

基于区块链的天地一体化信息网络非交互式密钥交换方法

刘梦如, 付玉龙, 曹 进, 李 晖

(西安电子科技大学网络与信息安全学院, 陕西 西安 710126)

摘 要: 面向天地一体化信息网络等卫星资源受限和通信时延较大的场景, 针对卫星通信网络中非交互式密钥交换的需求, 提出一个适用于天地一体化信息网络的、基于区块链和Diffie-Hellman密钥交换协议的非交互式密钥交换方案。该方案将区块链部署在天地一体化信息网络中, 组成TDYTH区块链。卫星节点完成注册后, 其相关信息保存在TDYTH区块链中。当卫星节点需要与地面网络控制中心等远距离节点完成卫星组网时, 双方可在非交互的条件下查询TDYTH区块链中不可篡改的信息来生成会话密钥、建立共识, 进而完成接入认证和密钥分发。仿真结果表明提出的方案可满足卫星等节点的非交互式密钥分发需求, 且在安全性、稳健性等方面提升显著。

关键词: 天地一体化信息网络; 非交互式密钥交换; 区块链

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2021030

A Non-interactive Key Exchange Scheme for Space-Integrated-Ground Information Network Based on Blockchain

LIU Mengru, FU Yulong, CAO Jin, LI Hui

School of Cyber Engineering, Xidian University, Xi'an 710126, China

Abstract: For scenarios such as space-integrated-ground information network where satellite resources are limited and communication delays are large, in response to the requirements of non-interactive key exchange in the satellite communication network, a non-interactive key exchange scheme for space-integrated-ground information network based on blockchain and Diffie-Hellman key exchange protocol was proposed. The scheme arranged the blockchain in space-integrated-ground information network to form TDYTH blockchain. After the satellite node was registered, its related information was stored in TDYTH blockchain. When the satellite node needed to communicate with the long-distance node such as NCC, the two parties could query the immutable information stored in TDYTH blockchain to generate the shared session key, established consensus, and then completed access authentication and key distribution under non-interactive conditions. The result of simulation demonstrated that the scheme we proposed could meet the requirements of non-interactive key distribution of satellites and other nodes, and could significantly improve security and robustness.

Keywords: space-integrated-ground information network, non-interactive key exchange, blockchain

1 引言

随着社会的进步和科学技术的飞速发展, 为了满足各种创造性需求, 全球信息化发展领域已经覆盖到海洋、

陆地、空中和太空等各个维度空间。原本相互独立的异构网络需要跨地域、跨空域进行信息共享、协同工作, 实现互通有无。这些需求推动了天地一体化信息网络的形

收稿日期: 2021-04-30; **修回日期:** 2021-08-10

基金项目: 陕西省自然科学基金基础研究计划资助项目(项目编号2021JM-137); 中央高校基本科研业务费(No. QTZX2106); 国家自然科学基金面上项目(No. 61772404); 陕西省重点产业创新链(群)-工业领域项目(No. 2020ZDLGY08-08); 国家自然科学基金重点类项目(No. U1836203)

Foundation Items: Natural Science Basic Research Program of Shaanxi (Program No. 2021JM-137), The Fundamental Research Funds for the Central Universities under grant QTZX2106, The National Natural Science Foundation of China under Grants 61772404, Key Research and Development Program of Shaanxi (No. 2020ZDLGY08-08), Key Program of National Natural Science Foundation of China (No. U1836203)

成和发展。2006年沈荣骏给出了天地一体化航天互联网的概念^[1]。2015年张乃通等^[2]给出了对天地一体化信息网络定位、边界的说明以及对网络基本架构的设想。参考文献[3]和参考文献[4]给出了天地一体化信息网络的整体架构：由天基信息网（包括天基骨干网、天基接入网和地基节点网3部分）、地面互联网和移动通信网互联互通形成天地一体化信息网络。系统组成示意如图1所示。其中天基骨干网由多个高轨骨干节点（处于地球同步轨道）组成，主要实现的功能有宽带接入、数据中继、信息存储等。天基接入网由多个接入节点（处于高轨或低轨）组成，在陆地、海洋、空中、太空各层次满足海量用户的语音、数据等多种网络接入服务需求。地基节点网由多个地基骨干节点联网组成，主要实现对天基网络的控制管理、信息处理，以及天基信息网络与地面互联网和移动通信网等地面系统的连通等功能^[5]。

