计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180431
55(10):2244-2255,2018

基于共识机制的LEO低轨卫星网络区域合作认证协议

魏松杰[1] 李 帅[1] 莫 冰[2] 王佳贺[1]
[1](南京理工大学计算机科学与工程学院 南京 210094)
[2](南京理工大学机械工程学院 南京 210094)
(swei@njust.edu.cn)

Regional Cooperative Authentication Protocol for LEO Satellite Networks Based on Consensus Mechanism

Wei Songjie[1], Li Shuai[1], Mo Bing[2], and Wang Jiahe[1]
[1](*School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing* 210094)
[2](*School of Mechanical Engineering, Nanjing University of Science and Technology, Nanjing* 210094)

Abstract Authentication is an important point of satellite network security. On the premise of security, it is one of the research hot spots that how to design efficient authentication scheme according to the ability of satellite network. Nowadays, researches about authentication scheme of LEO satellite network mainly focus on reducing the calculation consumption with low cost computation, like Hash operation, while ignoring the features of LEO satellite network like dynamic topology and frequent link switch etc. On the other hand, the consensus mechanism of blockchain is drawing more and more attention. Through the consensus mechanism, internal nodes of network reach a consensus and confirm the synchronization of transactions among the whole network. Based on these, a regional cooperative authentication protocol is proposed, which makes LEO network dynamic topology abstract with regional division and implements efficient handover authentication by consensus among satellites. Additionally, the proposed protocol reaches the fast switch by combining the method of distributed Hash table and Hash lock, which are light in computation and can avoid the defect that each authentication with normal authentication way is a brand new authentication phase. For the security and performance, a contrastive analysis to relevant researches in these years is made. At last, the protocol is simulated with a LEO network scenario similar to Iridium system upon OPNET network stimulation platform. And the results of simulation show that the performance of the protocol is obviously superior to existing authentication protocols in satellite network.

Key words consensus mechanism; LEO satellite network; access authentication; distributed Hash table; regional division

收稿日期:2018-06-12;**修回日期**:2018-08-11

基金项目:国家自然科学基金项目(61472189);航天科技创新基金项目(F2016020013);空中交通管理系统与技术国家重点实验室开放课题(SKLATM201703)

This work was supported by the National Natural Science Foundation of China (61472189), the CASC Innovation Fund (F2016020013), and the Opening Project of the State Key Laboratory of Air Traffic Management System and Technology (SKLATM201703).

通信作者:李帅(116106000732@njust.edu.cn)

摘 要 接入认证是卫星网络安全的重要课题,在保证安全性的前提下,如何根据卫星网络的能力设计快速高效的认证方案是研究的热点之一.目前,针对 LEO 低轨卫星网络的接入认证方案研究主要集中在利用 Hash 等计算消耗低的方式减轻认证方案的计算消耗,而忽视了 LEO 低轨卫星网络动态拓扑以及链路切换频繁等特点.另一方面,区块链的共识机制一直以来是区块链领域的研究热点,通过共识机制,网络内节点以特定方式达成对某一交易的共识,完成其在全网的同步.借鉴于此,在总结 LEO 卫星网络的特点基础上,利用区域划分抽象 LEO 卫星动态拓扑的特点,同时利用区块链中的共识机制思想,在 LEO 卫星网络分布式环境下建立卫星间对用户认证的共识.此外,通过结合分布式 Hash 表与 Hash 锁定等方式以较低的存储和计算开销,实现了用户在 LEO 卫星网络中的快速切换,规避了原有的每一次认证都是全新认证的缺陷,提高了切换认证的性能.在安全性和性能上,将所提出协议同近年来的相关研究进行了对比分析,得出提出的协议具备安全高效的特点.最后,通过在 OPNET 网络仿真平台构建类铱星网络场景,对所提出协议进行了仿真.仿真结果表明:该协议的性能要明显优于现有卫星网络中的其他认证协议.

关键词 共识机制;LEO 卫星网络;接入认证;分布式 Hash 表;区域划分

中图法分类号 TP393.02

众所周知,LEO(low earth orbit)卫星网络凭借其低延时、链路损耗低、全球覆盖性、部署灵活性等特点,愈来愈受到研究者们的关注,且随着通信技术的进一步发展,尤其是 5G 通信标准,LEO 卫星网络越来越成为建设空天地全方位通信网络不可或缺的部分.此外,对于新式的全球网络通信服务,如飞机上的网络服务等,LEO 卫星网络也以其诸多独特优势占据重要地位.

与此同时,卫星网络场景中的接入认证却仍然以传统的用户接入卫星、卫星通过网关传导至地面控制站的来回方式进行,此种方式一方面受到星上路由协议的性能影响,一方面因为认证涉及层级过多以及 LEO 卫星网络的链路频繁切换特点使得每一次切换导致的认证都是一次新的认证,从而导致效率非常低下.

另一方面,区块链技术以其不可篡改、去中心等特点日益受到全球学者的关注,并在近几年得到了飞速发展.目前,区块链主要分为公有链、联盟链(许可链)、私有链 3 种形式.公有链较为著名的有比特币和以太坊等,联盟链主要包括小蚁链、超级账本等,私有链则没有实际的研究价值.区块链中著名的蒙达尔不可能三角,即安全、去中心、高效三者不可能同时达成,决定了区块链技术在实际应用场景下往往需要采用联盟链的方式,即牺牲一定的去中心化程度来达成效率上的提升,以此来满足各种各样的业务需求.

LEO 卫星网络中,星上处理能力不断加强,多颗卫星处于平等地位,星上网络整体属于分布式环境,LEO 链路频繁切换的特点使得其不能继续沿用传统卫星网络中的认证策略,因而本文在借鉴联盟链多区域跨域共识思想的基础上提出了一种 LEO 卫星网络内的区域合作认证协议.

