDSA 签名算法对认证信息进行签名验证来确定待接入网络无人机的身份，只有通过验证的无人机才能接入网络，身份验证失败时无人机不能够加入网络。因此该认证方案可以保证接入网络的无人机身份合法。

（2）抗假冒攻击

在无人机身份认证过程中，使用 ECC 数字证书和 ECDSA 签名算法对认证消息进行签名。攻击者接入网络时，需要提供合法的数字证书f_i，来证明自己身份的合法性与真实性。但攻击者无法得到由第三方可信任机构颁发的合法无人机证书。因此，该方案能够抗假冒攻击。

（3）抗重放攻击

无人机在认证过程中所传输的认证消息m_r均携带有随机数 R_0 和时间戳消息 T_0。在进行认证时，首先需要确认待入网的无人机所使用的随机数和之前的随机数不同，且消息时延在合理范围ε范围内，两者均验证通过后，无人机才可加入网络。否则，若攻击者使用一个截获的以前使用过的认证消息，则随机数 R_0 必定使用过，并且时间戳不符合消息时延要求。因此，该认证方案可抵御重放攻击。

（4）抗信息窃取攻击

无人机在进行身份认证时，使用接收方的公钥加密所传输认证消息随机数 R_0 和时间戳 T_0 和身份标识符 ID_A 传输加密后的密文 $E_{pubB}(R_0||T_0||ID_A)$。对于攻击者截获得到的认证消息m_r，若没有接收方私钥$Priv_i$是无法解密的。因为攻击者无法得到接收方秘密保护的私钥，进而无法得到发送方有效的身份信息。因此，该方案可以抵御无线劫持攻击。

（5）完整性保护

为提高无人机网络间认证的安全性，对所传输的认证消息使用哈希函数 SHA-1 和对称会话密钥 K 对认证消息 m 进行了摘要的计算。当接收方接收到数据报时，需要确认对该数据报计算所得的哈希值与接收到的哈希值是一致的，若不一致，则丢弃该数据包。只有两者值一致时，才对消息进行处理。因此，该方案可以保证传输消息的完整性。

（6）不可否认性

万方数据

在身份认证过程中，使用基于 ECC 算法的 ECDSA 签名算法对随机数 R_0 和时间戳 T_0 等认证信息进行签名，然后发送至接收方。当需要核对消息发送者的身份时，因为攻击者无法得到无人机的私钥$Priv_i$，所以其无法对消息进行签名。因此，该方案可以保证消息发送者对于消息的不可否认性。

（7）一致性检验

在双方身份认证通过后，使用哈希函数 SHA-1 对双方无人机所生成的会话密钥 K 进行哈希计算，并发送至对方无人机。确认接收到的哈希值与对生成的会话密钥进行哈希计算后的结果一致时，才能够说明会话密钥生成成功。否则，生成会话密钥失败。因此，该方案可以保证所生成的会话密钥是一致的。

3.4.4 认证方案性能测试

在对认证方案功能测试的基础上，完成了对基于 ECC 算法认证方案的性能测试，主要对比了在网络安全协议中比较流行的两种算法 RSA 和 ECC 的性能。

首先，从理论上分析了 DH 和基于 ECC 的 ECDH 密钥交换算法的性能差异，具体比较了 DH 密钥交换算法和 ECDH 密钥交换算法。DH 算法的安全性建立在离散对数求解比较困难的基础上，它的核心数学运算公式如下：

$$(g^a \bmod p) \bmod p = (g^b \bmod p) \bmod p \tag{3-2}$$

ECDH 密钥交换算法是在椭圆曲线有限域上实现的 DH 算法，数学运算公式可以表示为：

$$d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A \tag{3-3}$$

从数学公式的表示上可以看出，DH 的主要计算都是模幂运算，并且模幂运算通常进行的轮次比较多，计算量比较大。而椭圆曲线是一个集合，定义了一套计算规则，相比较于 DH 密钥交换算法计算量更小。具体使用 DH 算法和 ECDH 算法进行密钥协商交互过程的差异可以表示为如表 3.3。

ECDH 算法基于椭圆曲线上的点计算密钥，当把椭圆曲线上点的加法记作乘法时，原来的乘法就变成了幂运算，形式便和离散对数问题一致了。尽管两者形式一致，但并不等价，实际上椭圆曲线离散对数难题比大整数质因子分解（RSA）和 DH 难题要难得多。同时，ECDH 在计算共享密钥时将 DH 密钥交换算法中的模幂运算替换成点乘运算，计算量会小很多。因此，ECDH 的运算速度更快，可逆更难。

万方数据

表3.3 DH 算法和 ECDH 算法交互过程对比

步骤	DH 算法	ECDH 算法
初始化	加载 DH 参数，（主要是一个大素数 P 和系数 G），由 DH 参数决定密钥长度	加载双曲线，由双曲线决定密钥长度
服务器系数	公布 DH 算法的 P（大素数）、G、GY（G^Y mod P），保留私有数据 Y。其中 P、G 和 GY2 字节长度	公布双曲线 group 和公钥点 Q，保留私钥点 d。其中，曲线 ID 为 2 字节，Q 为 1 字节
客户端读取系数	读入 P、G,记录 GY 为服务器端公钥	读入双曲线算法 group，记录 Q 为服务器端公钥
客户端创建公钥	随机出 X，计算并公布 GX（G^X mod P），保留私有数据 X	生成并公布公钥 Q_p，保留私钥点 z
客户端计算密钥	根据 P、G、GY、X 计算出密钥	根据 group、Q、z 计算出密钥
服务器计算密钥	根据 P、G、GX、Y 计算出密钥	根据 group、Q_p、d 计算出密钥

另一方面，在保证了能够使用较小密钥实现较高安全等级的情况下，需要对所实现的认证方案进行性能方面的测试。首先，测试了生成不同长度 RSA 和 ECC 密钥所需要的时间开销。具体结果如图 3.9 所示。