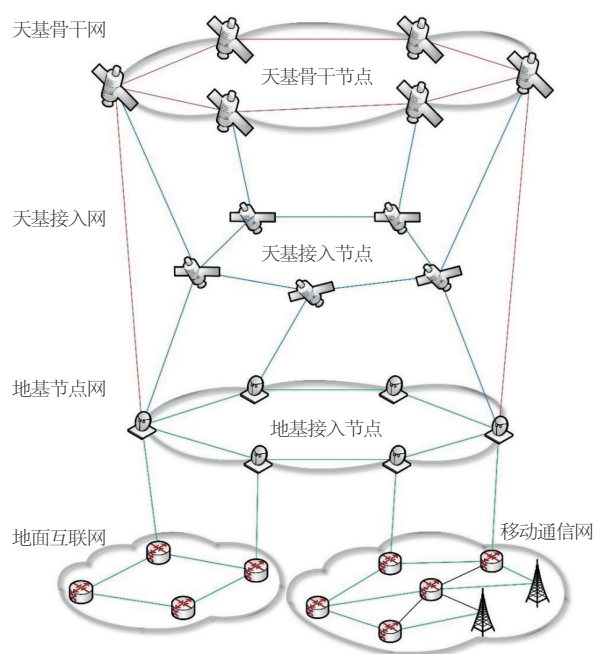


图1 系统组成示意

在天地一体化信息网络场景中，卫星节点与地面站需进行通信来实现接入认证等机制，因此如何保证通信数据的安全至关重要。常见的思路是应用密码学相关知识对通信数据进行加密处理，而加解密算法所需的对称密钥需要通信双方通过密钥交换得到，因此密钥交换是重点所在。密钥交换（也称为密钥协商）在密码学中是一种基本的协议，它允许通信参与方在公开的网络环境中通过交互建立一个共享的会话密钥，通过对传输数据进行加解密来实现通信内容的隐私和安全。

天地一体化信息网络中节点的存储空间和带宽是有限的，卫星网络和地面网络在计算能力、存储空间、高丢包率、动态拓扑、响应时间等方面区别很大，因此卫星网络中使用的协议需满足上述特定需求。第一，卫星节点上运行的密钥交换协议需尽可能的轻量级、低成本。对此本文考虑使用非交互式密钥交换协议的原型和基石——Diffie-Hellman密钥交换协议，非交互的特性可以满足天地一体化信息网络场景中通信能耗和通信带宽小的需求；第二，卫星节点中运行协议过程的短响应时间也需要考虑。集中式协议存在计算复杂、中心瓶颈、响应时间长等问题，短响应时间难以实现。对此本文考虑使用具有分布式、去中心化等特性的区块链技术。

Diffie-Hellman密钥交换协议未对协议参与者进行身份认证，无法抵抗中间人攻击，需引入认证保护机制，对Diffie-Hellman交换进行鉴别来抵抗中间人攻击。区块链的用户节点通过对自己创建的交易进行数字签名来实现身份认证，因此Diffie-Hellman密钥交换协议结合区块链技术可以弥补未进行身份认证的安全性缺陷、增强协议的安全性。综上，本文面向天地一体化信息网络场景提出基于区块链和Diffie-Hellman密钥交换协议的非交互式密钥交换方案，有其理论研究价值和实际应用价值。在天地一体化信息网络场景下，卫星节点和地面网络控制中心等远距离节点可在非交互的条件下基于区块链完成非交互式密钥交换，得到共享密钥，进而加密通信内容来保证通信的安全性和隐私性。

2 相关工作

2.1 区块链在卫星通信领域的应用

区块链的蓬勃发展使得其在许多领域被广泛使用。在卫星通信领域，WEI等^[6]结合基于身份的加密和区块链技术，提出了一种在低轨道卫星移动通信系统中进行快速有效访问的验证协议，其中密钥生成中心、卫星和用户基于区块链组成信任链，基于区块链存储用户和卫星信息来保证存储数据的准确性、完整性、一致性和可追溯性，并在OPNET上对提出的协议进行仿真来检验其有效性、可靠性和快速切换的效率。马煜^[7]基于区块链技术设计了一个星间通信网络安全加密系统，其中区块链技术的载体是低轨卫星，基于区块链技术实现分布式数字化身份加密技术，进而实现星间通信网络的安全加密，并通过实验验证了该系统的有效性。CLARK等^[8]利用区块链技术为卫星中继网络设计了一个安全的、分布式的信誉系统，利用区块链对卫星和地面站已有的信誉数据进行维护和更新，通过Python编写的离散事件网络模拟器对分布式信誉系统进行仿真，并从平均时延、计算复杂性和存储等

方面分析网络性能。参考文献[8]最先对卫星网络中基于区块链的信誉系统进行研究。FENG等^[9]利用区块链和卫星通信的优势,提出了一个区块链增强型移动卫星通信网络的新框架,通过数值模拟和实验验证了该框架的有效性,不仅可以有效检测网络攻击,还可以通过通信和卫星管理更好地保护移动卫星通信网络。