本文的主要贡献有 4 个方面:

1) 提出了一种 LEO 卫星网络中基于区块链共识思想的区域合作认证协议.通过将 LEO 卫星网络内多颗卫星按照轨间及轨道内进行区域划分,形成多区域的逻辑认证区域结构;

2) 基于多区域合作认证,每一区域内的任一卫星所认证的结果都在其所在区域内通用,从而满足快速链路切换的认证需求,此外,当出现跨域的切换时,认证将依赖于跨域间的共识认证,更加安全高效;

3) 在区域合作认证的基础上,将传统的认证层级进行缩减,由于 LEO 卫星具备了一定的星上处理能力,因而我们通过一定的存储和计算开销实现用户在星端的直接认证;

4) 在区域划分的方案上,本文综合分析不同区域划分方案的优劣,同时通过实验比对现有不同方案与本文所提协议的实验结果,仿真结果表明我们提出的 LEO 卫星网络内区域合作认证协议可以实现 LEO 卫星网络内的高效认证.

1 相关工作

在 LEO 卫星网络认证算法的研究上,较早期的为 Cruichshank[1] 提出的使用公钥机制以及加密数

据传输来对用户和卫星进行相互验证的认证协议，但是存在其涉及到的操作太过复杂的问题. 2003年，Hwang 等人[2]提出了一种不需要公钥体制的认证协议，但是存在每次用户需要验证的时候共享私钥都要更新的问题. 2005 年，Chang 等人[3]提出了一种只需要异或和 Hash 的双向认证协议，且在每一次认证会话中，网络控制中心不需要为用户生成私钥以及一个临时的身份，但是由于网络控制中心参与了每一次用户接入认证会话，因而其负担还是很重. Hwang 和 Chang 等人[2-3]提出的方案中网络控制中心都是一个瓶颈所在，因而整个系统的性能都会受限于网络控制中心，且一旦网络控制中心出现任何问题，整个系统就无法正常运转. 2012 年，GZheng[4]等人提出的认证协议中通过提高网关在认证过程中的作用改善了网络控制中心计算开销过大的问题，但是认证流程除了涉及到用户和卫星还包含了网关、网络控制中心等，增加了交互的层级数，增大了认证完成的用时. 2016 年，Wu[5]等人提出了一种轻量级的认证和密钥协商协议，其主要基于用户暂时性 ID 的同步机制. 以上这些认证协议往往只是在协议本身计算开销上的改进，认证的架构皆为包含网络控制中心(network control center, NCC)的集中式交互认证，忽略了 LEO 卫星网络的分布式环境.

在提升区块链平台性能的研究上，主要有 3 种流派，分别是以闪电网络为主、以股份授权证明(delegated proof of stake, DPOS)共识结合增加一定数目的超级节点为主、以重新设计区块链底层架构为主. 1)第 1 种方案的核心思想是将大量的交易在链外执行，并将最终的结果写入链上，以此来提高系统的交易吞吐量；2)第 2 种方案的核心思想依赖于股份授权证明共识机制，类似于人民代表大会制度，通过选取一定数量的代表来实现快速记账，提高系统交易 TPS 性能，同时结合设定一定数目的超级节点，来分别负责对应区域内的交易，从而进一步提升交易的记账和确认速度；3)第 3 种方案主要是通过构建并行化的底层区块链架构，如超级账本的 Fabric 项目[6]通过设立多个 channel 来实现针对不同领域账本的并行，同时多个 channel 之间可以互相读取，以此打通多个 channel，不再孤立.

蒙代尔不可能三角中的安全一般来说对于有安全需要的环境都是不可缺省的，因而本文借鉴区块链中的共识思想，通过将 LEO 卫星网络划分为多个区域，在多区域间对用户的认证达成共识，以此来完成用户在多区域间的快速切换，同时对于仅在单区域内发生的切换通信，本协议通过区域内对某一卫星认证的共识，完成用户在区域内的无缝切换，最终形成区域内部合作，外部跨域共识认证的分布式区域合作认证协议.

2 LEO 卫星网络中的区域划分方法

在本节中，我们主要介绍 LEO 卫星网络中逻辑认证区域的划分方法. 其中，2.1 节给出了区域组成的定义. 2.2 节描述了如何动态划分区域.

2.1 基本定义

目前传统的卫星网络认证协议往往着重于对用户、卫星、NCC 三者间认证协议所使用的密码体制研究，而忽视了 LEO 卫星网络低时延、分布式、具备星上处理能力和星间链路的特点，同时原有的集中式认证体系也使得 NCC 处于高负载，存在单点失效和性能瓶颈的问题. 区域合作认证的方式可以有效满足用户在 LEO 卫星网络场景中的快速切换需求. 在详细描述区域合作认证协议之前，我们先给出基本的符号解释和定义.

对于给定的 LEO 卫星网络，定义其轨道数为 p，每一轨道上常用卫星数目为 n，区域划分总数为 v，给定一划分区域 $A_i=(S_i,C_i)$，其中 S_i 为第 i 个划分区域中包含的非核心卫星集合，C_i 为第 i 个划分区域中的核心卫星集合，且有

$$p\times n=\sum_{i=1}^{v}(S_i+C_i), \tag{1}$$

其中，核心卫星集合为存储当前区域内所有卫星认证用户 token 的卫星集合，token 为经 NCC 签名后用户相关权限通证. 在区域划分较小时，核心卫星集合一般包含 1 颗或 2 颗卫星，多颗时会采用冗余备份策略，同时也用于区域内其他卫星根据认证索引寻求对应用户 token 时产生的路由负载上的优化与均衡. 非核心集合为存储当前区域内部分卫星认证用户 token 的卫星集合. 非核心卫星集合中的卫星采用分布式 Hash 表(distributed Hash table, DHT)的方式，在增加一定冗余的情况下，分布在非核心卫星集合的卫星中.

同时，因为 LEO 卫星网络的规律性拓扑，使得给定时刻的网络拓扑都是可以预测或者计算出来的，因而对于一特定轨道而言，其上划分的区域内卫星理论上会以轨道周期与区域划分范围的比值周期性重复.

对于一特定轨道,特定区域 A_i 划分而言,定义此区域的轨内划分规模为该区域在此轨道上包含的连续卫星数目减一,记为 q;对于轨间链路而言,该区域轨间划分规模为其所跨轨道数减一,记为 e,因此对于一划分区域,其规模即为 $q\times e$,且随着轨道周期,区域 A_i 将在同一位置上空周期性不断重复出现.