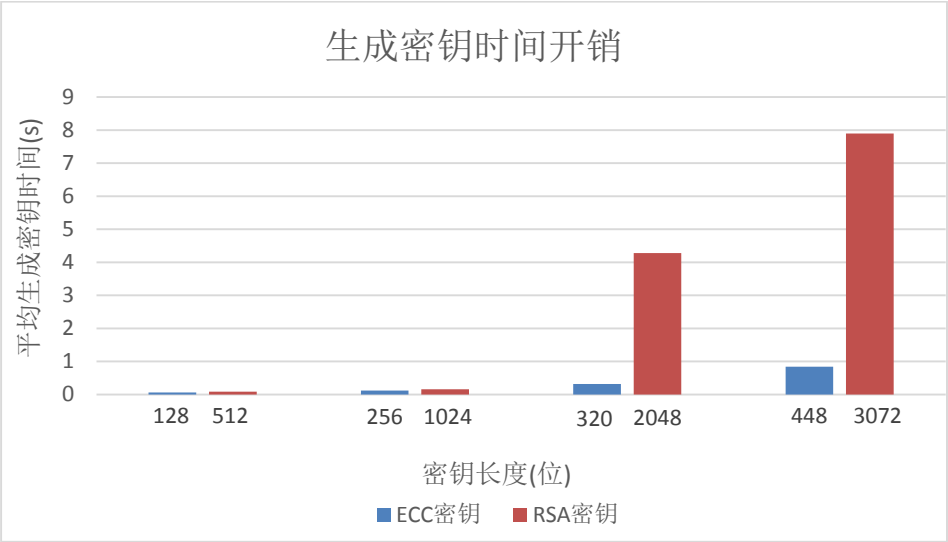

图3.9 生成密钥时间开销

从图 3.9 可以看出，生成 ECC 密钥的平均生成时间比 RSA 短，并且随着密钥长度的增加此性能优势更加明显。

其次，分别对 RSA 和 ECDSA 数字签名和验证签名的时间进行了测试。实验结果如图 3.10、3.11 所示。

万方数据

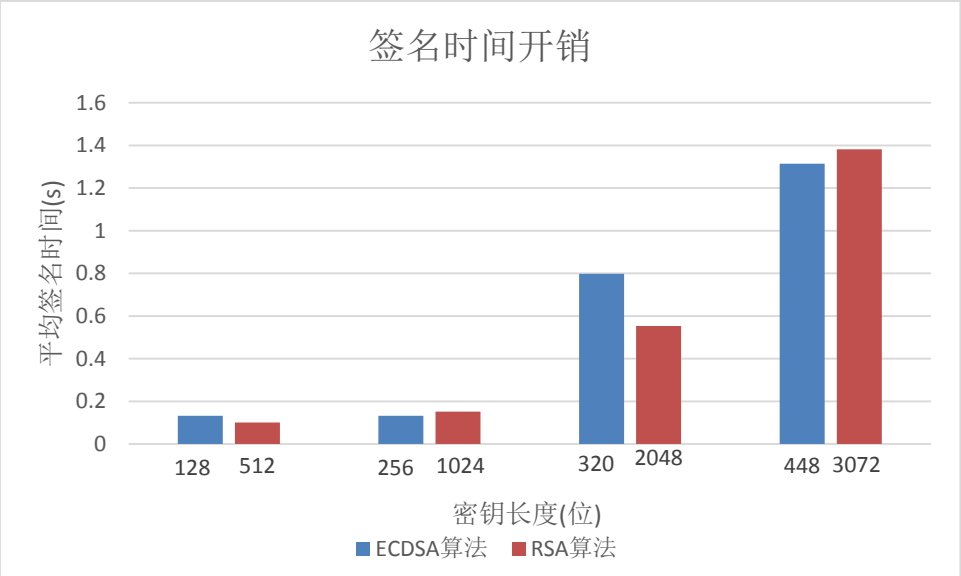

图3.10 签名时间开销

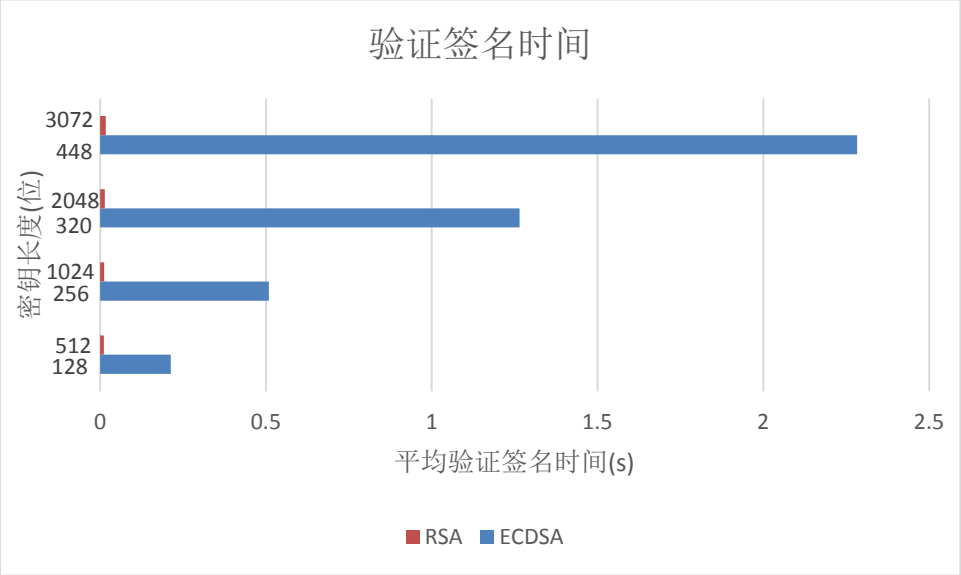

图3.11 验证签名时间开销

在密钥长度较小时，两者签名的性能差别不是很大，当密钥长度逐渐增大时，ECC的签名优势逐渐显现。RSA 验证签名性能比 ECDSA 更好，几乎可以忽略不计，但 ECDSA 验证签名时间随着密钥长度的增加而增加。

最后，对 DH 和 ECDH 密钥交换算法生成会话密钥的时间进行了测试。实验测试了生成 128 位、256 位和 512 位这三种长度密钥所需的时间。具体测试结果如图 3.12 所示。

万方数据

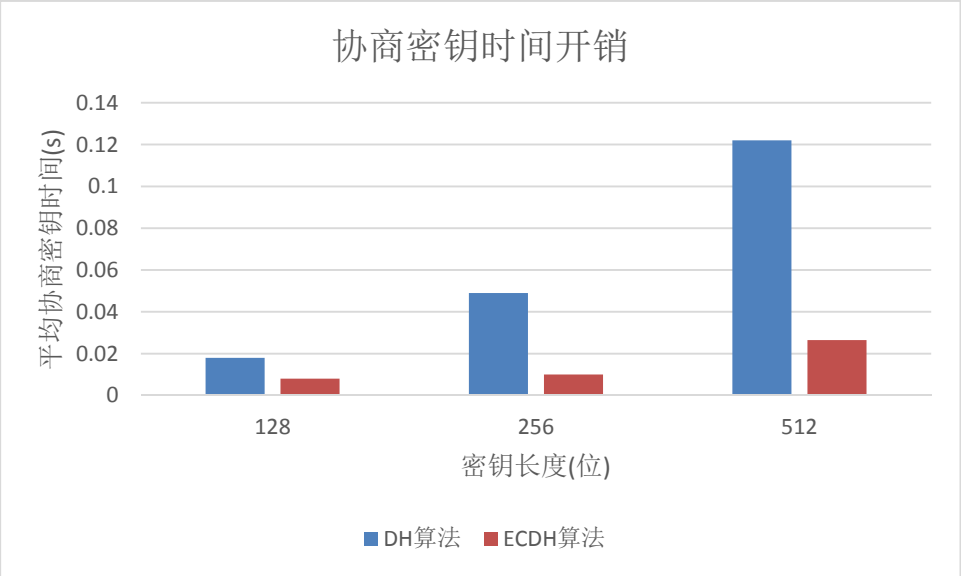

图3.12　　协商密钥时间开销

从实验结果可以看出，基于 ECC 算法的 ECDH 密钥交换算法比 DH 算法在生成相同长度密钥时所需要的时间更短，性能表现更好。

综合上述实验，在实现相同较高安全等级的认证时（如 210 位的 ECC 密钥就可以实现与 2048 位 RSA 密钥相同的安全等级），基于 ECC 算法的认证方案比基于 RSA 的认证方案性能表现更好。在计算和存储资源更小的设备上，密钥生成的计算成本可被视为选择签名算法的重要因素，较长的密钥不仅在计算时需要消耗大量的计算资源和带宽，并且在存储时也要消耗大量的存储资源。从实验结果可以看出最耗费时间的操作是密钥的生成，而 ECC 算法的密钥生成时间比 RSA 算法快了将近 10 倍。在签名和验证签名方面，当实现的认证安全等级较低时，RSA 与 ECDSA 签名算法的时间开销相差无几，随着安全强度的增强和密钥长度的增加，ECDSA 签名的时间比 RSA 要更短，RSA 算法验证签名的时间可以忽略不计，ECDSA 验证签名时间也保持着较低开销。最后，进行密钥协商时，ECDH 密钥交换算法性能明显比 DH 算法更好。

在实现无人机网络的安全性认证时，至少需要 2048 位的 RSA 密钥才能保障其安全性，而 RSA 体制在长密钥下的性能表现较差。此时可以用基于 ECC 体制的认证方案，不仅能够实现相同的安全等级，还能以更小的密钥长度和更好的性能优势满足无人机网络认证的轻量级需求。因此，在进行身份认证时，综合考量密钥生成时间、签名时间、验证签名时间和密钥协商时间，本文认为：基于 ECC 算法的认证方案能够以较小的计算量实现较高安全性，这种性能优势在资源受限的设备（如嵌入式系统）中具有重要的意义。

万方数据

3.5 本章小结

本章首先介绍了无人机网络身份认证的安全需求和攻击者模型。然后介绍了基于椭圆曲线 ECC 算法的轻量级身份认证方案。最后，为了说明本章所提出认证方案的有效性和轻量级，对所设计的认证方案进行了安全性分析，并在模拟环境下对所开发的软件进行了功能测试和性能测试，并与基于 RSA 算法的认证方案进行了对比。功能测试部分说明本认证方案能够完成对通信双方无人机身份的认证功能并能够生成后续通信所需的会话密钥。性能测试部分证明了所设计的认证方案具有轻量级的特性，具体表现在实现相同安全强度下所需的 ECC 密钥比 RSA 密钥长度要短的多，并且基于 ECC 算法的密钥生成、ECDSA 签名算法和 ECDH 密钥交换算法所需要的总时间比基于 RSA 算法的认证方案要短。

万方数据

万方数据

第四章 轻量级安全通信机制

由于无人机网络的开放式特性，其外部的环境复杂，具有潜在的风险，容易受到各种攻击。攻击者会破坏无人机之间的连接，截获通信链路上传输的信息，干扰无人机间的任务消息，因而要求我们对无人机节点间数据进行加密。当前主流的无人机网络通信采用对称加密算法，速度较快但针对网络丢包问题表现出健壮性较差。本章的创新点在于提出了一种基于 SM4 算法的加密通信方案，并对 SM4 算法的流加密模式（CTR）进行了改进，与传统的 SM4_CTR 算法相比加解密速度提升了 7.7%，与 ChaCha20 流加密算法相比更能容忍丢包。

4.1 无人机网络通信安全需求

目前，针对无人机网络通信所存在的安全威胁，是由于缺乏加密和其他保护机制而导致的在开放环境下设备之间交换信息的泄露，容易被其他攻击者直接访问。由于安全机制的不够完善而导致的无人机网络中存在着巨大的安全隐患，因此，为了实现无人机群之间安全的信息交换，无人机网络安全通信方案应该实现的安全目标包括：

身份匿名：使用长期身份可能会导致隐私泄露，符合条件的方案应提供身份匿名，以确保攻击者无法从窃听或捕获的消息中获取用户的真实身份。

消息可用性：即使在受到攻击时也要保持通信，特别是在高压力时期，对于成功的军事行动至关重要。可用性可能受到电子装置干扰或通过操纵网络的影响。在后一种情况下，可以损坏或修改路由信息，或者可以将大量流量引导到各个节点或用户。可用性被定义为网络安全的关键特征，这意味着无人机可以在必要时提供有效的服务，即使它受到攻击。

消息机密性：对于复杂环境中的无线网络，消息机密性是必不可少的安全要求，在没有消息机密性的情况下，任何对手都可以通过简单地拦截无线信道来获得敏感信息。因此需要机密性相关机制确保无人机之间的通信信息不能被泄漏。

消息完整性：完整性是指接收者可以确信他获得的消息来自有效的发送者并且在传输过程中没有以某种方式被更改。因此，完整性监视包括防止通信路径中间的人或者通信路径中的错误（包括无线信道错误）中的消息修改。如果不使用完整性机制保护整个网络，那么整个无人机网络可能会受到攻击者的恶意攻击或者遭受无线信道的干扰，从而导致所传输的信息被破坏。