2.2 基于区块链的非交互式密钥交换

非交互式密钥交换(Non-Interactive Key Exchange, NIKE)是一种基本的但易被忽视的密码学原语,DIFFIE和HELLMAN于1976年发表的论文^[10]中提出了在开放的信道上建立共享密钥的协议——Diffie-Hellman密钥交换协议,在非交互式密钥交换这一领域具有开创性的贡献。不过该协议本身是一个匿名的密钥交换协议,没有进行身份认证,攻击者可以拦截并篡改消息内容伪造通信对方来实现中间人攻击。FREIRE等^[11]给出了非交互式密钥交换的概念:在非交互式密钥交换方案中,任何双方都可以在不进行任何交互的情况下计算得到一个公共的共享密钥。具体来说,NIKE方案使得A方可以从A的私钥 sk_A 和B的公钥 pk_B 计算出双方共享的密钥 $K_{AB}=K_{BA}$ 。

非交互式密钥交换协议可以结合区块链技术来实现密钥交换、密钥分发和身份认证等功能。MCCORRY等^[12]首次提出了比特币密钥交换协议来保证通信的安全性,协议中使用了椭圆曲线数字签名算法。张佳妮等^[13]在此基础上进行了改进,针对物联网场景提出了两个物联网密钥协商协议,其中基于Diffie-Hellman的比特币密钥协商协议属于非交互式密钥交换的范畴,使用了基于身份的Schnorr签名算法来实现轻量级的身份认证,参与通信的用户需要获取对方的交易签名对来计算得到共享密钥。OWOH等^[14]提出了一个移动区块链的集成框架,其中使用椭圆曲线Diffie-Hellman算法来解决基于移动区块链的传感应用中客户端和边缘节点之间的密钥交换问题。MUTH等^[15]将Diffie-Hellman密钥交换方案以智能合约的形式实现,并对其进行测试和评估。

综上所述,由于区块链具有去中心化、不可篡改、不可伪造、可追溯、可信任等特性,区块链技术在卫星互联网中具有很大的应用价值,通过仿真和实验,证明在一定场景下应用区块链技术可提高卫星网络的通信效率和安全性。因此在天地一体化信息网络卫星安全组网认证过程中,本文考虑利用区块链技术来解决高速移动的卫星节点与地面认证节点之间的非交互式密钥交换问题。

3 背景知识

下面对Diffie-Hellman密钥交换协议和区块链技术等

背景知识分别进行简要介绍。

3.1 Diffie-Hellman密钥交换协议

Diffie-Hellman密钥交换协议流程如下。若用户A和B要进行Diffie-Hellman密钥交换:

(1) A和B需要共享相关参数:素数 p 和它的本原根 g ($2 \leq g \leq p-1$);

(2) A和B分别随机生成会话私钥 a 、 b ,计算会话公钥 K_A 、 K_B 并发送给对方

$$K_A = g^a \bmod p \quad (1)$$

$$K_B = g^b \bmod p \quad (2)$$

(3) A和B分别计算它们的共享密钥 K_{AB} 和 K_{BA} ($K_{AB}=K_{BA}$)如下

$$K_{AB} = K_B^a \bmod p \quad (3)$$

$$K_{BA} = K_A^b \bmod p \quad (4)$$

3.2 区块链技术

区块链技术起源于比特币。2008年,NAKAMOTO发布的文章^[16]标志着基于分布式可信系统建立的数字资产——比特币的成功问世,从比特币中抽离出来的区块链技术也引起了人们的热切关注。区块链属于链式数据结构,每个区块包含前一个区块信息的散列值来形成一条区块链。区块链具有去中心化、开放透明、可靠数据库、自治性、不可篡改、准匿名性等特征,融合了密码学、共识机制、分布式存储等多种技术。其应用密码学中的非对称加密、数字签名等相关知识来保证系统的安全性;应用共识机制可以在区块链去中心化的系统中使不同节点达成一致;应用分布式存储使得记账过程由多个节点共同完成,保证了记账的安全性。区块链高速发展的同时给物联网、医疗、经济、卫星通信等多领域多行业带来了更大的潜在影响和应用价值。

区块链可以分为公有链、私有链和联盟链。

(1) 公有链:公有链类似于公共数据库,面向大众,所有人均可自由参与和退出,其特点是完全去中心化。

(2) 私有链:私有链的应用场景通常是一个组织或企业内部,私有链的权限仅掌握在一个组织手中,由组织定义读写、记账等规则。

(3) 联盟链:联盟链具有多中心化或部分去中心化的特征,预选节点可控制共识过程、一起决定区块的生成,其他节点无法参与记账,只能参与交易。联盟链的共识机制常使用效率较高、多中心化的共识算法。相比公有链,联盟链在安全、性能方面的要求较高,需要一定的权限才能加入联盟链;并且联盟链节点数量受限制,易达成共识,交易速度很快。因此本文考虑在天地

