一种面向分布式卫星网络的安全可靠通信方案

顾 俊[1],赵泓光[1],胡玉军[2],杨 旭[3],齐赛宇[1*],齐 勇[1]
(1. 西安交通大学,陕西 西安 710049;
2. 联勤保障部队第 903 医院信息科,浙江 杭州 310013;
3. 西北工业大学 电子信息学院,陕西 西安 710072)

摘 要:卫星网络在现代通信和导航中具有至关重要的作用。然而,传统的中心化卫星网络易受到单点故障的影响,降低系统的可用性和可拓展性。为此,该文提出了一种面向分布式卫星网络的安全、可靠卫星数据通信方案。为了实现高效的权限管理,首先引入 WKD-IBE 技术,设计了支持细粒度的分布式密钥生成、分发与权限撤销的密钥管理机制。相较于以往由中心化的服务器管理密钥,该密钥管理机制支持任何合法订阅者在其租期内为其他订阅者授予对资源的访问权限。在此基础上,基于密钥复用思想,设计了一种安全、轻量的两步广播加密算法,在保证数据私密性的前提下降低了卫星节点的计算开销。为了提升系统的可用性,降低节点失效对系统的影响,该文基于拜占庭容错共识协议,设计了一种故障检测与恢复机制。实验结果表明,设计的方案在低带宽分布式卫星网络场景下,具有较低的计算开销与通信开销。

关键词:卫星网络;分布式授权;广播加密;密钥复用;安全信道;故障恢复
中图分类号:TP302 **文献标识码**:A **文章编号**:1673-629X(2025)05-0054-06
doi:10.20165/j.cnki.ISSN1673-629X.2024.0398

A Reliable and Secure Data Communication Scheme for Distributed Satellite Network

GU Jun[1],ZHAO Hong-guang[1],HU Yu-jun[2],YANG Xu[3],QI Sai-yu[1*],QI Yong[1]
(1. Xi'an Jiaotong University,Xi'an 710049,China;
2. Information Department,903 Hospital of the People's Liberation Army Joint Logistics Support Force,Hangzhou 310013,China;
3. School of Electronics and Information,Northwestern Polytechnical University,Xi'an 710072,China)

Abstract: Satellite networks play a crucial role in modern communication and navigation. However, traditional centralized satellite networks are vulnerable to single points of failure, which can reduce system availability and scalability. We propose a secure and reliable data communication scheme for distributed satellite network scenarios. To achieve efficient access management, we introduce the WKD-IBE technology and design a key management mechanism that supports fine-grained distributed key generation, distribution, and revocation. Compared to the traditional approach where keys are managed by centralized servers, the proposed key management mechanism allows any legitimate subscriber to grant access to resources to other subscribers during their subscription period. Building on this, a secure and lightweight two-step broadcast encryption algorithm is designed, which reduces node computational overhead while ensuring data privacy through key reuse. To enhance system availability and minimize the impact of node failures, a fault detection and recovery mechanism based on Byzantine fault tolerance consensus protocol is designed. Experimental results show that the proposed scheme exhibits lower computational and communication overhead in low-bandwidth distributed satellite network scenarios.

Key words: satellite networks; distributed authorization; broadcast encryption; key reuse; secure channel; fault recovery

0 引 言

在现代通信和导航系统中,卫星网络发挥着至关重要的作用。然而,传统的卫星网络架构往往依赖于中心节点,这使得系统容易受到单点故障的影响。因

收稿日期:2024-08-19 **修回日期**:2024-12-19
基金项目:空间微波通信全国重点实验室稳定支持基金资助项目(HTKJ2023KL504006);国家自然科学基金面上项目(62172328)
作者简介:顾 俊(1986-),男,博士,研究方向为数据安全、医疗数据共享、医疗人工智能等;通信作者:齐赛宇(1986-),男,副教授,博士,研究方向为区块链数据库数据隐私安全保护、不可信外包服务场景下数据存储及查询安全、开放网络环境下数据确权及交易安全等;齐 勇(1957-),男,教授,博士,CCF 会士(05211F),研究方向为操作系统、分布式系统、云计算虚拟化技术以及系统安全与应用等。