计算机网络防御：是保护无人机系统内部的新关注点，用来保护网络的一种方法，特别是支持通信和保护网络数据的路由表网络，阻止访问或修改数据文件。

万方数据

以上介绍了无人机网络所要满足的安全需求，除此之外，由于无人机和智能物体采用电池供电，因此能效也是另一个关键性的问题。在进行无人机安全机制的设计时，应尽快完成协议的执行以节省能源的消耗。同时，针对无人机系统计算资源的受限性，所使用的加解密算法应该具有良好的性能优势，能够实现以较快的计算速度完成数据的加解密操作。为了满足无人机网络通信安全和性能需求，需要设计并实现一种安全有效的轻量级安全通信方案。

4.2 攻击者模型

无人机网络中各节点间通信时，攻击者可能发起各类攻击以获取网络中传输的敏感信息，本文假设攻击者可以在网络通信过程中发起信息窃取、篡改和中间人攻击，攻击示意图如 4.1 所示。

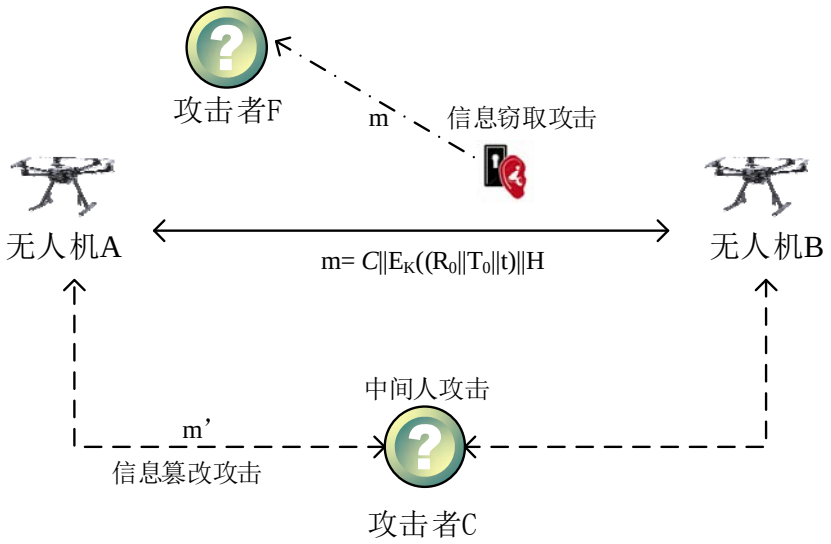

图4.1 攻击示意图

将明文信息定义为变量 P，计数器序列表示为变量 T，对计数器序列使用 SHA-1 函数计算得到 X 序列值，无人机公钥Pub_i、无人机私钥$Priv_i$，加密函数 E 和解密函数 D 用以实现对数据的加解密操作。同时将无人机传输的信息定义为：

$$m= C||E_K(T_0||R_0||t||H) \tag{4-1}$$

其中 C 是明文变量 P 与 X 序列值异或得到的密文消息变量，T_0表示初始计数器值，H 表示所传输消息的摘要值，R_0 表示随机数和t表示时间戳，||表示连接符，$E_K(T_0||R_0||t||H)$表示基于协商密钥 K 使用改进的 SM4 算法加密需要保护的数据 T_0, R_0, t, H。

万方数据

（1）信息窃取攻击

无人机在开放环境下传输数据时，数据将以 m=C||E$_K$(T_0||R$_0$||t||H)的数据报格式在通信链路上传输，攻击者 F 可以不使用物理或其他分析设备就能够在覆盖了无线网络信号的范围之内，监听并得到通信双方无人机间传输的信息 m，若攻击者掌握了协商密钥 K，便可以得到T_0从而可以推断出明文信息 P。

（2）信息篡改攻击

攻击者 C 可以利用一些技术或者工具捕获网络中传输的信息 m，并对消息进行篡改得到虚假的信息m'，并将虚假信息m'发送给网络中的节点，使网络中的接收方无人机接收虚假的错误信息并对虚假错误进行处理，干扰无人机间正常通信。

（3）中间人攻击

攻击者 C 能够与相互通信的双方无人机 A、B 分别建立联系，并对实线链路上所传输的信息 m 进行截获并篡改得到消息m′，并将m′通过虚线所示路径转发给 B，使通信的双方无人机误以为他们正在通过私密的连接与对方直接对话。通过这种方式，攻击者可以在整个会话期间控制双方无人机的通信。

4.3 轻量级安全通信方案

基于 4.1 节对无人机网络安全和性能两方面的需求分析，由于无人机网络的开放式特性，其外部的环境复杂，具有潜在的风险，容易受到各种攻击。攻击者会破坏无人机之间的连接，截获通信链路上传输的信息，干扰无人机间的任务消息，因而要求我们对无人机节点间数据进行加密。当前主流的无人机网络通信采用对称加密算法，速度较快但针对网络丢包问题表现出健壮性较差。为了解决通信网络受到外界因素干扰的影响而造成的因传输信息丢包而无法正常解析的安全缺陷问题，要求设计能够容忍非实时数据丢弃导致密文无序、密文分组丢失的高健壮性安全通信方法。

因此我们提出使用基于对称分组密码 SM4 算法的流密码运行模式（CTR 模式），并对该算法进行改进，高效地实现了 CTR 模式会话密钥的协商，并基于改进的 CTR 模式设计实现了支持高实时性、容忍密文无序的加解密。同时使用 HMAC 算法保证传输消息的完整性。

万方数据

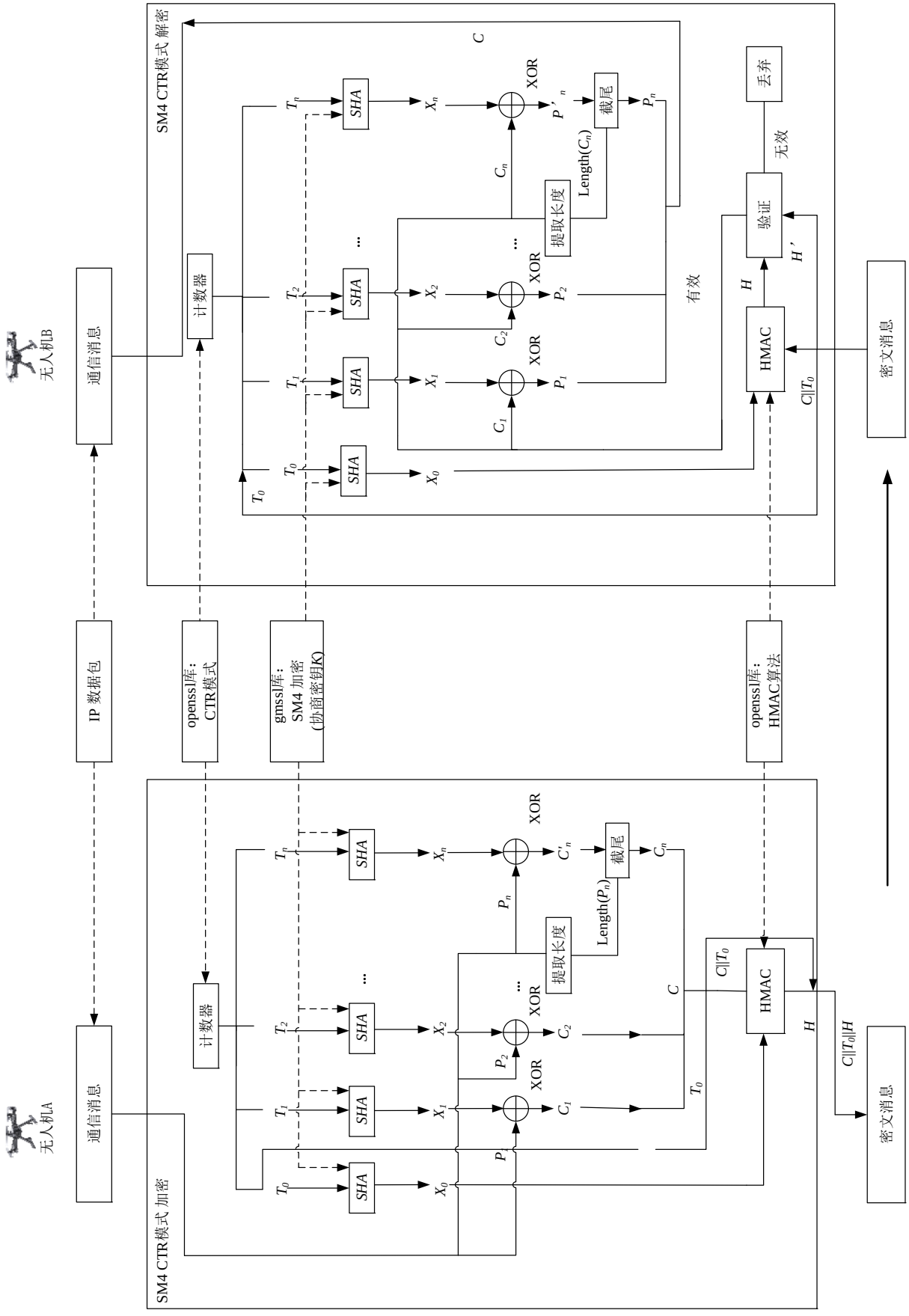

图4.2 轻量级端到端安全通信方案

万方数据

轻量级安全通信方案所使用的 SM4 算法是一个分组算法，是为低功耗芯片应用领域所设计的加密算法，因此特别适用于具有低功耗芯片的系统使用。该算法对于分组和密钥的长度都有具体的要求，均为 128 比特。使用 SM4 进行加密和解密时的结构相同，唯一的不同之处在于加密时轮密钥的使用顺序和解密时是相反的。SM4 算法的优势在于其算法设计简单，结构有特点，安全并且高效，符合轻量级安全通信机制的要求。