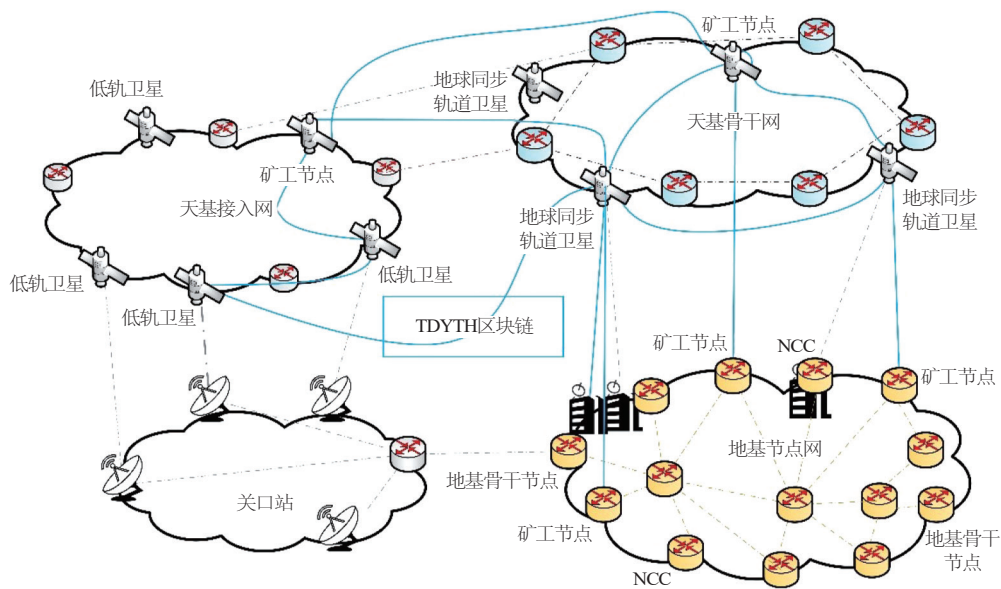


图2 场景示意

一体化信息网络中部署联盟链。

4 方案设计

天地一体化信息网络由于天地一体的组网结构，存在卫星资源受限、通信时延大、有限的信道和计算条件下通信双方无法达成长久有效共识等问题，因此不适合直接使用密码强度高、轮数多的密码协议来完成必要的密钥更新、密钥交换和接入认证。针对上述问题，本文基于天基卫星网络及区块链的共识机制，提出了一个基于区块链的非交互式密钥交换方案，其中非交互式密钥交换基于Diffie-Hellman密钥交换协议。在接入认证过程中，当卫星节点需要和地面网络控制中心（Network Control Center, NCC）进行安全通信时，可通过查询区块链中保存的特征信息来创建共享密钥，进而加密通信内容来保证通信的安全性。

4.1 网络拓扑与安全模型

本文提出的方案基于联盟链的思想，在天地一体化信息网络中部署区块链的可信网络——本文称之为TDYTH区块链。天基骨干网、天基接入网的卫星节点以及地基节点网的关键网络节点（如NCC、关口站）均通过注册成为TDYTH区块链中的节点共同构成TDYTH区块链的分布式网络，如图2所示。TDYTH区块链中的节点按角色可划分为矿工节点和用户节点。TDYTH区块链中的矿工节点接收用户节点发来的信息，竞争得到记账权后记录上链（类似于挖矿过程，不过由于卫星节点资源受限，矿工节点使用的工作量证明的共识机制可通过将难



图3 会话结构

度乘以较小的权重，减少散列运算来降低记账难度，减少其对卫星资源的消耗）。用户节点主要通过非交互式密钥交换来协商得到共享密钥，其非交互式密钥交换记录均存储在TDYTH区块链账本中，由TDYTH区块链中的各节点共同维护。本文提出的TDYTH区块链对传统区块链的交易模式进行了改进，改进后的交易称为会话，其结构如图3所示，TDYTH区块链结构如图4所示。