同时,区域的划分应当尽量减少轨间链路,轨内链路也应当适量包括,以上原则基于一个事实,以 LEO 卫星网络的典型代表 Iridium 铱星系统来说,轨间链路的持续时间往往只有 10 min 左右,但是轨内的卫星都是处于相对静止的,通信稳定且可持续.

2.2 区域的动态划分

区域的划分理论上可以有很多种,但需要结合 LEO 卫星网络系统以及使用该系统的群体的相关性:

区域的划分对于不经常移动的个人卫星通信用户而言,应当尽量覆盖.同时对于新式的卫星通信服务,如航班上的卫星网络服务,因其往往会大范围跨越轨道,包括轨间与轨内,而发生多次的切换通信.因而,在区域的划分上,卫星用户的认证 token 需在尽可能少的轨间链路上传播即可实现跨区域的共识认证.基于 token 的区域跨域共识认证协议将会在第 3 节阐释,这里暂不作详细描述.同时,用户接入卫星的活动也呈现区域性特点.综上,区域的划分往往需要结合实际的卫星通信接入流量的分布来作改善,且卫星通信接入流量的分布往往是不均匀的.另一方面,需要注意的是,随着 LEO 卫星通信网络在 5G 时代的发展和应用,其原本的接入流量分布不均等特点也会因为 LEO 网络相对更低的成本、更好的通信性能以及其固有全覆盖的优势而慢慢消失.因而基于以上,我们提出 3 种区域划分模型,并可根据星端的接入流量分布特性,由 NCC 通过指令进行动态部署.

在时间的维度上,区域 A_i 随同其所包含轨道卫星的运动而运动,即对于轨道运行周期的每一静止时间片内,区域 A_i 内的卫星成员都不变.在 2.1 节基本定义的基础上,对于任一 $q_i\times e_i$ 规模的区域 A_i,其轨内星间链路的通信代价记为 x,轨间星间链路的通信代价记为 y,则在用户接入卫星后所跨区域数目为 m 时,区域共识认证协议的通信代价 K:

$$K=\begin{cases} r(x\parallel y)_{q_i\times e_i}, & m=1;\\ m\times r(x\parallel y)_{q_i\times e_i}+(m-1)(x\parallel y), & m>1; \end{cases} \tag{2}$$

其中,r 为所采用冗余策略决定的冗余数.

由式(2)可以看出,跨域将使得区域共识认证的通信代价呈线性上升.对于活动范围始终在某一卫星可见通信区域或通信时间较短使得用户在通信期间仅见接入卫星所在区域内的卫星,用户的切换认证不发生跨域共识认证,仅在该区域内,通过区域内部卫星间的共识来达成对用户快速切换认证的实现.对于跨域的情况,通信代价会随着用户所跨区域的增多而线性增加.根据式(2)可以发现,在跨域时可以通过轨间星间链路或是轨内星间链路,因而,在区域划分时,所划分的不同区域间需要有处于同一轨道内的卫星,以减少跨域时的通信代价.另一方面,对于给定的冗余数,区域共识认证协议的存储代价 J:

$$J=m\times(r+1)\times b. \tag{3}$$

因而,划分区域需要在满足覆盖不跨域用户的前提下,范围尽可能的小.如果区域范围过大,虽然此时通信代价会较小,但会导致用户访问到冗余的非核心节点可能性很低,同时距离核心节点的通信距离又很远,因而接入认证的通信代价会很大.如果区域范围过小,虽然此时用户访问到冗余的非核心节点可能性很高,同时即使冗余的非核心节点中没有此用户的 token 存证,此用户接入的卫星到拥有此用户 token 存证的核心卫星集合的通信代价也会较小,但是相应的因为区域过小,所以会导致此用户的 token 存证在星端冗余的存储代价较高.综上,本节以类铱星系统(Iridium)提出了 3 种区域划分的方案,并可以动态根据需要使用,如图 1~3 所示.

首先对于跨域而言,因其在各种业务场景中的需要,如新型航空航天的互联网服务,因而要求区域间提供轨内星间链路,同时对于一定量活动范围较为固定的用户,区域需要尽可能地覆盖,而不是划分成多个区域来覆盖.图 1 所示三角相对于图 2 所示的矩形划分,每一区域内少了 2 条轨间星间链路,因而如果在同样覆盖用户的条件下,三角形的区域划分,通信上更优.但相对而言,矩形的区域划分又会覆盖更广的用户范围,耗费的存储代价也更小,缺点就是用户 token 在区域内按照 DHT 同步时,会耗费更高的通信代价.因而基于存储和通信代价的均衡考量,图 3 的区域划分则是一种较为适中的方案.值得注意的是,如果是活动范围小于所划分区域,同时用户接入时间分布上随机且独立于卫星运行的轨道周期,那么此用户的 token 存证将按照特定冗余策略在其所在区域的所属轨道上普遍存在.