流密码运行模式（CTR 模式）通过使用计数器产生递增连续的长时间不重复的加密密钥流。使用 CTR 模式能够允许其在解密时随机地进行存取，同时可以并行处理加密和解密操作，因此多处理器的硬件可能更适合使用 CTR 模式进行加解密。CTR 模式的加密原理是基于计数器序列加密产生一个 16 字节的伪随机码块流，然后与明文进行异或，生成最后的密文。同理，将密文与同样的伪随机码进行异或后可以重新产生明文。相对于其他模式而言，CTR 模式可以同时多处理多块明文/密文，并且可以并行计算，使用异或运算加密可以极高地提高吞吐量，CTR 模式仅使用同一种算法便可以进行加密和解密操作，因此可以高效地作为流加密使用。

传统 SM4 算法 CTR 模式在进行加解密时，使用密钥加密计数器序列后的输出与明文异或产生密文，其中加密计数器序列使用加密算法 SM4，这项操作将消耗大量时间。由于哈希计算时的开销比加密算法要小，因此本轻量级通信方案使用哈希算法 SHA-1 对对计数器序列进行哈希计算而不采用传统使用加密算法加密的方法。

具体的通信方案设计如图 4.2 所示。从图中可以了解到轻量级通信的具体方案。系统 A 将明文消息交给 CTR 模式加密，系统 B 收到密文消息通过 CTR 模式解密。为保证消息传输的完整性，采用轻量级 HMAC-SHA1 生成每个消息的摘要，添加在密文后，以验证系统 A 和系统 B 间消息传输的完整性。CTR 模式的 SM4 算法可以保证系统 A 与系统 B 间实时有序的安全通信。为保证 CTR 计数器的安全性，在 CTR 计算器用完一轮后重新协商密钥，保证端到端通信的安全性。

具体地，可以将所设计的轻量级通信方案分为密钥更新、数据加解密和数据完整性检验三个部分。

4.3.1 密钥更新

为实现基于 CTR 加密模式的容忍密文无序的安全通信，首先通过密钥交换得到 CTR 所需的加密密钥。由于会话周期的时效性，需要考虑会话密钥的更新问题，从而防止因密钥泄露导致信息被窃取威胁的发生。

根据第三章所述的轻量级身份认证过程，设置 K 和 K'（二者相等）即为通信双方的会话根密钥。根据生成的会话根密钥，协商每次通信的会话密钥，并设置更新机制，定期更新会话密钥，以避免密钥长期使用导致的会话密钥安全性降低。设计会话

万方数据

密钥的有效期为 30min，通信双方使用单向散列函数计算当前密钥的散列值，并将这个散列值用作新会话密钥。简单说，就是用当前密钥的散列值作为下一个密钥来更新密钥，具体过程如图 4.3 所示。

其中，密钥更新过程中的消息摘要计算算法是基于 SHA-1 接口实现的。通过上述的密钥更新方案，可以保证会话周期的有效性。密钥交换后，需要采用加解密算法对无人机网络中所传输的数据进行加解密操作。具体地，可以基于对称加密算法 SM4 的流加密模式（CTR 模式），并对 CTR 模式进行改进实现对于数据的加解密并提高加解密的效率。

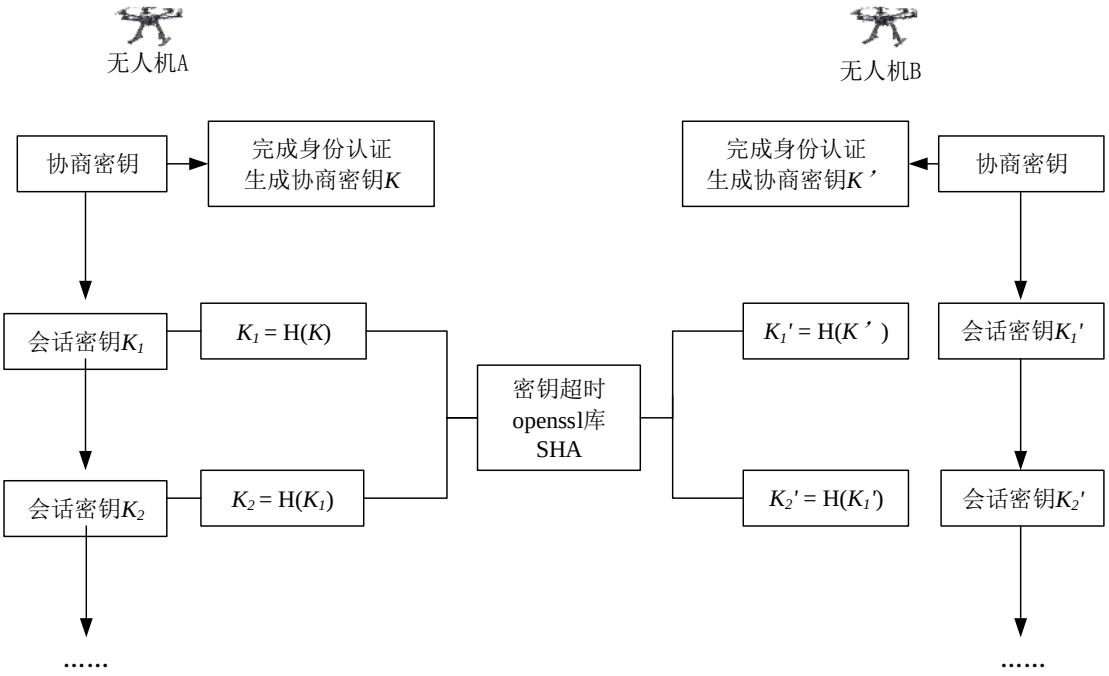

图4.3 会话密钥更新过程

4.3.2 数据加解密算法

为保证密钥流的安全性，对 SM4 算法的 CTR 模式进行改进，高效地实现了 CTR 模式的加解密。SM4 算法对长度是 128 位整数倍的明文数据进行加解密操作，因此首先需要将明文消息分为 128 位长度的分组。定义明文消息 P 为 n 个明文变量 P_1，P_2，...，P_n 所组成的序列（其中，P_1，P_2，...，P_n 为 128 位，P_n 为 m 位）；使用 128 位协商密钥 E_k；n 个计数序列 T_1，T_2，...，T_n，每块都为 128 位；n 个密码输出块 X_1，X_2，...，X_n，每块都为 128 位；密文变量为 C_1，C_2，...，C_n（其中，C_1，C_2，...，C_{n-1} 为 128 位，C_n 为 m 位）；明文消息的消息摘要变量 H 为 128 位。具体地，所设计的轻量级安全通信加解密算法可以描述如下。

万方数据

算法 4.1 轻量级加解密算法

输入：明文数据 Plaint；

输出：密文变量 C，密文所对应的哈希值 H，并将 C、H 和初始计数器值 T0 合并为 Msg 发送给对方无人机。

```
1  Procedur CreateCipher()
2        P  ← SplitPlaint() ;
3        T0 ← ComeRandom(); /*产生计数器初始值 T0*/
4        T  ← CountSerial() ; /*产生计数器序列 T*/
5        for T[i] ∈ T  do /*对计数器序列 T 使用 SHA-1 进行哈希计算*/
6             X[i] ← HashCompute(T[i]);
7        C ← Xor(P, X);  /*将明文和加密后的随机数序列异或后产生密文 C*/
8  End Procedure
9  Procedure PacketAndSend()
10       H ← HMAC(X0，C) ; /对密文变量生成哈希值 H*/
11       Msg ← Packet(C，H，T0);  /*将 C、H 和 T0 封装成消息 Msg 发送*/
12       sockfd ← new socket(IP，Port，0);
13       sendto(Msg，dest); /*发送数据至目标飞行器*/
14       sockfd .close();
15 End Procedure
```

从算法 4.1 来看，轻量级加解密算法可以分为数据加密（第 1~8 行）、数据封装和数据发送（第 9~15 行）两个阶段。实际开发时，首先在进行数据加密时需要将明文数据分为长度 128 位的明文变量分组，并对产生的计数器序列使用 SM4 算法进行加密，并于明文变量进行异或操作生成密文。对于通信过程中针对密文生成的摘要值是基于 SHA1 算法生成。接着，要向目标飞行器发送加密后的密文变量，并使用套接字建立连接并发送数据。进行通信的双方具体步骤可以描述如下:

发送方 A：

（1）将明文数据 P 切分成 n 个明文变量 P_1，P_2，. . . ，P_n；

（2）首先生成 HMAC 的密钥 $X_0=E_k(T_0)$，128 位。

（3）对计数序列进行哈希计算：$X_i=HMAC_{k_i}(T_i)$，$I=1,2$，…,n，其中使用 SHA-1 进行哈希计算；

（4）对明文数据 $i=1,2$，…,n-1 产生密文变量：$C_i=P_i\oplus X_i, i=1,2$，…，n-1。对于，最后未满 128 位的明文分组首先生成密文变量 $C_n=P_n\oplus X_n$，然后对密文变量根据明文数据截取得到最终密文变量 C_n。