4.2 基于区块链的天地一体化信息网络卫星接入非交互式密钥交换方案

在天地一体化信息网络卫星接入认证场景下，地面的NCC主要负责对卫星节点进行身份注册、存储注册的相关信息以及验证卫星节点的身份。接入认证前，合法

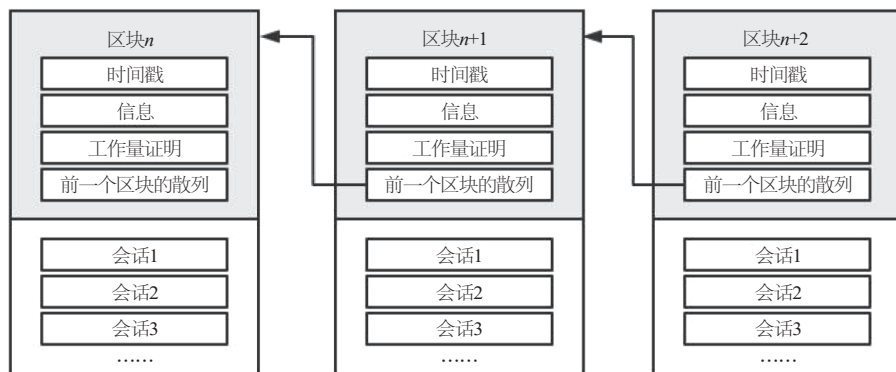


图4 TDYTH区块链结构

的卫星节点需线下向NCC进行身份注册，注册相关的特征信息存储在放置于卫星节点内部的认证卡中，同时也存储在NCC中。基于TDYTH区块链，卫星节点与NCC可通过会话形式进行非交互式密钥交换得到共享密钥、加密通信内容来实现安全通信。在非交互式密钥交换进行前，有以下流程需执行。

(1) 卫星节点和NCC均注册成为TDYTH区块链中的用户节点，拥有自己的公钥（等同于地址，对应身份信息）、私钥（即主私钥，可派生得到会话私钥）以及非交互式密钥交换所需参数（素数、原根）。

(2) 卫星节点线下向NCC进行身份注册，注册信息包括卫星节点的公钥、素数和原根等。

(3) NCC接收到卫星节点发来的身份注册信息后，将注册信息包含的卫星节点的公钥、素数和原根存储到TDYTH区块链账本中，即TDYTH区块链账本中存储着已向NCC进行身份注册的合法卫星节点的相关信息。

(4) NCC自己的公钥、素数和原根也存储到TDYTH区块链账本中。

注册阶段完成后，卫星节点和NCC即可进行非交互式密钥交换。假设卫星节点想要和NCC进行通信，且卫星节点和NCC均已知对方在TDYTH区块链中的公钥（地址），非交互式密钥交换方案具体流程如下。

(1) 卫星节点由主私钥派生成会话私钥，然后创建会话，提交自己的公钥（地址）、NCC的公钥（地址）、附加信息（可设定特定格式代表进行非交互式密钥交换），由自己的素数和原根计算得到会话公钥和会话签名，将包含以上内容的会话进行广播。

(2) 接收到卫星节点发出的会话、竞争获得记账权的矿工节点通过验证签名确认会话有效性后，将会话所在的当前区块添加到TDYTH区块链上。

(3) 用户节点可以从矿工节点的指定接口查询得到

TDYTH区块链中存储的会话，通过查询，NCC可得到卫星节点的地址、附加信息、会话公钥等信息，得知某个卫星节点想与自己进行非交互式密钥交换。此时NCC可查询注册阶段存储在TDYTH区块链账本中的合法卫星节点（存储信息包含地址、素数和原根）是否包含该卫星节点。若包含，说明该卫星节点是合法的，可进行接下来的密钥交换流程，NCC创建会话，由查询得到的该卫星节点的素数和原根计算得到会话公钥，其余信息同流程（1），然后将会话进行广播。此时NCC可由自己的会话私钥、卫星节点的会话公钥和素数进行模幂运算得到共享密钥；若不包含，说明该卫星节点不是合法的，NCC可拒绝进行后续流程。

(4) 同流程（2），矿工节点将包含NCC会话的当前区块添加到TDYTH区块链上。

(5) 卫星节点通过查询会话，可以得到NCC的会话公钥等信息。卫星节点可由自己的会话私钥、素数以及NCC的会话公钥进行模幂运算得到共享密钥。

非交互式密钥交换方案流程如图5所示。

5 实验设计与验证

由于实验条件限制，本工作仅针对所提出的基于区块链的非交互式密钥交换过程进行仿真实验。

5.1 实验环境与参数设置

本文在搭建TDYTH区块链平台的基础上仿真实现卫星节点和NCC间的非交互式密钥交换流程。系统前端使用Bootstrap框架，后台使用Python语言进行功能模块的开发，采用B/S架构仿真实现基于区块链的非交互式密钥交换方案。