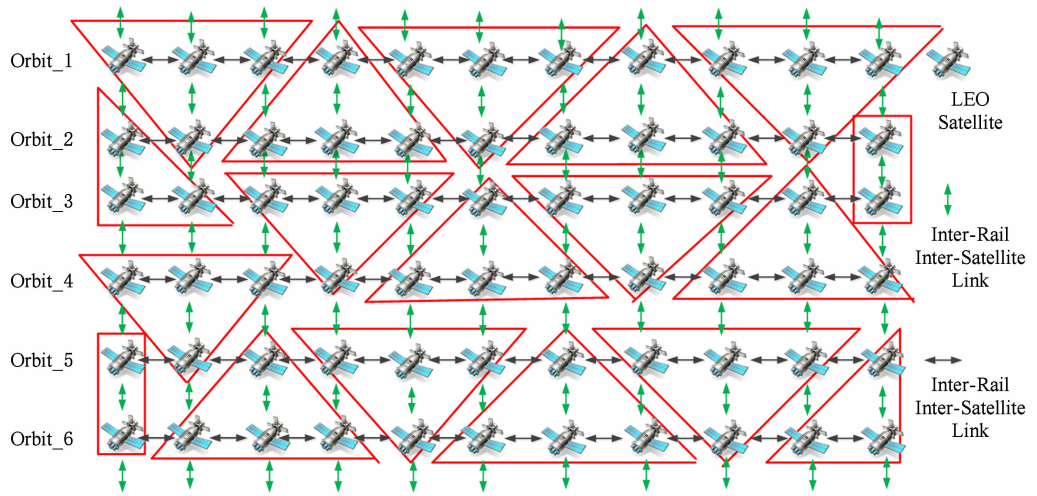

Fig. 1 Triangle-area division network structure

图 1 三角形区域划分网络结构

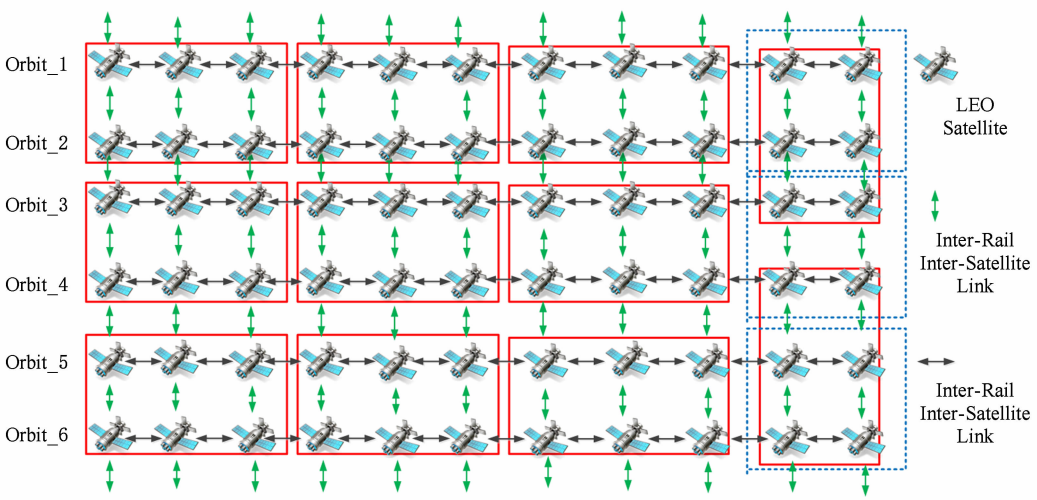

Fig. 2 Rectangle-area division network structure

图 2 矩形区域划分网络结构

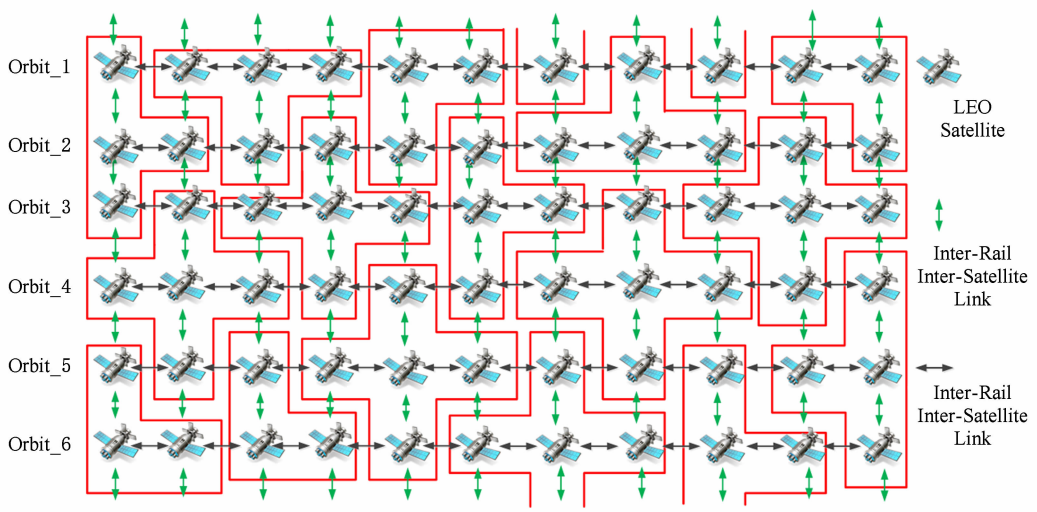

Fig. 3 Cross-area division network structure

图 3 十字形区域划分网络结构

3 基于共识的区域合作认证协议

本节详细介绍如何在给定划分区域的情况下,对于用户只在一颗卫星处持续使用通信服务、在一划分区域内持续使用通信服务和在多个划分区域间持续使用通信服务这 3 种情况下的区域共识认证协议.在阐述之前,首先阐释并分析目前现有的共识机制的缺点与优势.

3.1 共识机制

由于公链中广泛使用的共识机制[7-8],如基于工作量证明共识机制(proof of work, PoW),需要网络内节点通过付出算力来计算符合特定难度值的随机数串,从而使得其不适合于卫星等计算能力有限的网络场景,同时公链普遍存在的系统吞吐量(transactions per second, TPS)低的问题,也限制了这些共识机制可以应用的场景.

在传统卫星网络中,卫星充当的更多是一个通信路由中继的角色,不具备太多的星上处理能力,而在 LEO 卫星网络中,由于低轨和全覆盖特性,卫星数目明显多于传统卫星网络,星上网络为分布式环境,卫星节点具备一定星上处理能力和轨间星间链路,因而在网络架构上,LEO 卫星网络同联盟链具备共通点.同时,在共识机制上,联盟链一般通过对特定证书授权机构(certificate authority, CA),也就是公钥基础设施 PKI 的方式(如 Fabric)或者采用类似委任权益证明共识机制 DPOS 的方式,通过所有或大部分节点投票选出代表(也有称为主节点或超级节点),由代表进行交易的共识验证.PKI 的方式在卫星网络的认证方面早已有了广泛的应用,因而对于 PKI 的使用和改良会非常适合 LEO 卫星网络.在 DPOS 方面,考虑到所有卫星本身皆属于同一方以及卫星网络上投票方式的有效性受限于卫星网络链路和所使用路由算法的性能,其并不适合用于卫星网络的认证.