此,建立分布式的卫星网络架构具有重要的意义[1-2]。

然而,建立分布式的卫星网络架构面临多方面的挑战。首先,卫星之间的数据传输需要经过无线信道,易受到窃听和篡改攻击[3-4]。同时,点对点网络中,传统的广播加密技术难以支持访问控制,使用集中式授权可能造成隐私泄露。刘潇等[5]通过在广播身份集合中增加虚拟用户实现了选择密文安全,然而,该工作无法支持分布式授权。这样的问题广泛存在于广播加密的相关研究中[6-8]。此外,由于太空中的低温与强电磁辐射环境,卫星可能发生故障,从网络中离线,导致网络的功能出现异常。

2019 年,Kumar 等提出了一种物联网系统中的安全广播加密机制 Joint Encryption and Delegation for IoT (JEDI)[9],通过 IBE 技术实现分布式授权。尽管 JDEI 被设计用于多层物联网场景,而非对等网络,其设计思路仍然值得思考与借鉴。

针对以上问题,该文提出了一种卫星间安全、可靠的数据通信方案。首先,基于 WKD-IBE 技术设计了支持细粒度的分布式密钥生成、分发与权限撤销的密钥管理机制。在此基础上,设计了一种安全、轻量且可复用密钥的广播加密机制,保护数据的私密性与完整性。为了应对卫星网络中可能发生的节点失效问题,基于拜占庭容错共识协议设计了一种故障检测与恢复机制,增强了系统的容灾容错能力。该文的贡献总结如下:

- 利用 WKD-IBE 技术的密钥推导特性,设计了一套支持密钥生成、分发与撤销的密钥管理机制,允许节点构建分布式的授权链,且可以指定任意粒度的租期。
- 设计了一种安全、轻量的两步广播加密算法,在保证访问控制的前提下,降低节点因加密/解密导致的计算开销。
- 基于拜占庭容错共识协议,设计了一种故障检测与恢复机制,提高系统的可用性。
- 设计并开展仿真实验,结果证明,该方案在低带宽卫星网络场景下具有良好的表现。

1　相关概念

1.1　WKD-IBE 加密技术

首先定义模式(pattern),模式是一个包含若干值的列表,即 $P=(\mathbb{Z}_p^* \cup \{*\})^{\ell}$,其中符号 $*$ 为通配符。记 $P(i)$ 为模式的第 i 个元素。定义模式 P_1 匹配模式 P_2,当且仅当 $\forall i \in [1,\ell]$ 都有 $P_1(i)=*$ 或 $P_1(i)=P_2(i)$。例如,假设 $P_1=ab*$,$P_2=abc$,则称模式 P_1 匹配模式 P_2。

WKD-IBE[10]是一种广泛应用的基于身份加密技术,可以高效地解决多层的基于身份加密问题(HIBE)。WKD-IBE 技术基于模式,根据模式对消息进行加密,每个模式对应一个解密密钥。同时,WKD-IBE 拥有密钥推导性质,假设一个模式 P 对应的解密密钥为 k,对于任意匹配 P 的模式 P',可以根据 k 与 P' 推导出模式 P' 对应的解密密钥 k'。下面给出 WKD-IBE 的具体定义:

- Setup()→params, msk:初始化得到一组参数 params 和主密钥 msk。
- Keyderive(params, k_p, P')→$k_{p'}$:当模式 P 匹配 P' 时,根据模式 P 对应的密钥 k_p 推导出模式 P' 对应的密钥 $k_{p'}$。
- Encrypt(params, pattern, msg)→ct:根据模式 pattern 加密消息 msg,得到密文 ct。
- Decrypt(k,ct)→msg:使用模式对应的密钥 k 解密。

1.2　分布式共识协议

分布式共识协议是一类用于在分布式系统中达成一致决策的协议。根据容错机制,分布式共识协议可以分为两类:崩溃容错协议(Crash Fault Tolerance, CFT)和拜占庭容错协议(Byzantine Fault Tolerance, BFT)。崩溃容错协议(如 Paxos[11],Raft[12]等)用于应对崩溃故障,即节点可能会突然宕机,但不会表现出恶意行为。拜占庭容错协议(如 PBFT[13], Tendermint[14])用于应对拜占庭故障,即节点可能表现出任意恶意行为。

2　整体框架

2.1　系统模型

文中方案的系统模型如图 1 所示。卫星网络是一个点对点网络,每个卫星节点能够独立运行和通信,不依赖于中心节点。通信模式方面,采用发布-订阅模式,节点可以发布消息,也可以获取授权并订阅其他节点的消息,即节点可以同时拥有发布者与订阅者两种身份。例如,图 1 中节点 A 在获取节点 B 的授权后,可以订阅得到节点 B 发送的消息。消息投递由底层路由协议处理,不在该文讨论范围之内。