系统的硬件、软件测试环境见表1、表2。

5.2 实验结果与分析

TDYTH区块链的用户节点（卫星节点和NCC）在注

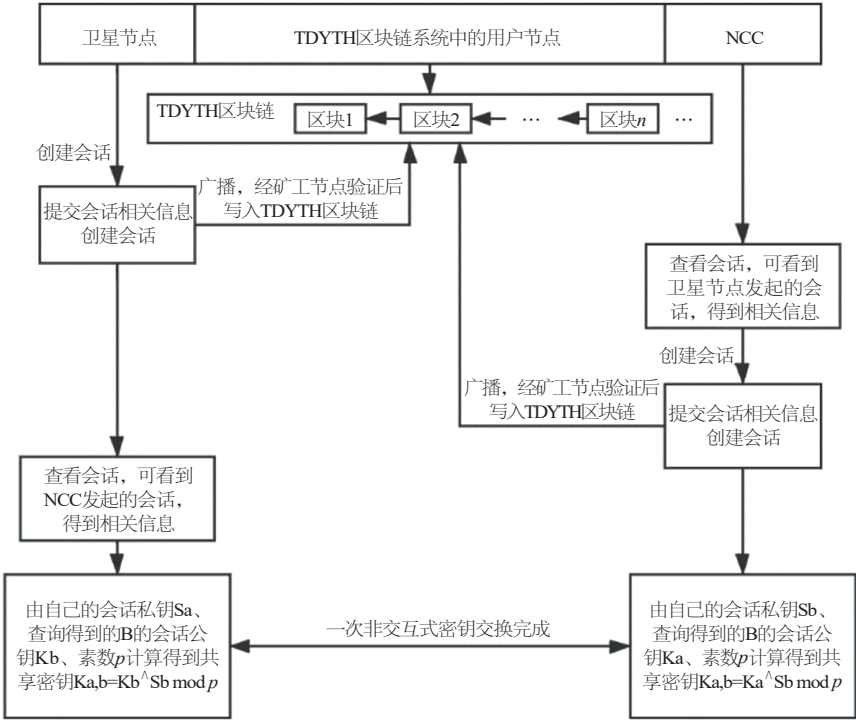


图5 非交互式密钥交换方案流程

表1 硬件测试环境

硬件配置	版本型号
处理器	Intel(R) Core(TM) i5-4210H CPU @2.90 GHz 2.90 GHz
内存	8.00 GB
硬盘	KINGSTON SUV400S37240G
网卡	Intel(R) Dual Band Wireless-AC 3160
显卡	Intel(R) HD Graphics 4600

表2 软件测试环境

软件配置	版本型号
操作系统	Windows 10
编程语言环境	Spyder 3.3.1
系统开发框架	Flask 0.12.2
数据库	MySQL 8.0.15

册时获得自己的公钥（等同于地址）、私钥、素数 p 和 p 的原根 g ，通过会话的形式公开附加信息、会话公钥，对会话进行数字签名来实现认证功能。通信对方通过查询会话得到所需信息后即可创建共享会话密钥，如图6所示。每次创建会话生成的会话私钥以及每次计算得到的共享密钥均存储在本地数据库MySQL中，输入双方的地址即可查询得到对应的共享密钥，如图7所示。TDYTH区块链的矿工节点接收到用户节点发出的会话后，通过

竞争获得记账权，然后将当前包含用户节点发出会话的区块添加到TDYTH区块链上。如果TDYTH区块链中有多个矿工节点，则利用一致性算法；若矿工节点存储的区块链不是最长的可以替换为最长的区块链来解决节点间的冲突问题。

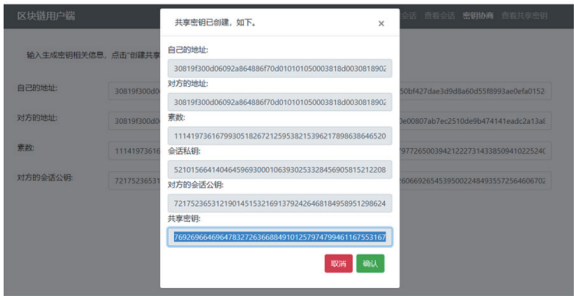


图6 共享会话密钥创建成功



图7 用户查看共享密钥

方案中用户节点的私钥长度设置为1 024 bit, 大素数 p 的长度设置为512 bit。运行方案的整体流程50次, 得到了方案的平均执行时间, 分为前期准备阶段P1和密钥交换阶段P2。前期准备阶段从创建会话开始到查询得到对方的会话公钥等相关信息结束。密钥交换阶段即双方通过计算得到共享会话密钥。方案执行时间见表3, 耗时较长的前期准备工作完成后, P2阶段实现密钥交换所需的轻量运算用时很短即可完成, 因此本方案具有合理的计算开销。

表3 方案执行时间

阶段	所用时间/ms
P1	$201 \times 2 = 402$
P2	1.815
总计	403.815

经测试, 本文提出的基于区块链的非交互式密钥交换方案可以成功实现。通信双方(卫星节点和NCC)每次计算得到的当前最新的会话私钥以及共享密钥均存储在本地数据库中, 所需存储空间较小。此外, 本方案中双方公开自己的会话公钥后, 只需计算就可以获得共享密钥, 交互次数大大减少, 密钥交换效率得到了提高。在天地一体化信息网络卫星接入认证场景下, 即使NCC和卫星节点连接中断, 在已知双方会话公钥的前提下, 它们仍可以通过查询TDYTH区块链中已存储的信息得到共享密钥来进行通信。