在 PKI 方面,以超级账本项目中的 Fabric 项目为例,其主要通过一个可信 CA 来进行证书管理,并基于此,完成身份认证和对应交易的认证,如图 4 所示.可信的 CA 负责对某一个通道(channel)(在 Fabric 中存在多个并行的 channel,每个 channel 是一个独立于其他 channel 的账本)生成根证书,同时对于此 channel 内的每一成员生成注册身份证书,用于对接入此 channel 的节点的认证管理.同时,在 CA 设置方面,CA 由多个根 CA(root CA, RCA)及多个中间 CA(intermediate CA, ICA)组成,对于 Fabric 网络内的任何 channel,它都由一个根 CA 及多个中间 CA 组成的信任链来进行证书管理的相关工作.这一方面是为了扩展性考虑,另一方面,此种方式也限制了根 CA 的暴露,提高了安全性.

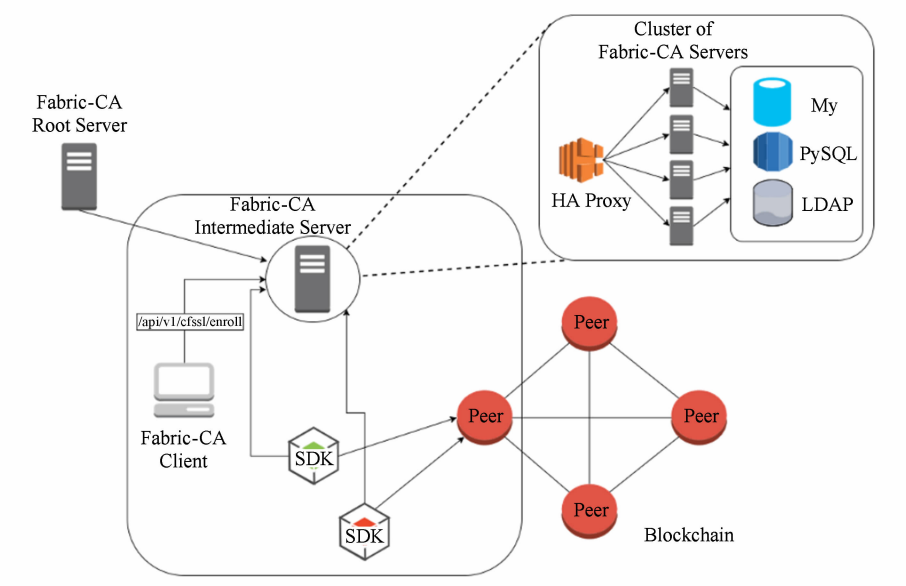

Fig. 4 Principles of CA authentication in Fabric

图 4 Fabric 中的 CA 认证机制原理

同时,值得注意的是,著名的公链平台以太坊目前针对以太坊 TPS 只有 7~15 笔/秒交易的低性能情况,将要研究采用分片技术来提高系统的扩展性和性能.其核心思想为对网络整体状态的划分,区域只

负责区域内的交易,区域的校验块(collation,为了和block概念区分,但本质类似)中校验块头(collation header)将会以区块的方式存在于主链之上,以此来扩展以太坊的系统吞吐能力.同时这只是次方分片方案,还会有超二次方分片方案,但其核心都是分区域的思想.基于以上分区域的思想,考量LEO卫星网络内的认证方式,本文所提出的区域合作共识认证协议通过在区域内卫星节点间建立一种共识,克服传统卫星网络中每一次切换带来的认证都会是一次全新的认证的缺点.同时,在多区域间,达成一种对于用户认证的共识.

3.2 区域合作认证协议

本文所提区域合作认证协议分为区域内和跨区域2部分.对于区域内,同一用户在区域内不同卫星处的认证结果共识主要通过DHT来达成.其基于一个合理的原则,即当用户因为在星间发生切换而不得不同切换后的卫星重新认证时,切换后的卫星应当同切换前的卫星通过某种方式达成对此用户先前认证结果的共识,而不是同用户进行一次全新的认证过程.借由此共识,正常认证过程中涉及的计算以及卫星和用户间的通信都可以避免,从而在保证安全性的前提下为用户提供无缝切换的用户体验.对于跨区域,则通过Hash锁定及群签名的方式实现多区域间不同卫星对于用户认证结果的共识.以下将分别详细介绍区域内及跨区域合作认证协议.以图3中区域划分方式为例,在一给定划分区域A_i内,多颗卫星间存在安全通信链路,且同步维持一个占用存储空间很小的DHT,其结构如图5所示.图5中所示DHT为区域A_i内所维持的整个DHT内容,在不同卫星处,只可以查询到存储在本卫星处的数据条目.区域内维护的DHT可以看作是当前区域的一个认证共识账本,当用户通过正常的方式接入认证后,用户所接入卫星即会立刻存储以此用户全局唯一的ID为Hash索引的数据条目,每条数据条目中都包含用户的token、用户认证成功后卫星给其分配的会话密钥以及此数据条目存储在当前区域内的哪些卫星中.用户的token包含用户的权限、用户ID、权限有效期等信息,且由NCC使用群签名算法签名.