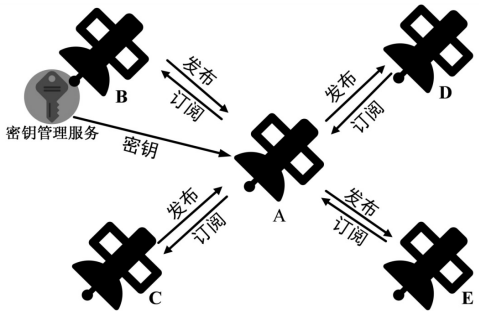

图 1　系统模型(卫星 B 运行密钥管理服务)

为了实现安全的广播加密,方案使用分布式的密钥管理服务,支持密钥的生成、分发、轮换和撤销以及授权链。卫星网络中的消息以密文形式传输,在租期内,订阅者可以使用发布者授权的密钥对密文解密,得到消息明文。例如,图 1 中节点 B 授权节点 A 以解密密钥,节点 A 在租期内可以解密节点 B 发布的消息。

2.2 威胁模型

该文假设卫星网络中所有节点都是有恶意的,其潜在的恶意行为陈述如下:

- 恶意节点监听信道中传输的数据,尝试获取消息明文的信息,破坏数据私密性。
- 恶意节点篡改并伪造网络中的传输数据,破坏数据完整性。
- 恶意节点攻击分布式密钥管理服务,尝试在没有某节点授权的情况下伪造解密密钥,从而获取访问权限外的数据。

此外,该文假设恶意节点之间不存在共谋,即节点间不会交换拥有的密钥。

3 卫星间安全可靠的数据通信方案

该文介绍一种卫星间安全、可靠的数据通信方案,通过设计基于 WKD-IBE 技术的密钥管理机制,此方案可以支持细粒度的密钥生成、分发与权限撤销,避免密钥滥用。在此基础上,又设计了一种安全、轻量且可复用密钥的广播加密机制,保护数据的私密性与完整性。由于卫星网络中节点可能发生拜占庭错误,又设计了一种基于拜占庭容错共识协议的检测机制,可以快速检测故障并恢复,保证了系统的高可用性与容灾容错能力。

3.1 密钥分发机制

首先设计支持细粒度密钥分发与权限撤销的密钥管理机制。考虑图 1 中的例子,节点 B 作为发布者,需要控制订阅者的访问权限,即哪些节点可以订阅消息,以及各节点订阅的时长(租期)。具体的访问控制规则体现在三个方面:

- 对于未获取授权的节点,即使它通过广播得到了发布者发送的消息密文,仍然无法解密。
- 对于获取授权的节点,它拥有发布者授予的解密密钥和一个租期,解密密钥当且仅当在租期内有效。
- 租期内,获得授权的节点可以授权其他节点获取发布者的消息,对应的租期应当被包含在发布者提供的租期之内。

例如,图 2 中节点 B 为发布者,节点 A 向其申请订阅权限。节点 B 首先指定租期 2024/1/1/00-2024/2/2/00(格式为“年/月/日/时”)并生成解密密钥 k,将其发送至节点 A。之后,节点 A 可以为节点 C 制定租期 2024/1/10/00 - 2024/1/20/00(节点 C 的租期应当小于等于节点 B 的租期),并生成解密密钥 k'。最终,节点 C 可以在租期 2024/1/10/00 - 2024/1/20/00 内对节点 B 发布的消息进行解密。因此,如图 2 所示,节点可以分布式地构造一条授权链。

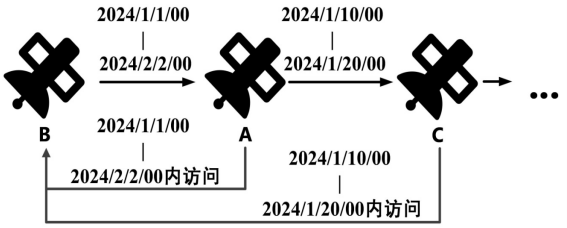

图 2 分布式授权

(通过分布式授权机制,系统构造了 B→A→C 的授权链)