ETSI EN 301 790 V1.5.1^[17]中规定的主密钥交换(Main Key Exchange, MKE)协议同样是在Diffie-Hellman密钥交换协议的基础上生成NCC和回传链路卫星通信终端(Return Channel Satellite Terminal, RCST)之间的共享会话密钥, 不过MKE存在中间人攻击的安全缺陷, 攻击者可以截获双方传输的通信消息并进行篡改。本方案中由于使用区块链, 通信双方NCC和卫星以会话的形式发出信息, 并包含对应身份信息的地址, 因此攻击者不能冒充一方对信息进行篡改以实现中间人攻击。此外使用区块链技术, 使得本方案具有可溯源特性。

综上, 本文提出的方案适用于在天地一体化信息网络等资源受限和时延较大的环境中使用。

5.3 安全性分析

由于密钥交换协议需要具备一定的安全性, 故依次分析本方案是否满足下列安全属性。

(1) 抵抗已知会话密钥攻击: 即使攻击者获得了以前使用过的某个或某些共享会话密钥, 也无法通过计算

和推导来确定现在使用的和以后将要使用的会话密钥是什么, 这就是抵抗已知会话密钥攻击。本方案中TDYTH区块链中用户节点的会话私钥由主私钥密钥派生得到, 其中加入了盐值和迭代次数, 因此每次产生的会话私钥都不同, 计算得到的共享密钥也不同, 可以保证共享会话密钥间的独立性。所以本方案可以抵抗已知会话密钥攻击。

(2) 抵抗中间人攻击: 中间人攻击是指攻击者通过非法窃听得到通信内容, 然后拦截、篡改消息, 成为网络双方通信的中间者, 从而控制整个会话, 获取双方的通信信息, 包括生成的共享密钥。中间人攻击可以执行的根本原因是协议双方无法通过身份认证来证明自己的身份。本方案中TDYTH区块链的用户节点使用私钥签名会话来进行身份认证, 且会话均记录在TDYTH区块链账本上, 攻击者不能在通信双方不知情的情况下成为它们之间的中间者来控制会话密钥的生成, 所以本方案可以抵抗中间人攻击。

(3) 前向安全性: 前向安全性是指即使通信参与者的私钥长期被泄露, 攻击者也无法计算得到在此之前产生的共享会话密钥, 即不影响之前产生的共享会话密钥的使用。本方案中, 即使攻击者知道了TDYTH区块链用户节点的私钥, 每次密钥交换由私钥密钥派生得到的会话私钥都是随机产生的(密钥派生函数中使用的盐值是随机产生的, 迭代次数也会改变), 所以攻击者无法由会话私钥计算得到共享密钥。同时如果攻击者想要查询共享密钥也是不可能实现的, 因为查询操作针对的是本地数据库的内容, 攻击者无法得到用户节点本地数据库中存储的内容, 所以攻击者即使知道通信双方的地址, 也无法得到它们的共享密钥。由此可见本方案可以满足前向安全性。

(4) 密钥不可控制性: 密钥交换协议应该满足通信双方对密钥交换协议的贡献程度是相同的。所有协议参与方都不能控制密钥交换过程及预先控制生成的共享会话密钥的值, 这就是密钥不可控制性。本方案中, 通信双方每次的会话私钥和会话公钥都不相同, 无法提前预测, 且双方计算得到共享密钥的贡献程度是相同的, 所以本方案可以满足密钥不可控制性。

(5) 抵抗密钥泄露攻击: 假如用户的私钥长期被泄露, 攻击者可以冒充该用户与其他用户通信, 但是其无法冒充其他用户与该用户通信, 这就是抵抗密钥泄露攻击。本方案中TDYTH区块链中用户节点的地址就是其公钥, 是公开、唯一且记录上链的, 攻击者无法假冒已有的用户来进行攻击, 所以本方案可以抵抗密钥泄露攻击。

6 结束语

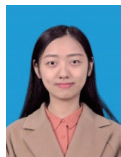
本文在区块链技术的基础上提出了一个非交互式密钥交换方案并进行了仿真实验,区块链只能增加不能篡改及删除的存储特性以及去中心化、不依赖第三方机构的特性使得密钥交换过程更加公开透明,降低了被攻击的可能性,提高了非交互式密钥交换的安全性。在天地一体化信息网络场景下搭建TDYTH区块链,TDYTH区块链中的用户节点通过会话形式公开密钥交换所需信息,对会话进行数字签名来实现身份认证功能;之后只需查询对方公开的会话即可计算得到共享会话密钥,交互次数大大减少,传输效率得到了提高。用户节点本地数据库中保存的会话私钥和共享会话密钥都是当前最新的,所需存储空间较小,因此适用于卫星等资源受限的节点。在天地一体化信息网络卫星接入认证过程中,即使NCC和卫星的通信中断,它们仍可通过查询TDYTH区块链中存储的公开信息来计算得到共享密钥。因此本文提出的方案适合在天地一体化信息网络等资源受限和时延较大的环境中使用。本文主要将区块链、Diffie-Hellman密钥交换协议结合到一起初步应用于天地一体化信息网络场景中,为天地一体化信息网络场景下应用区块链技术提供了一种新思路,下一步将在此基础上,结合天地一体化信息网络场景设计和实现详细的认证协议。