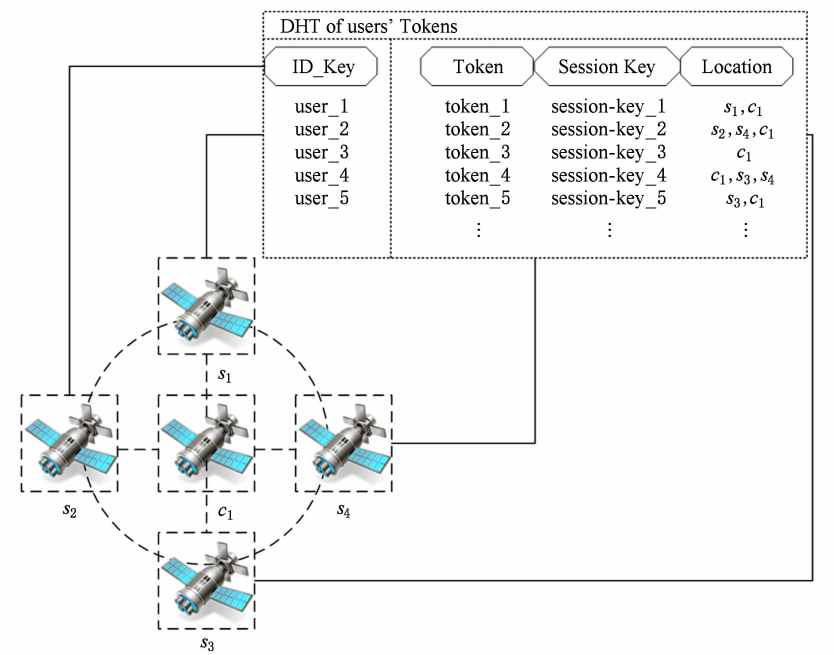

Fig. 5 Structure of DHT maintained by satellites in a same area

图5 区域内卫星共同维护的DHT组成结构

图6中的实线为安全信道,虚线为开放信道.当用户在同卫星通信时因用户与卫星间的相对移动导致链路需要切换时,用户同切换前与切换后的卫星进行6个步骤:

1) 用户通过卫星信号强弱或其他规则选取下一切换后的卫星,同时向当前连接的卫星发送切换信号,以及欲切换后的卫星ID.

2) 当前的卫星根据本地DHT查询用户欲切换的卫星是否存有此用户的token及当前会话密钥,如果有,则只发送截止时间戳,此时间戳用来表明一个时刻,当超过该时刻时,用户不可以通过切换认证的方式继续使用卫星通信服务.如果没有,则连同此用户完整的数据条目和截止时间戳一同发送给此用户欲切换的卫星.

3) 用户在通知当前卫星其将会切换链路后,生成随机数 w,然后发送自身 ID 及 w 至欲切换的卫星处,请求切换.

4) 切换后的卫星在收到用户的请求后,判断是否超时,如果未超时,则比对用户 ID,通过 DHT 或切换前卫星发送来的完整数据条目,获取对应会话密钥,并生成随机数 r,随后利用会话密钥加密返回 r 及 $w+1$.

5) 当用户收到此消息后,此用户利用自身与切换前的会话密钥解密此消息并验证 w 的正确性,随后将解密获得的随机数 r 加一,并利用此会话密钥加密返回.

6) 当切换后的卫星利用会话密钥解密得到正确的 $r+1$ 时,代表此用户是经过区域内其他卫星认证成功切换而来的,因而达成共识,以此会话密钥继续安全地提供服务.

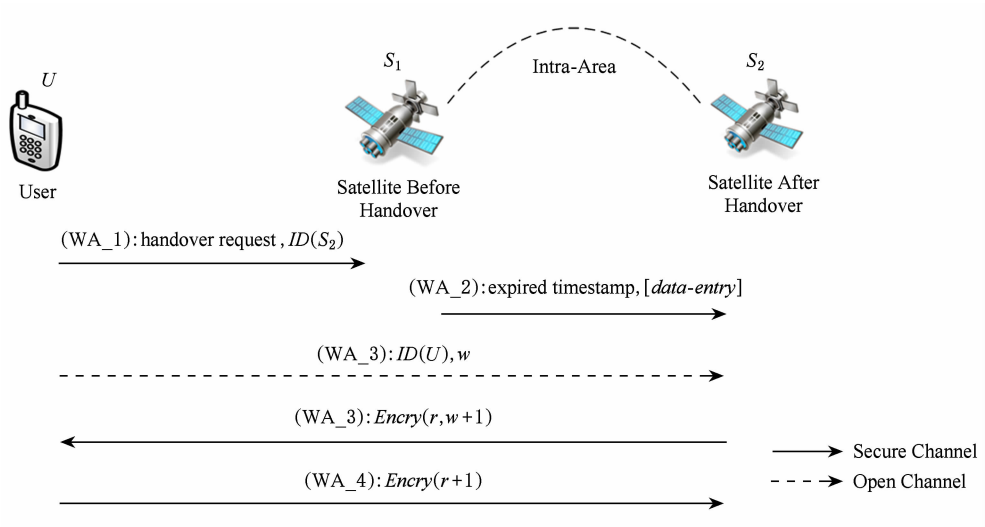

Fig. 6 Principles of intra-area handover authentication

图 6 区域内切换认证协议原理

区域内的共识认证核心思想是通过 DHT 的方式,信赖区域内其他卫星对用户的认证结果.用户只有在某一卫星处认证成功时,方能获取到正确的会话密钥,因而在切换后,通过挑战应答的方式,如果用户在截止时间戳之前可以有效准确地解密随机数,则代表是由区域内其他卫星处成功认证过的用户.此种方式要求区域内星间链路需要是安全信道.截止时间戳可以按照切换可以忍受的最长时间来设置,同时,在共识认证成功后,切换后的卫星会通过用户 token 内记录的用户权限,利用原先的会话密钥继续提供安全通信服务.此外,在每一次用户通过正常的方式认证接入后,此用户数据条目中的会话密钥都会在区域内相应更新.另一方面,为了切换认证的无缝通信,切换前卫星和切换后卫星之间的通信代价要尽量的低,也就是区域划分范围要足够简单,这一点已在第 2 节中分析过.

跨区域的合作认证主要依赖于 Hash 锁定及群签名的方式实现,不同区域连同 NCC 归属于一个卫星系统群组,区域内卫星拥有同一区域的群签名公私钥对.通过这种群签名的方式,任一卫星可以确认所收到的授权条目是否来自同一卫星网络系统内其他有效区域.授权条目采用 Hash 锁定的方式,而不再依赖于正常认证时所需要的 token 及用户私钥等,因而在满足安全性的前提下,认证效率大幅度上升,其原理如图 7 所示.

跨区域的合作认证主要有 6 个步骤:

1) 用户告知当前链接的卫星其准备切换,以及欲切换的卫星 ID.

2) 当前卫星接收到此消息后,利用自己所在区域的群签名私钥签署此用户的 token,形成此用户的签名授权条目,同时此卫星生成一新 会话密钥 k,连同签名后的授权条目通过原先的安全信道返回给用户.