设计满足上述访问控制规则的密钥管理机制是富有挑战性的,传统的对称加密算法(如 AES,DES 等)难以满足这样的要求。已有的方案[15-17]往往使用基于属性的加密技术(ABE)解决该问题,然而,ABE 基于昂贵的双线性对操作,其计算开销对于卫星节点是不可接受的。

WKD-IBE 的密钥推导基于模式。假设用户 A 具有模式 $P_A = ab*$,密钥为 k_{P_A}。若根据 P_A 加密消息 msg 得到密文 ct,则用户 A 可以使用 k_{P_A} 正确地解密 ct。用户 B 具有模式 $P_B = abc$,则用户 A 的模式 P_A 匹配用户 B 的模式 P_B,用户 A 可以根据 P_A 与 k_{P_A} 推导得到密钥 k_{P_B}。若根据 P_B 加密消息得到密文,则用户 B 可以根据此前推导得到的密钥 k_{P_B} 正确地解密。可见,WKD-IBE 密钥推导的过程与授权通过链传递的过程相似。因此,该文选择使用 WKD-IBE 作为基础密码学组件,利用其密钥推导特性支持授权链结构。

首先设计 WKD-IBE 模式的结构。发布者向订阅者授权时,首先要设置租期,然后根据租期生成解密密钥,因此模式中需要包含加密时的时间信息。此外,为了保证不同发布者加密消息时的模式是不同的,模式中也需要包含发布者的标识符 id。假设卫星网络中每个节点拥有公开且固定的标识符 id,时间戳格式为“年/月/日/时”,那么模式包含两部分:(1)发布者的标识符 id,长度为 $\ell_1 = 1$。(2)发布消息时刻的时间戳 ts,长度为 $\ell_2 = 4$。在图 2 的示例中,假设节点 B 在时刻 2024/1/1/02 发布消息,则对应的模式为 < B,2024,1,02 > 。

在此基础上,授权等价于授予一组密钥的集合。发布者首先设置订阅者的租期,然后计算租期对应的密钥集合。考虑一种直接的做法,发布者 B 设置某订阅者 A 的租期为 2024/1/1/00 - 2024/2/2/00,并枚举租期内每个可能的时间戳,即 TS = {2024/1/1/00,2024/1/1/01,…,2024/2/1/23,2024/2/2/00},然后根

据这些时间戳构造若干模式,最后为每个模式推导出一个密钥,得到的密钥集合与 TS 大小相同。然而,当租期较长时, TS 中有大量的时间戳,导致订阅者需要在本地储存庞大的密钥集合,其存储开销对卫星节点来说是不可接受的。

为了尽可能减少密钥数量,这个集合需要恰好覆盖租期,且是最小的,即最佳范围覆盖[18](BRC)。如图 3 所示,之前的例子中对应于租期的 BRC 集合为 S = {2024/1/ * ,2024/2/1/ * ,2024/2/2/00}。然后,发布者 B 根据 S 构造对应的模式为 P = { < B,2024,1, * ,* > , < B,2024,2,1, * > , < B,2024,2,2,00 > },并根据这 3 个模式推导得到 3 个密钥,作为授予订阅者 A 的解密密钥。可见,通过使用 BRC,本方案有效地降低了密钥存储开销。需要注意的是,当订阅者向其他节点授权时,需要的操作与上述发布者向订阅者授权的流程相同。

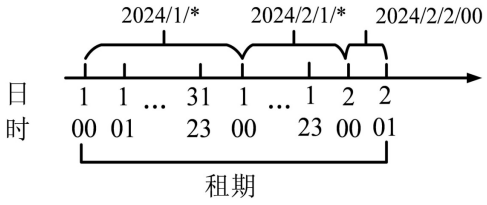

图 3　订阅者 A 的租期

(通过使用 BRC,租期被分为 3 个区间)

当订阅者的租期结束时,可以向发布者申请新的租期。发布者可以选择拒绝续租,从而实现订阅者的权限撤销,订阅者无法使用旧的 WKD-IBE 密钥解密新时间段的密文。实际使用中,用户可以通过调整时间戳的粒度来灵活地控制权限撤销的及时性,例如将时间戳的最小粒度调整为 10 分钟,从而更及时地撤销订阅者的权限。