（5）对密文消息以及初始计数器进行 HMAC，生成消息摘要变量 $H=HMAC(X_0,C||T_0)$。

（6）将密文变量、计数器与消息摘要变量连起来 $C_1||C_2||...C_n||T_0||H$ 组成密文数据

万方数据

发送给系统 B，并标识密文变量的序号。

系统 B：

（1）收到密文数据，首先按消息格式分解成密文消息 C、初始计数器 T_0 和消息摘要变量 H。生成 HMAC 的密钥 $X_0=E_k(T_0)$。

（2）生成密文消息和初始计数器的消息摘要 $H'=HMAC(X_0,C||T_0)$。判断消息摘要与接收的消息摘要是否一致 $H=H''$。不一致直接丢弃明文消息，若一致，继续下一步。

（3）将完整性验证通过的密文数据分解成密文变量 C_1，C_2，...，C_n。对计数序列加密：$X_i=HMAC_{k_i}(T_i)$,i=1,2,…,n。

（4）对密文数据 i=1,2,…,n-1，产生明文变量 $P_i=X_i\oplus C_i$。最后一个密文数据首先生成明文变量 $P_n'=X_n\oplus C_n$，并截取明文变量生成 P_n。

（5）最终将明文变量 P_1，P_2，...，P_n 组成明文数据，完成系统 A 与系统 B 之间的安全通信。

无人机网络合个嵌入式系统之间的相互通信过程如上所述。基于 SM4 分组加密算法的 CTR 模式对传输消息进行加解密，从而保证所传输消息的机密性。

4.3.3 数据完整性检验

为保证消息传输的完整性，通常使用事先约定的密钥对所传输的信息进行哈希计算。由于哈希函数是单向的，所以即使信息泄露，攻击者所能够得到的信息只有随机数和 HMAC 结果，并不能够根据这两个数据计算得到密钥信息。因此通信的双方可以根据发送的哈希值和接收到的消息计算出 HMAC 的值，并比较两者是否一致，从而验证消息传输过程中消息是否被篡改。本文采用轻量级 HMAC-SHA1 生成每个消息的消息摘要，添加在密文后，以验证系统 A 和系统 B 间消息传输的完整性。

HMAC 基于 HASH，但是相比较于 HASH，又多了密钥的加密，因此安全性上相比相同的 HASH 要高。HMAC 中使用的单向散列函数并不仅限于一种，任何高强度的单向散列函数都可以被用与 HMAC。本通信方案中采用 SHA1 哈希算法，当消息的长度不超过 2^64 位时，最终的消息摘要结果都会是 160 位。

根据 2.3 节所描述的 HMAC 基本原理， HMAC 算法除了需要信息摘要算法外，还需要一个密钥。HMAC 的密钥可以是任何长度，如果密钥长度超过了摘要算法信息分组的长度，则首先使用摘要算法计算密钥的摘要作为新的密钥。一般不建议使用太短的密钥，因为密钥的长度与安全强度是相关的。通常选取密钥长度不小于所选用摘要算法输出的信息摘要的长度。在我们所设计的轻量级安全按通信方案中，我们使用 SM4 加密算法加密计数器初始值 T0，作为 HMAC 的密钥。

使用 SHA1 哈希函数和加密初始计数器值的密钥生成消息的摘要，并添加在密文

万方数据

后发送至对方。当对方接收到消息的时候，这个消息摘要可以应用来验证数据的完整性，从而验证通信过程中消息是否被篡改。

4.4 实验与分析

实验所需要的环境同第三章认证方案的测试环境相同。首先需要部署进行实验的硬件环境，其次将轻量级通信方案的代码移植到 VxWorks6.9 开发板进行测试。

4.4.1 通信方案功能测试

根据无人机网络安全通信的具体要求，对所设计的通信方案进行了功能性测试，具体包括会话密钥的更新、数据加解密正确性测试和数据完整性检验的测试、时延结果如表 4.1 所示，具体实验测试界面如图 4.4。

实验结果显示，我们所设计的基于分组加密算法的轻量级安全通信方案，能够在无人机网络仿真环境下使用 SM4 分组加密算法的流加密模式（CTR 模式）对明文数据进行正确的加解密操作，完成无人机间安全的通信。并在通信过程中能够定期更新密钥，保证了加密通信的有效性，有效阻止了因密钥泄露可能引起的信息泄露问题。同时，对所传输的消息使用 HMAC 进行了数据完整性检验，通过比较发送所得到的消息摘要与基于消息计算所得的摘要是否一致来判断传输过程中消息是否被篡改或者截取。界面显示中的客户端和服务器端可以是无人机设备或地面站设备。综上所述，本章所设计的轻量级通信方案能够满足无人机网络安全通信的功能需求。

表4.1 通信方案功能测试结果

功能	测试项目	测试结果
会话密钥更新	通信时长超过 30 分钟，检查密钥是否更新	密钥更新，测试通过
数据加解密正确性	使用所设计通信方案中加密算法加密一段数据明文，再使用解密算法解密，查看解密后数据是否和明文数据一致	解密后与明文数据一致，测试通过
数据完整性检验	检查发送得到的消息摘要与计算消息所得摘要是否一致，同时对比接受到的消息与发送消息是否一致	计算结果一致，接收数据与发送数据相同，测试通过

万方数据

```
-> server
listening......
connect to client 192.168.0.205!
child created : 2749
receive data from client!
H equals to H'!
decrypted success : 12345678!
----------------------
send to client
plaintext: : abcdefgh!
communication time : 31 minutes!
Key negotiation restart!
Negotiation key create success!
```

(a) 通信测试服务器端输出

```
-> client
connect to server!
plaintext : 12345678!
sm4 encrypt success!
send ciphertext to server!
------------------------
receive data from server!
H equals to H'!
decrypte success : abcdefgh!
communication time : 31 minutes!
Key negotiation restart!
Negotiation key create success!
```

(b) 通信测试客户端输出

图4.4通信测试输出结果

4.4.2 安全性分析

本文提出的无人机安全通信方案，使用改进的 SM4 流密码运行模式对所传输的明文信息进行加密，可抵御网络窃听、中间人攻击。同时，在传统 SM4 流密码运行模式的基础上进行了改进，提高了算法加解密的性能，满足了无人机网络安全通信的轻量级需求。具体对无人机网络通信方案的安全分析如下：

（1）高效性

实现的无人机网络节点间高健壮性安全通信方法，能够容忍因为环境干扰导致的密文无序、非实时数据丢失导致的密文无法正常解密，与传统的 SM4_CTR 算法相比加解密速度提升了 7.7%，与 ChaCha20 流加密算法相比更能容忍丢包。

（2）抗信息窃听攻击

无人机间进行安全通信时，使用加密机制对所传输的计数器初始值T_0、随机数R_0和 t 进行了加密。攻击者只能监听得到加密后的密文消息 $E_K(T_0, R_0, t)$，攻击者需要协商密钥才可以解密得到明文信息。但攻击者无法得到双方无人机计算所得的协商密钥 K，因此该安全通信方案可以抵御网络窃听。

（3）抗信息篡改攻击

无人机间进行通信时，使用 SHA-1 对所传输的信息进行了哈希计算，并使用 SM4 加密算法对信息摘要值 H 进行了加密 $m= C||E_K(T_0||R_0||t||H)$。攻击者发送篡改后的消息m′，接收方对m′重新进行哈希计算得到H′并与信息中的哈希值 H 进行比较，只有当两者结果一致时才对消息进行处理，不一致时丢弃该消息。哈希函数是单向的，若消息经过篡改，则 H 与H′的值必然不一致，同时攻击者也无法修改 H 的值与H′使其保持一致，因为攻击者需要使用协商密钥 K 解密得到 H 的值。但攻击者无法得到协商密钥 K 的值，因此该方案可抵御信息篡改攻击。

万方数据

（4）抗中间人攻击

无人机安全通信时使用加密机制对所传输的信息进行加密来提高网络通信的安全性。攻击者所截获的传输消息 m，并转发经过篡改后的消息m′。接受方在接收到消息时需要使用SHA-1函数计算消息的摘要值以检测消息是否在传输过程中遭遇篡改，首先接受方需要使用协商密钥K解密得到H的值，与计算所得的摘要值H′进行比较，只有当 H 与H′一致时接受方才处理消息。由于哈希函数是单向的，消息m′的摘要值与消息 m 的摘要值必然不一致，同时攻击者也无法修改 H 的值与H′使其保持一致，因为攻击者需要使用协商密钥 K 解密得到 H 的值。但攻击者无法得到协商密钥 K 的值，因此该方案可以抵御中间人攻击。

（5）机密性

无人机间的通信内容均使用SM4流加密模式进行加密后以$m=C||E_K(T_0||R_0||t||H)$消息格式传输，由于加密所使用的密钥是使用密钥交换算法生成的对称密钥 K，被秘密地保存在双方无人机本地密钥管理区。在通信过程中每隔三十分钟对协商密钥K进行更新，并使用会话密钥 K 对传输的数据进行加密，确保了双方通信内容的机密性。

（6）完整性保护

无人机网络在通信报文中添加有传输消息的哈希值 H。攻击者对消息 m 进行篡改后得到m′发送至接收方无人机。接收方接收到数据报时，需要确认该数据报计算所得的哈希值H′与接收到的哈希值 H 是一致的，若不一致，则说明所传输的消息不完整并丢弃该数据包。只有两者值一致时，才对消息进行处理。因此，该方案可以保证传输消息的完整性。

4.4.3 通信方案性能测试

本轻量级通信方案对计数器序列进行哈希计算而不采用传统加密算法加密的方式，由于哈希计算时的开销比加密算法要小，因此所改进的轻量级安全通信方案在理论上性能比原始 SM4_CTR 要好。为了验证所设计的轻量级安全通信方案性能，需要在模拟环境下进行性能测试。