3) 在上一步骤完成的同时,用户切换前的卫星将截止时间戳,密钥的右部分 rk 连同密钥 k 的 Hash 值通过星间安全信道发往用户切换后的卫星.

4) 用户将其 ID,密钥的左部分 lk,签名后的授权条目以及自身生成的随机数 r 发送给切换后的卫星.

5) 用户欲切换的卫星会首先判断是否超时,接着将 lk 与自身拥有的 rk 拼接起来,并计算其 Hash 值,同切换前的卫星发来的会话密钥 k 的 Hash 值

进行比对,如果无误,则验证授权条目的签名.若签名无误,则利用拼接后的密钥返回 $r+1$ 给用户.

6) 用户验证随机数 r 的准确性,如果无误,则利用此会话密钥同切换后的卫星进行安全通信,同时切换后的卫星会通过授权条目中用户的权限信息,提供对应种类的服务.

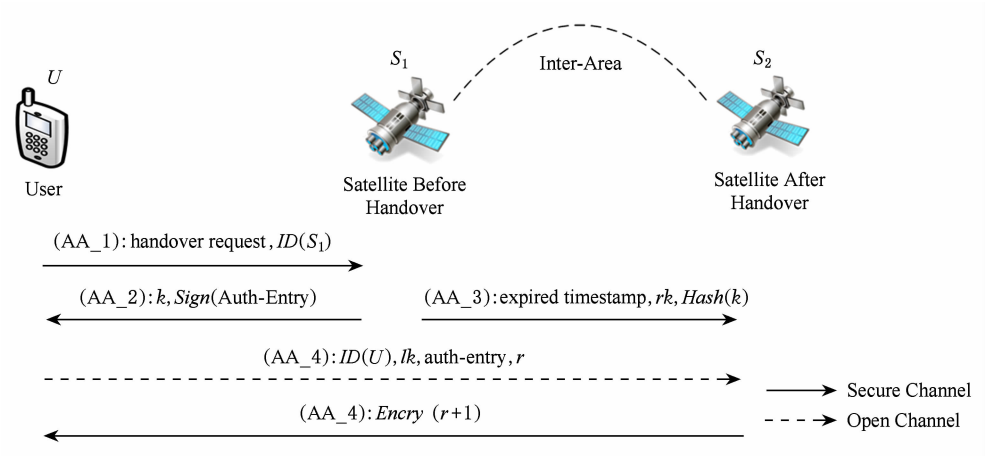

Fig. 7 Principles of cross-regional handover authentication

图 7 跨域切换认证协议原理

在所使用的群签名算法上,可以选用基于 NTRU 的群签名方案[9],一方面,NTRU 算法在存储和计算等方面更适合硬件;另一方面,NTRU 在安全性上也具备抵抗量子攻击等优势.

3.3 协议对比与分析

第 3.2 节主要介绍了协议原理,对于区域内卫星切换来说,用户的切换认证依赖于用户数据条目在区域内的同步,从而可以凭借切换前的会话密钥作为共识,在快速切换后继续享有原本的服务.对于跨区域卫星切换来说,用户在与切换前的卫星协商新密钥后,通过 Hash 锁定和随机数的方式完成用户和切换后卫星的双向验证,同时基于群签名算法,使得切换后的卫星向用户提供可靠准确的通信服务.

本协议的通信及存储开销已在第 2 节中进行了分析,在计算开销上,本协议也明显低于同类的其他协议,表 1 比对了本协议与其他卫星网络中常见协议的计算开销.表 1 中 Proposed-WA 代表区域内认证,Proposed-AA 代表跨域认证,表内 x/y 代表不同的协议在用户与 NCC 两端的计算开销,$x/y/z$ 代表本文所提协议在用户,切换前卫星和切换后卫星处的计算开销,小括号()代表离线计算或由其他认证中心进行的计算操作.

Table 1 Comparison of Computation Overhead

表 1 本协议与其他相关协议的计算开销对比

Reference	Hash Operation	MAC Operation	Symmetric Encryption/ Decryption	Asymmetric Encryption/ Decryption
Ref [10]	1/3	1/1	1/1	(0/3)
Ref [11]	1/4	2/2		
Ref [12]	3/4			
Ref [13]	5/5			
Proposed-WA			1/0/1	
Proposed-AA	0/1/1			0/1/1

由表 1 可以看出本认证协议在计算上的高效性,同时在安全性上,本协议也具备了抵抗常见攻击的能力,主要有以下 5 种:

1) 拒绝服务攻击.对于区域内切换认证来说,当有一攻击者尝试通过不断发出切换请求来进行拒绝服务攻击时,因其所指定的欲切换卫星根本不会收到来自切换前卫星的截止时间戳等信息,所以切换后卫星根本不会理会此类无意义的请求,更不会分配相关资源来做响应.对于已经正常认证通过的用户,如果其恶意发送假的用户 ID,来发动拒绝服务攻击,其会因为无法获得用户 ID 对应的正确会话密钥而使得攻击持续时间不会超过截止时间戳,

欲切换的卫星也不会对其进行应答,因而影响十分有限.同时,如果该用户利用自身正确的 ID 去发动拒绝服务攻击,卫星也可以根据请求的频次和用户 ID 对其进行拒绝,甚至是加入到黑名单中,同时此种攻击有效时间也不会超过截止时间戳.对于跨域切换认证来说,原理类似,用户必须正常认证之后,才有可能发起切换,同时切换具备时间限制,以及用户 ID 需要正确,否则无法进行拒绝服务攻击.因而本协议可以抵抗拒绝服务攻击.

2) 重放攻击.无论是区域内切换认证还是跨域切换认证,都通过基于随机数的挑战应答方式来完成对特定条件的共识,一旦攻击者将截获的某一消息进行重放,都会因为随机数的不正确而验证不通过.因而本协议可以抵抗重放攻击.

3) 中间人攻击.对于区域内切换认证而言,攻击者伪装成中间人将用户的切换请求转发给欲切换的卫星,但此攻击者会因为没有正确的会话密钥,而无法获取正确的随机数,因而在最后一步也就无法通过欲切换卫星的检测.对于跨域切换认证而言,其只能获得密钥的左部分,为了安全,通常左部分长度可以在保证密钥空间足够大的情况下充分的长,因而攻击者无法获得正确的会话密钥,自然也就无法通过接下来的验证.因而本协议可以抵抗中间人攻击.