在实际使用中,需要将模式中的每个元素映射到 $\mathbb{Z}_p^*$ 中,该文不再赘述。

3.2　安全的广播加密机制

在上述密钥分发机制的基础上,设计一种安全的广播加密机制,保证只有拥有权限的节点可以对发布者广播的消息进行解密。一种直接的思路是,发布者使用 WKD-IBE 的 Encrypt 功能将消息加密得到密文,并在网络中广播;拥有解密密钥的订阅者使用 WKD-IBE 的 Decrypt 功能对密文解密。这种方案易于实现,然而,WKD-IBE 的计算较为复杂,频繁使用 WKD-IBE 进行加密与解密将给卫星节点带来沉重的计算负载。

针对 WKD-IBE 计算复杂度大的问题,该文设计了一种简单、高效的两步加密算法。基于密钥复用的思想,每当时间的最小粒度更新时(默认时间的最小粒度为小时),发布者随机生成一个字符串 k_s 作为对称加密算法的密钥,缓存在本地。消息 msg 发布前,发布者对其进行两步加密:(1)使用 WKD-IBE 技术对 k_s 加密,得到密文 ct_1。(2)将 k_s 作为对称加密算法的密钥,对消息 msg 加密得到密文 ct_2。最终,发布者将 ct_1、ct_2 打包并广播。

当订阅者接收到广播的数据包后,它首先根据当前的时间戳构造模式,并使用本地储存的 WKD-IBE 解密密钥与该模式推导出对应于 ct_1 的解密密钥。然后进行两步解密:首先使用上述生成的解密密钥对 ct_1 解密,得到 k_s ;然后使用 k_s 解密 ct_2,得到消息 msg 。这样的设计保证了数据的私密性,只有拥有正确的解密密钥的订阅者才可以对数据解密。若恶意节点未被授予解密密钥,或解密密钥超过租期,都无法对 ct_1 解密。

上述方案仍存在优化空间。订阅者每次接收到广播的数据包,都需要进行一次 WKD-IBE 解密,这给订阅者带来了较大的计算开销。当时间的最小粒度为小时时,一个小时内 k_s 是不变的,因此 ct_1 也保持不变。订阅者可以在当前时段的第一次解密时,将 ct_1 与 k_s 缓存在本地。同一时段后续接收到新的数据包时,将本地缓存的 ct_1 与数据包的相应字段对比,若相同,则可直接使用本地缓存的 k_s 作为对称加密的密钥。这样的优化可以有效减轻订阅者的计算负载。

然而,当前方案缺少对数据完整性的保护。如图 4 所示,假如某个恶意节点 C 获取了发布者 B 的授权,它可以解密得到当前时间段的对称加密密钥 k_s 。由于一个时间段内 k_s 是固定的,恶意节点可以拦截发布者的广播消息,然后伪造消息 msg′ ,使用 k_s 对其加密得到 ct_2',最终恶意节点将 ct_1、ct_2' 打包并广播,其他订阅者解密得到恶意节点伪造的消息 msg′ 。因此,发布者需要在广播的数据中附上数据的数字签名。接收者首先使用发布者的公钥验证签名,验证通过后方可执行两步解密。

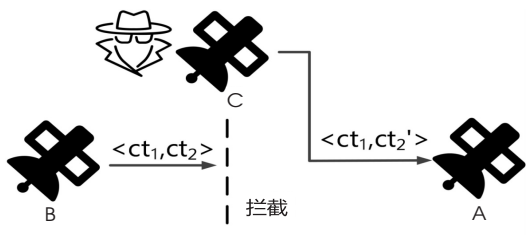

图 4　恶意用户拦截并伪造广播数据示意图

3.3　基于拜占庭容错共识协议的故障检测与恢复机制

WKD-IBE 技术需要预先设置一些参数,因此,需要卫星节点选举出一个节点作为密钥初始化服务器,记为 KIS(Key Initiate Server)。KIS 负责生成主密钥

msk 与参数 params,并为每个发布者生成密钥。在图 2 的例子中,发布者 B 向 KIS 申请密钥,KIS 设置模式为 < B, * , * , * , * > ,表明租期是无限的,即节点 B 的身份为发布者。然后,KIS 根据此模式与主密钥 msk 为节点 B 生成相应的密钥。