根据文献[52]，为了提高无人机群之间的通信安全性，对目前比较常用的几个加密算法包括 AES 加密算法的计数器模式（GCM）和 ChaCha20-Poly1305 算法在不同密钥长度下进行了加解密速度和吞吐量方面的性能测试对比，其中 ChaCha20 表示流加密算法，Poly1305 表示消息认证码。实验结果表明，ChaCha20 算法性能优越。本文将所设计的轻量级通信方案与 ChaCha20 算法和 SM4_CTR 加密模式进行了比较，具体可以从算法加解密速度、通信时间开销和容忍丢包三个方面比较这三种加解密算法的性能。

（1）算法加解密速度

万方数据

我们分别对 1KB~2MB 之间的多组数据进行了多次加解密，测试轻量级通信方案、ChaCha20 和 SM4_CTR 加解密速度方面性能的差异，并测试了加密和解密不同数据大小时两种算法的时间开销，并绘制程如图 4.5 和图 4.6 所示的结果。

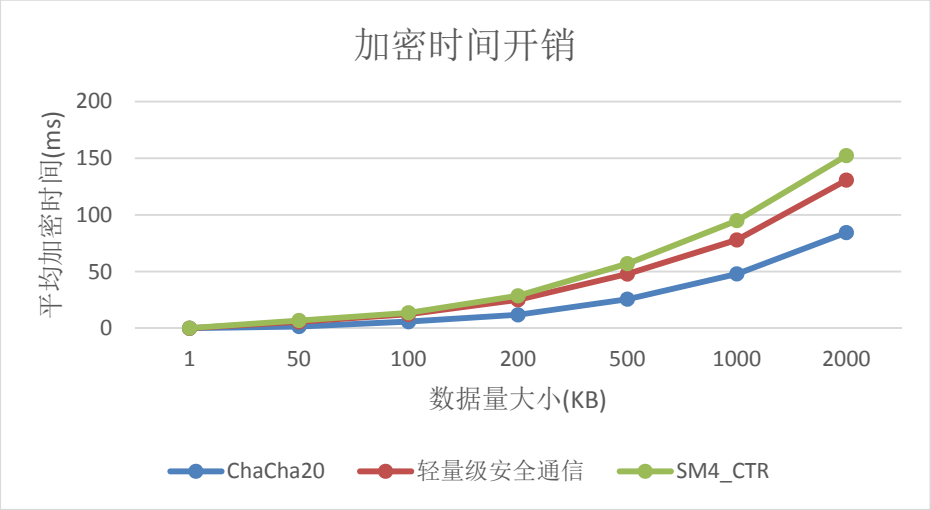

图4.5 加密时间开销

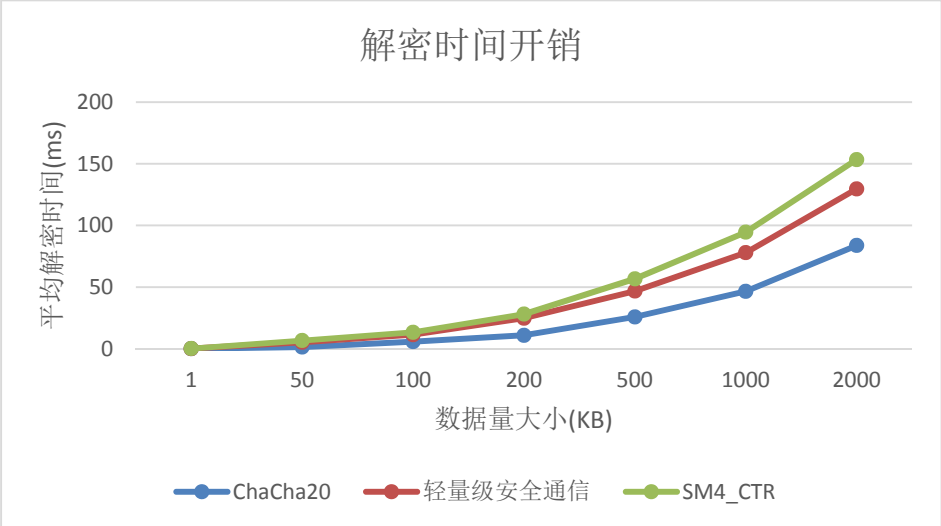

图4.6 解密时间开销

通过对比可以看出，当数据量较小时，三种算法加解密所需要的时间开销几乎差不多。但当数据量变大时，ChaCha20 的性能最好，其次是轻量级加解密算法，SM4_CTR 性能最差。

（2）算法通信开销

为了测试三种算法在通信开销方面的差异，首先从理论上分析三种算法传输密文所需要的时间开销。SM4 分组加密的流加密模式（CTR 模式）的加密原理是将所产

万方数据

生的伪随机码块流和明文变量进行异或运算后生成最后的密文变量。同理，将密文与同样的伪随机码进行异或后可以重新产生明文。SM4_CTR 加解密算法原理是将加密后的密钥与明文异或得到密文。因此，从理论上分析，使用 SM4 的 CTR 模式加密相同数据所产生的密文长度应该和明文长度是一致的。而流加密算法进行加解密的原理就是使用异或计算和密钥产生一个随机码流，然后和明文数据进行异或产生的密文。解密操作也是将随机码流和密文异或操作后得到明文。因此，流加密的密文长度和明文数据也是一致的。

从理论上分析，通信所需的时间开销和通信链路上所传输消息的长度是息息相关的，而这两种算法加密相同长度明文所产生的密文长度也是相同的。因此，从理论分析角度来讲，三种算法的通信时间开销应该是相同的。

另外，为了验证理论分析的正确性，我们对 1KB~2MB 之间的多组明文数据进行加密，并将密文发送至对方无人机。测试对不同长度明文数据进行加密后传输密文的通信时间开销，三种算法的通信时间开销结果如图 4.7 所示。

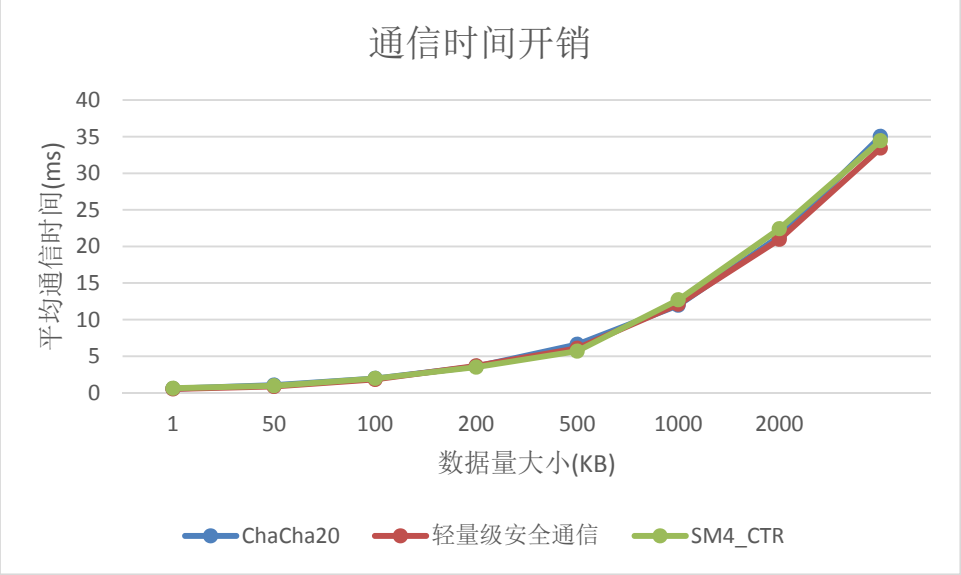

图4.7 通信时间开销

从图中可以看出，使用三种加密算法对 1KB~2MB 的明文数据加密后，传输密文所需要的时间基本是吻合的。因此，从实验角度也验证了我们理论分析的正确性。

（3）容忍丢包的性能

无人机网络中节点间的通信兼具强实时性和高安全性要求，要求设计能够容忍非实时数据丢弃导致密文无序、密文分组丢失的高健壮性安全通信方法。因此，需要测试所设计通信方案容忍丢包的能力。测试时，模拟网络丢包，测试在不同丢包率下算法所能解密出明文数据的百分比。具体地，分别测试在 1%~100%内多个丢包率下，

万方数据

我们所设计的通信方案对应所能够解密出的明文百分比。同时，在相同丢包率下测试使用流加密算法 ChaCha20、SM4_CTR 和轻量级安全通信中使用的加解密算法所能够解密出的明文百分比。将三者的测试结果进行对比，证明本通信方案支持健壮性，具体地，即丢失掉的数据包对解密其他密文无影响。测试结果如图 4.8。