参考文献：

- [1] 沈荣骏. 我国天地一体化航天互联网构想[J]. 中国工程科学, 2006, 8(10): 19-30.
- SHEN R J. Some thoughts of(Chinese) integrated space-ground network system[J]. Engineering Science, 2006, 8(10): 19-30.
- [2] 张乃通, 赵康健, 刘功亮. 对建设我国“天地一体化信息网络”的思考[J]. 中国电子科学研究院学报, 2015, 10(3): 223-230.
- ZHANG N T, ZHAO K L, LIU G L. Thought on constructing the integrated space-terrestrial information network[J]. Journal of China Academy of Electronics and Information Technology, 2015, 10(3): 223-230.
- [3] 张平, 秦智超, 陆洲. 天地一体化信息网络天基宽带骨干互联系统初步考虑[J]. 中兴通讯技术, 2016, 22(4): 24-28.
- ZHANG P, QIN Z C, LU Z. The space wideband backbone interconnected system in the integrated space and terrestrial information network[J]. ZTE Technology Journal, 2016, 22(4): 24-28.
- [4] 吴曼青, 吴巍, 周彬, 等. 天地一体化信息网络总体架构设想[J]. 卫星与网络, 2016(3): 30-36.
- WU M Q, WU W, ZHOU B, et al. The overall framework of integrated information network [J]. Satellite & Network, 2016(3): 30-36.
- [5] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.
- LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.
- [6] WEI S J, LI S, LIU P L, et al. BAVP: blockchain-based access verification protocol in LEO constellation using IBE keys[J]. Security and Communication Networks, 2018: 1-14.
- [7] 马煜. 基于区块链的星间通信网络安全加密控制系统设计[J]. 计算机测量与控制, 2021, 29(3): 171-175.
- MA Y. Design of inter satellite communication network security encryption control system based on blockchain[J]. Computer Measurement & Control, 2021, 29(3): 171-175.
- [8] CLARK L, TUNG Y C, CLARK M, et al. A blockchain-based reputation system for small satellite relay networks[C]// Proceedings of 2020 IEEE Aerospace Conference. Piscataway: IEEE Press, 2020: 1-8.
- [9] FENG M, XU H. MSNET-blockchain: a new framework for securing mobile satellite communication network[C]//Proceedings of 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). Piscataway: IEEE Press, 2019: 1-9.
- [10] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [11] FREIRE E S V, HESSE J, HOFHEINZ D. Universally composable non-interactive key exchange[M]//Lecture Notes in Computer Science. Cham: Springer International Publishing, 2014: 1-20.
- [12] MCCORRY P, SHAHANDASHTI S F, CLARKE D, et al. Authenticated key exchange over bitcoin[M]//Security Standardisation Research. Cham: Springer International Publishing, 2015: 3-20.
- [13] 张佳妮, 何德彪, 李莉. 基于区块链的物联网密钥协商协议[J]. 中兴通讯技术, 2018, 24(6): 23-27.
- ZHANG J N, HE D B, LI L. Blockchain-based key agreement protocol for Internet of Things[J]. ZTE Technology Journal, 2018, 24(6): 23-27.
- [14] OWOH N P, MAHINDERJIT M. Applying Diffie-Hellman algorithm to solve the key agreement problem in mobile blockchain-based sensing applications[J]. International Journal of Advanced Computer Science and Applications, 2019, 10(3): 59-68.

- [15] MUTH R, TSCHORSCH F. SmartDHE: Diffie-Hellman key exchange with smart contracts[C]//Proceedings of 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS). Piscataway: IEEE Press, 2020: 164-168.
- [16] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB].
- [17] ETSI EN 301 790 V1.5.1. Digital Video Broadcasting (DVB); Interaction Channel for Satellite Distribution Systems[S]. 2009.

[作者简介]



刘梦如（1998-），女，西安电子科技大学硕士生，主要研究方向为区块链、隐私保护。



付玉龙（1983-），男，西安电子科技大学副教授，主要研究方向为移动网络安全、大数据及人工智能安全、形式化安全。



曹进（1985-），男，西安电子科技大学教授、博士生导师，主要研究方向为4G/5G网络、天地一体化信息网络安全性及认证协议设计与分析。



李晖（1968-），男，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。