在太空环境下,卫星可能因电磁辐射等发生宕机从而离线;此外,网络中可能存在恶意节点。因此,该文设计了一种高效的故障检测与恢复机制。首先,每个发布者持续监控 KIS 的状态,KIS 定期向发布者发送心跳消息,证明其正在正常工作。如果某个发布者在一段时间内未收到 KIS 的心跳消息,它将认为特殊节点可能已故障,并尝试联合其他发布者发起选举。选举阶段,所有发布者使用拜占庭容错共识协议(如 PBFT,Tendermint 等)选举得到新的 KIS。选举结束后,所有发布者需要向新的 KIS 申请新的 WKD-IBE 密钥。

4 实验与分析

本节将评估方案各阶段在计算和通信方面的开销。基于 BLS12-381 椭圆曲线与 C++语言实现了两步加密与解密模块。测试环境为 Ubuntu 18.04 服务器,Intel(R) Core(TM) i7-1070 处理器,64 GB 内存。

4.1 计算复杂度

定义双线性映射 $\mathbb{G}^* \times \mathbb{G}^* \rightarrow \mathbb{G}_T$,模式长度为 L ,节点在授权链中的层级为 ℓ 。首先将系统流程分为以下三个部分:密钥推导;发布者端两步加密;订阅者端两步解密。

密钥推导:设某模式 P 的层级为 l ,为了生成匹配 P 的模式 P' 对应的密钥,首先需要执行 L 次幂运算,然后在 $\mathbb{G}^*$ 上执行 $W + L - \ell$ 次乘法运算,其中 W 为模式 P' 在层级 ℓ 以下的非通配符元素个数。

假设发布者的模式为 < B, * , * , * , * > ,层级为 5。若发布者为订阅者授予 2024 年的访问权限,则目标模式为 < B,2024, * , * , * > ,目标模式在层级 5 下的非通配元素为 1,即“2024”。如图 5 所示,当前层级下非通配符元素个数增加时,密钥推导的时间开销随之线性增长,即密钥推导时间与授权的粒度成正比。

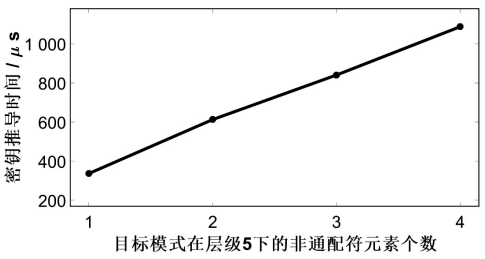

图 5 密钥推导性能

两步加密:对每个时段,当发布者第一次加密消息时,需要使用 WKD-IBE 加密密钥 k_s 。具体地,发布者首先需要执行 L 次幂运算,然后执行一次双线性映射操作和一次 $\mathbb{G}_T$ 上的乘法操作。之后,发布者使用对称加密算法加密消息,时间开销与消息长度呈线性。

两步解密:对每个时段,当订阅者第一次收到某发布者的消息时,需要使用 WKD-IBE 解密,得到当前时段的密钥 k_s 。具体地,订阅者需要首先执行 L 次双线性映射操作,然后执行一次 $\mathbb{G}_T$ 上的乘法操作。之后,订阅者使用对称加密算法解密消息,时间开销与消息长度呈线性。

显然,使用 WKD-IBE 技术加密密钥 k_s 时,所需的时间仅与模式长度 L 有关。如图 6 所示,当使用不同对称加密算法(AES128,AES192 等)时,密钥 k_s 的长度不同,但 WKD-IBE 加密与解密时间基本保持不变。因此,该方案拥有良好的可拓展性,支持任意长度的对称加密密钥,且不影响加密性能。此外,由于 WKD-IBE 的解密操作基于大量双线性映射操作,WKD-IBE 的解密速度略低于加密速度。但是得益于密钥复用机制,每个时段订阅者只需执行一次 WKD-IBE 解密操作,因此其带来的计算开销可忽略不计。

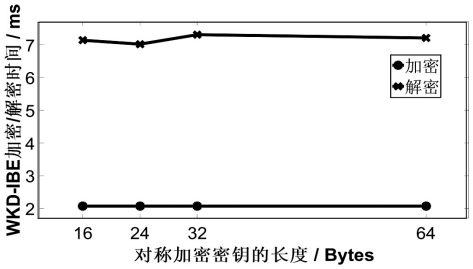

图 6 WKD-IBE 加密/解密时间

4.2 通信复杂度

发布者广播的加密消息包括两部分 ct_1、ct_2。其中, ct_1 由 $L + 1$ 个大整数组成。该文在实验中设定模式长度为 $L = 5$,使用 32 字节编码整数,则 ct_1 为 192 字节。ct_2 的长度与消息的长度相等(不考虑填充)。因此,额外的通信开销只有 192 字节,不会给低带宽卫星网络带来显著的通信负担。