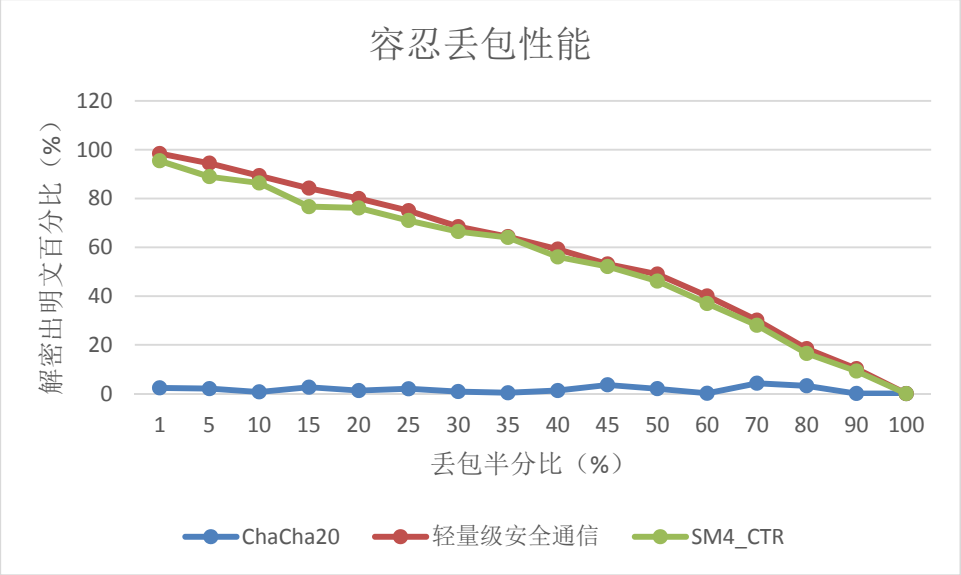

图4.8 容忍丢包性能

从图中可以看出，流加密算法 ChaCha20 在不同丢包率下所能解密出的明文数据接近 0，即 ChaCha20 流加密算法不能够容忍丢包，接收方对于不完整的密文数据无法解密得到明文。而轻量级通信方案和 SM4_CTR 能够容忍丢包，对于环境变化或链路干扰造成的丢包问题，接收方能够对接收到的不完整密文信息解密，提高了通信过程的健壮性。

综上所述，从加解密速度和通信开销两个方面比较轻量级安全通信方案、SM4_CTR 加密模式和流加密算法 ChaCha20 算法的性能。实验结果表明，轻量级安全通信方案的加解密速度比 ChaCha20 慢，比 SM4_CTR 快。但 ChaCha20 算法不能容忍丢包，即当通信链路或外部环境造成数据丢包时，接收方对于接收到的不完整的密文信息不能够解密得所对应的明文信息。但轻量级安全通信方案和 SM4_CTR 具有容忍丢包的能力，能够将接收到的不完整的密文解密得到明文信息，即丢失的数据包对于解密其他密文没有影响，提高了通信过程的健壮性。因此，本文提出的轻量级安全通信方案的具有更快的加解密速度和容忍丢包的能力，更能满足无人机网络各个设备之间安全通信需求。

万方数据

4.5 本章小结

鉴于无人机网络具有拓扑结构动态变化和易受自然环境影响等特点，为了满足不同无人机节点之间的信息安全交互需求，同时考虑到物理资源有限的实际情况，设计并实现了轻量级的安全通信技术方案。首先具体分析了无人机网络通信的安全需求，并针对这些安全需求设计出支持健壮性的轻量级安全通信方案。然后，设计并改进了SM4 的 CTR 模式，实现了支持高实时性、容忍密文无序的安全通信方法。根据所设计的轻量级安全通信方案实现对于通信数据的加密传输，并基于 HMAC-SHA1 对传输数据进行完整性检验。最后，对所设计和实现的轻量级安全通信方案进行了功能和性能方面的测试，并与流加密算法 ChaCha20 和 SM4_CTR 模式进行了性能对比。实验结果证明本章所设计的轻量级安全通信方案性能较好，能够满足无人机网络中实时系统之间的通信需求，并能够容忍网络丢包。

万方数据

第五章 总结与展望

5.1 本文总结

无人机网络是一种开放式的系统网络，具有动态拓扑、灵活接入和计算节点物理资源有限的特点，在民用、军用、商业和政府部门有关领域具有广泛的应用。无人机网络容易受到外部恶劣环境影响，面临诸多安全威胁，如伪造攻击、中间人攻击、重放攻击、信息泄露或篡改等。本文针对无人机网络中无人机节点之间存在的信息交互需求，为了保证通信双方身份的真实正确和传输信息的安全性，同时鉴于计算节点物理资源有限的特点，开展了远程安全接入与安全通信技术研究。

（1）在身份认证研究方面，本文针对传统基于 RSA 签名算法的 RSA 数字证书验证方法的不足之处，提出了基于椭圆曲线 ECC 算法的无人机网络身份认证方案。使用 ECC 数字证书作为合法无人机的身份证明，同时使用计算量和资源消耗更小的基于椭圆曲线的 ECDSA 签名算法对节点身份进行签名验证，并使用 ECDH 密钥交换算法生成通信所需要的会话密钥。对接入无人机网络中的节点身份进行验证后，对生成的会话密钥进行了密钥一致性检验。

为了说明基于椭圆曲线 ECC 算法认证方案的有效性，对所设计的轻量级认证方案在实际的多节点无人机网络环境下，以 VxWorks6.9 嵌入式开发板作为载荷计算模块，进行了功能和性能测试。实验结果表明所设计的轻量级身份认证方案能够对无人机的身份进行正确的验证，同时基于 ECC 算法的认证方案与基于 RSA 签名算法的 RSA 数字证书验证方法相比，能够以较短的密钥长度和较小的计算量，实现较高的安全性。

（2）在安全通信研究方面，首先分析了无人机网络通信的安全需求，并基于此和分组密码 SM4 算法的流密码运行模式原理，设计并改进了 CTR 模式的无人机高效会话加解密，并基于所改进的 CTR 模式设计和实现了支持高实时性、容忍密文无序的安全通信方法。同时，使用 HMAC 算法保证传输消息的完整性。

最后，为了说明所设计通信方案的有效性，在实际的多节点无人机网络环境下，以 VxWorks6.9 嵌入式开发板作为载荷计算模块对所实现的轻量级通信方案进行了功能和性能测试。功能测试结果表明该通信方案能够支持设备间安全的通信。性能测试结果表明该方案能够容忍因为环境干扰导致的密文无序、非实时数据丢失导致的密文无法正常解密，加解密速度比传统的 SM4_CTR 算法提升了 7.7%，与 ChaCha20 流加密算法相比更能容忍丢包。

万方数据

5.2 未来工作展望

本文提出的基于 ECC 算法实现的无人机网络轻量级安全认证方案与基于改进的分组加密算法 SM4 流密码运行模式（CTR 模式）的轻量级安全通信方案，对于无人机网络轻量级的身份认证与安全通信方案依然存在许多不足。本方案仍存在需要改进和完善的地方：

1.本文虽然使用了性能较好的 ECC 算法为无人机网络提供了身份认证的功能，但仍然使用数字证书作为合法无人机的身份凭证。因而该认证方案中仍然存在使用数字证书进行认证所存在的问题，即需要传递数字证书并维护证书撤销列表，这将消耗系统一部分的资源与空间。因此，可以进一步考虑使用非证书的认证方案，如可以基于无人机其他物理指纹或其他认证方式实现对于无人机网络中节点身份的认证。

2.从无人机网络轻量级通信方案的性能测试结果来看，所设计的轻量级安全通信方案性能还存着一定的优化空间，具体可以更加优化轻量级加解密的代码，提高算法的性能，构建性能更加优越和健壮的轻量级安全通信方案。

万方数据

参考文献

[1] 沈林成, 牛轶峰, 朱华勇. 多无人机自主协同控制理论与方法[M]. 北京: 国防工业出版社, 2013: 5-9.

[2] Motlagh N H, Bagaa M, Taleb T. UAV-Based IoT Platform: A Crowd Surveillance Use Case[J]. IEEE Communications Magazine, 2017, 55(2):128-134.

[3] Kersnovski T, Gonzalez F, Morton K. A UAV system for autonomous target detection and gas sensing[C]// Aerospace Conference. 2017.

[4] Kumbhar A, Guvenc I, Singh S, et al. Exploiting LTE-Advanced HetNets and FeICIC for UAV-assisted Public Safety Communications[J]. IEEE Access, 2017, PP(99):783-796.

[5] Bupe P, Haddad R, Rios-Gutierrez F. Relief and emergency communication network based on an autonomous decentralized UAV clustering network[C]// Southeastcon. 2015.

[6] Merwaday A, Guvenc I. UAV assisted heterogeneous networks for public safety communications[C]// Wireless Communications & Networking Conference Workshops. 2015.

[7] Sharawi M S, Aloi D N, Rawashdeh O A. Design and Implementation of Embedded Printed Antenna Arrays in Small UAV Wing Structures[J]. IEEE Transactions on Antennas & Propagation, 2010, 58(8):2531-2538.

[8] Maza I, Caballero F, Capitán J, et al. Experimental Results in Multi-UAV Coordination for Disaster Management and Civil Security Applications[J]. Journal of Intelligent & Robotic Systems, 2011, 61(1-4):563-585.

[9] Barrado C, Messeguer R, Lopez J, et al. Wildfire Monitoring Using a Mixed Air-Ground Mobile Network[J]. IEEE Pervasive Computing, 2010, 9(4):24-32.

[10] BENASHER, Yosi, FELDMAN, et al. Distributed Decision and Control for Cooperative UAVs Using Ad Hoc Communication[J]. IEEE Transactions on Control Systems Technology, 2008, 16(3):511-516.

[11] S. Peterson and P. Faramarzi. Iran hijacked US drone, says Iranian engineer .2011.url:http://www. url:http://www.csmonitor.com/World/MiddleEast/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian engineer-Video (Retrieved 02/27/2015).

[12] Rodday, N.: Hacking a professional drone (2016).https://www.Rsaconference.com/events/us16/ /agenda/sessions/2273/hacking-a-professional-drone.

[13] N. Valencia and M. Martinez. Drone carrying drugs crashes south Of U.S. border. 2015. url: http://edition.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border/ (Retrieved03/10/2015).

万方数据

[14] The Guardian. Drone near miss with passenger plane close to Heathrow airport investigated. 2015. url: http://www.theguardian.com/ world/2014/dec/07/drone- near- miss- passenger- plane-heathrow (Retrieved 03/10/2015).

[15] Ding G, Wang J, Wu Q, et al. Robust Spectrum Sensing With Crowd Sensors[J]. Communications IEEE Transactions on, 2014, 62(9):3129-3143.

[16] S. Gorman, Y.J. Dreazen, and A. Cole. Insurgents Hack U.S. Drones.$26 Software Is Used to Breach Key Weapons in Iraq; Iranian Back-ing Suspected. 2009. url: http://www.wsj.com/articles /SB126102247889095011 (Retrieved 02/28/2015).

[17] Arthur, C.: SkyGrabber: the $26 software used by insurgents to hack into US drones (2009). https://www.theguardian.com/https://www.theguardian.com/technology/2009/dec/17/skygrabber -software-drones-hacked.

[18] Cao X, Kou W, Dang L, et al. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks[J]. Computer Communications, 2008, 31(4):659-667.

[19] H. Chan, A. Perrig, and D. Song. Random key redistribution schemes for sensor networks[J]. In IEEE ymposium on Security and Privacy, 2003.

[20] Chatterjee K, De A, Gupta D. An Improved ID-Based Key Management Scheme in Wireless Sensor Network[M]// Advances in Swarm Intelligence. 2012.

[21] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks[J]. In CCS '03. Proceedings, 2003.

[22] Watro R J , Kong D , Cuti S F , et al. TinyPK: securing sensor networks with public key technology[C]// Acm Workshop on Security of Ad Hoc & Sensor Networks. ACM, 2004.

[23] Wong K H M , Zheng Y , Cao J , et al. A Dynamic User Authentication Scheme for Wireless Sensor Networks[C]// IEEE International Conference on Sensor Networks. IEEE, 2006.

[24] Das, Lal M . Two-factor user authentication in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2009, 8(3):1086-1090.

[25] Tseng, H.R.; Jan, R.H.; Yang, W. An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks[J]. In Proceedings of IEEE Globecom, Washington, DC, USA, 26–30 November 2007; pp. 986-990.

[26] Khan M K , Alghathbar K . Security Analysis of "Two－Factor User Authentication in Wireless Sensor Networks"[C]// International Conference on Advances in Computer Science & Information Technology. Springer-Verlag, 2010.

[27] Khan M K , Alghathbar K . Cryptanalysis and Security Improvements of "Two-Factor User Authentication in Wireless Sensor Networks"[J]. Sensors, 2010, 10(3):2450-2459.

[28] Chen T H , Shih W K . A Robust Mutual Authentication Protocol for Wireless Sensor Networks[J].

万方数据

ETRI Journal,32,5(2010-10-06), 2010, 32(5):704-712.

[29] Yeh HL, Chen TH, Liu PC, Kim TH, Wei HW. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. Sensors 2011(11):4767–79.

[30] Xu J , Zhu W T , Feng D G . An improved smart card based password authentication scheme with provable security[J]. Computer Standards & Interfaces, 2009, 31(4):723-728.

[31] Song R . Advanced smart card based password authentication protocol[J]. Computer Standards & Interfaces, 2010, 32(5-6):321-325.

[32] Gupta L , Jain R , Vaszkun G . Survey of Important Issues in UAV Communication Networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(2):1123-1152.

[33] Li X , Zhang Y D . Multi-source cooperative communications using multiple small relay UAVs[C]// IEEE Globecom Workshops. 2010.

[34] A. Vassilev, "Annex A: Approved Security Functions for FIPS PUB140-2,security Requirements for Cryptographic Modules,"[J] National Institute of Standards and Technology, Gaithersburg, Maryland,2016.

[35] H. O. Alanazi, et al., "New Comparative Study between DES, 3DES and AES within Nine Factors,"[J] Journal of Computing, vol. 2, no. 3, pp. 152-157, 2010.

[36] N. Sullivan. (2015, Feb. 23). Do the ChaCha: better mobile performance with cryptography [Online]. Available: https:// blog.cloudflare.com/do-the-chacha-better-mobile-performance-with-cryptography/.

[37] E. Bursztein. (2014, Apr. 24). Speeding up and strengthening HTTPS connections for Chrome on Android [Online]. Available:https://security.googleblog.com/2014/04/speeding-up-and-strengthening-https.html.

[38] Bernstein D J . The Salsa20 Family of Stream Ciphers[M]// New Stream Cipher Designs. Springer-Verlag, 1970.

[39] Diffie, W., Hellman, M.: New directions in cryptography[J]. IEEE Transactions on Information Theory IT-22 (1976) 472-492.

[40] Rivest R L , Shamir A , Adleman L . A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the Acm, 1978, 21(2):120-126.

[41] Rabin M O . Digitalied Signatures and Public Key Functions as Intractable as Factorization[M]. Massachusetts Institute of Technology, 1979.

[42] El-Gamal T . A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans. Inf. Theory, 1985, 31(4):469-472.

[43] Schnorr C P . Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3):161-174.

万方数据

[44] National Institute of Standards and Technology (1994) Digital signature standard. FIPS Publication 186, available from http://csrc.nist.gov/encryption/.

[45] Nyberg K . A new signature scheme based on the DSA giving message recovery[C]// 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, Nov. 1993. ACM, 1993.

[46] Nyberg K, Rueppel R Message recovery for signature schemes based on the discrete logarithm problem[C]. Des Codes Cryptography 1996 7:61–81.

[47] 陈月波，解勤华，潘明风，电子商务实务[M]，电子工业出版社，2007.

[48] 文卉，胡剑波，信息安全技术简述[M]，计算机与数字工程，2008 年第 8 期.

[49] (美)威廉·D.江恩(William D.Gann)，江恩华尔街选股方略解读版[M]，人民邮电出版社，2018.

[50] Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information[J] Theory IT-22 (1976) 472-492.

[51] Patterson W . Mathematical cryptology for computer scientists and mathematicians[M]// Mathematical cryptology for computer scientists and mathematicians /. Rowman & Littlefield, 1987.

[52] Thompson R B . Confidential and Authenticated Communications in a Large Fixed-Wing UAV Swarm[C]// IEEE International Symposium on Network Computing & Applications. IEEE, 2016.

万方数据

致谢

时光如白驹过隙般，就这样悄无声息地过去了。三年的研究生时光和属于我的学生时代，也就这样缓缓地向我挥手告别了。在或短或长的三年时间里，在老师、同学和朋友们的帮助下，一次次地克服了生活和学习中的种种困难，也让自己有勇气和信心去面对之后的社会生活。

首先要由衷地感谢我的研究生导师马建峰老师。刚刚加入马老师团队那一天的场景还历历在目，马老师严谨的治学态度、在学术上深刻的见解以及对我们的谆谆教诲都给我留下了深刻的印象。在此后的生活学习中，马老师也以言传身教的方式不断地鞭策着我们、带领着我们。因此，我感谢我的导师马建峰老师。

同时感谢我们无人机项目组的孙聪老师、习宁老师和卢笛老师。感谢他们在科研过程中对我的指导与督促，对我学术学习上的帮助。特别感谢孙聪老师经常夜以继日的对我的报告和论文进行修改，并且以他严谨务实、耐心细心的态度深深地影响着我，让我的报告书写能力和科研能力都有了很大的提升。

感谢我们气氛活跃并且温馨的 1002 实验室，能够让我在这样放松的环境中成长学习。感谢孙召昌、吴奇烜、帕尔哈提江·斯迪克、冯鹏斌、李腾等师兄，在日常的科研和生活中对于我的帮助。感谢魏大卫、赵昊罡、张兆一、马承彦、田创等 16 级的伙伴们，对于我平常的鼓励和帮助。感谢师弟师妹们对我的支持。感谢实验室的每一个人，与你们的每一次交流都让我感觉到由衷的开心并且受益匪浅，谢谢你们。

此外，还要感谢我们 127 的室友们，对于我生活上的照顾与鼓励，感谢你们。

最后，要感谢爱我的家人们，在背后默默地支持我，在我成长的道路上所给于我关怀和鼓励，能够让我专心学业。

谢谢你们。

万方数据

万方数据

作者简介

1. 基本情况

孟悦，女，陕西渭南人，1993 年 11 月出生，西安电子科技大学计算机科学与技术学院计算机技术专业 2016 级硕士研究生。

2. 教育背景

2012.09～2016.07 西北工业大学计算机学院，本科，专业：计算机科学与技术
2016.09～2019.07 西安电子科技大学计算机科学与技术学院，硕士研究生，专业：计算机技术

3. 攻读硕士学位期间的研究成果

3.1 申请（授权）专利

[1] 马建峰;孟悦;孙聪.等. 无人机网络轻量级安全认证系统:中国,发明专利，201610708035.X. 2016.08.23.

3.2 参与科研项目及获奖

[1] 国防项目，《***机制研究》，2017.10~至今，负责装备嵌入式计算机中设备间远程安全接入控制与安全通信机制的研究，并将代码部署在 VxWorks 系统中。
[2] 国防项目，《无人机安全组网》，参与时间 2016.9~2017.12，已完成。负责无人机之间安全认证方案的设计与实现。
[3] 国防项目，《XXX 操作系统 PCS 和 Guard 信息安全中间件技术》，2017.8~至今，负责多级安全关键系统中的多个不同安全级别的分区间认证和通信机制的研究，同时根据安全策略，实现了 Guard 模块的降级功能。

万方数据

万方数据