5 结束语

该文提出了一种卫星网络中安全、可靠的数据通信方案。通过引入 WKD-IBE 技术,该方案以构建授权链的形式,实现高效的分布式密钥推导与分发,并灵活地设置授权粒度。相较于以往由中心化的服务器管理密钥,该文的密钥管理机制支持任何合法订阅者在其租期内为其他订阅者授予对资源的访问权限。在此基础上,基于密钥复用思想设计了一种高效的两步广播加密机制,有效地降低了 WKD-IBE 技术在加/解密

过程中导致的计算开销。此外,为了提升系统的容灾容错能力,该方案包含基于拜占庭容错共识协议的故障检测与恢复机制。最终,通过实验验证了该方案在低带宽卫星网络场景下具有良好的性能。

参考文献:

[1] 刘晔伟,周庆瑞,黄　昊. 分布式卫星系统动态任务协同规划算法研究[J]. 空间控制技术与应用,2022,48(4):46-53.

[2] 王丽冲. 分布式卫星组网系统关键技术研究[D]. 北京:中国科学院国家空间科学中心,2016.

[3] 吴流丽,廖建华,苏怀方. 卫星通信系统安全风险分析及防御对策初探[J]. 航天电子对抗,2021,37(5):49-52.

[4] 韩　帅,李季蹊,李静涛. 卫星地面融合网络的窃听威胁与物理层安全解决方案[J]. 中兴通讯技术,2021,27(5):43-47.

[5] 刘　潇,刘巍然,伍前红,等. 选择密文安全的基于身份的广播加密方案[J]. 密码学报,2015,2(1):66-76.

[6] 王戌琦,程相国,王　越. 一种新的基于 RSA 广播加密方案[J]. 网络空间安全,2019,10(2):80-85.

[7] 赖建昌,黄欣沂,何德彪. 一种基于商密 SM9 的高效标识广播加密方案[J]. 计算机学报,2021,44(5):897-907.

[8] 崔　岩,黄欣沂,赖建昌,等. 基于 SM9 的匿名广播加密方案[J]. 信息安全学报,2023,8(6):15-27.

[9] KUMAR S,HU Y,ANDERSEN M P,et al. JEDI:many-to-many end-to-end encryption and key delegation for IoT[C]//28th USENIX security symposium. Santa Clara:USENIX Association,2019:1519-1536.

[10] ABDALLA M,KILTZ E,NEVEN G. Generalized key delegation for hierarchical identity-based encryption[C]//Computer security - ESORICS 2007:12th European symposium on research in computer security. Dresden:Springer,2007:139-154.

[11] LAMPORT L. The part-time parliament[M]//Concurrency:the Works of Leslie Lamport. [s. l.]:[s. n.],2019:277-317.

[12] ONGARO D,OUSTERHOUT J. In search of an understandable consensus algorithm[C]//2014 USENIX annual technical conference. Philadelphia:USENIX,2014:305-319.

[13] CASTRO M,LISKOV B. Practical byzantine fault tolerance[C]//1999 USENIX symposium on operating systems design and implementation. New Orleans:USENIX,1999:173-186.

[14] BUCHMAN E,KWON J,MILOSEVIC Z. The latest gossip on BFT consensus[J]. arXiv:1807.04938,2018.

[15] WANG F,MICKENS J,ZELDOVICH N,et al. Sieve:cryptographically enforced access control for user data in untrusted clouds[C]//13th USENIX symposium on networked systems design and implementation. Santa Clara:USENIX,2016:611-626.

[16] WANG G,LIU Q,WU J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services[C]//Proceedings of the 17th ACM conference on computer and communications security. Chicago Illinois:ACM,2010:735-737.

[17] WANG G,LIU Q,WU J,et al. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. Computers & Security,2011,30(5):320-331.

[18] AKHAVAN MAHDAVI R,NI H,LINKOV D,et al. Level up:private non-interactive decision tree evaluation using levelled homomorphic encryption[C]//Proceedings of the 2023 ACM SIGSAC conference on computer and communications security. Copenhagen:ACM,2023:2945-2958.