4) 假冒攻击.本文所提出的协议分别基于 DHT 以及基于群签名和 Hash 锁定判断用户和欲切换的卫星是否都拥有正确的密钥.在认证的过程中,用户和卫星通过双向发送随机数的方式对彼此进行挑战应答验证.在跨域时,用户欲切换的卫星通过 Hash 锁定的方式可以快速认证此用户是否为拥有正确会话密钥的用户,用户也可以根据欲切换的卫星返回回来的加密的随机数判断此卫星是否是有效的.因而本协议可以在用户及卫星间进行双向认证,即可以抵抗假冒攻击.

5) 其他类型攻击.常见的如智能卡丢失攻击、验证表丢失攻击等,因本协议未包含智能卡或验证表,自然也就不会受到此类攻击.

4 实验与结果

在本节中,我们使用 OPNET 构建类铱星星座 LEO 卫星网络场景,同时在其中仿真本协议的性能.

4.1 仿真参数

在 OPNET 中,我们通过支持应用属性的卫星节点构建类铱星网络拓扑,同时每个轨道上不备有后备卫星.仿真的卫星网络参数为,高度:780 km,倾角:86.4°,轨道周期:6 027.14 s,11 个轨道,每个轨道上 6 颗卫星.OPNET 中搭建的网络场景如图 8 所示:

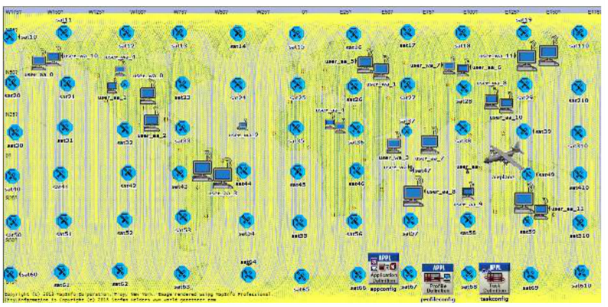

Fig. 8 Topology structure of OPNET simulation network

图 8 OPNET 仿真网络拓扑结构图

用户完整数据条目采用的冗余策略为区域内全部冗余,以此来考察协议的最坏存储消耗情况.同时,在共识认证协议的实现上,Hash 算法采用 SHA-256 算法,用户同卫星以及卫星与卫星间的安全信道采用 AES-256-CTR 算法,群签名算法采用基于 NTRUSign-251 的群签名方案,其安全性相当于 RSA1024 的安全性.在 OPNET 中构建 LEO 卫星网络场景时,用户节点采用 wlan_workstation_advanced 高级节点,同时依据用户与卫星间的相对运动以及区域内和跨域认证发生条件,设置用户节点为固定不动的 wlan 节点,以及按照某一特定运动轨迹飞行的飞行器.区域合作认证协议的阶段主要由 task_config 任务配置器来完成,主要分为 2 个阶段:区域内共识认证阶段和跨域时认证阶段.协议中包含的字段都以实际使用的算法和约定来设定,如安全信道的密钥为 256 位,Hash 计算出来的结果为 256 位等.协议中涉及相关字段大小如表 2 所示:

Table 2 Field Settings During Simulation Unit

表 2 仿真中协议字段设定

Field	Length/b	Field	Length/b
Data Entry	1 479	Random num	32
Auth Type	8	Separator	16
ID	240	Token	823
Expired Timestamp	120	Auth Entry	1 086

4.2 仿真结果与分析

首先,本协议在区域划分上所导致存储及通信开销是极低的,以铱星系统最顶峰时期的用户量来说(150 000)来说,所有用户在星端占据的总空间为 211 MB 左右,假定用户分布均匀的话,平均每个轨道

上的卫星只会消耗 35 MB 左右,因而其带来的存储开销是极低的.在区域内,通过 DHT 方式实现的用户数据条目的同步,耗费的通信代价也因区域的足够小而局限于几次的轨间通信与轨内通信.

在验证本文所提认证协议的性能上,我们通过 OPNET 中的 Profile 配置、Application 配置及 Task 配置对象设置用户同星端的定制流量交互.仿真实验设定为运行 4 h,在 4 h 内,假定用户发生切换认证符合泊松分布,且仿真时依次考量 1 h 内平均发生切换认证次数 λ 为 10,100,1 000 的 3 种量级.区域内(WithinArea, WA)及跨域(AcrossArea, AA)认证的发生服从 0-1 分布.仿真结果如表 3 所示:

Table 3 Simulation Results of WA and AA Handover Authentication

表 3 区域内与跨域切换认证仿真结果 s

Phase	10 users/1 h	100 users/1 h	1 000 users/1 h
AA_1	0.125 754	0.089 007	0.084 679
AA_2	0.158 635	0.193 636	0.239 346
AA_3	0.196 389	0.190 625	0.192 31
AA_4	0.264 804	0.264 827	0.235 964
WA_1	0.126 02	0.108 65	0.108 988
WA_2	0.298 714	0.269 167	0.313 929
WA_3	0.187 787	0.188 324	0.185 655
WA_4	0.201	0.227 647	0.168 32
AA_response	0.549 194	0.547 47	0.559 989
WA_response	0.533 807	0.436 973	0.422 917
AA_delay	0.073 121	0.059 143	0.074 408
WA_delay	0.095 631	0.075 816	0.074 89

从表 3 中可以看出,区域内认证平均响应时间在 465 ms 左右,而跨域认证的平均响应时间在 552 ms 左右,相比于文献[4]与文献[14]的 500 ms 级别,有小幅的优势.同时跨域相对于区域内的响应时间会稍高一些,这主要是因为跨域认证过程中往往会涉及到轨间的通信.此外,AA1-4 及 WA1-4 分别代表着跨域以及区域内切换认证中的每一子步骤,AA2-3 为并行的阶段,相应的响应时间可以看出在用户规模变化时没有明显的影响,所以本协议足够高效稳定且不会影响到卫星网络的服务质量(QoS).从切换认证的角度讲,如果以用户向切换卫星发起切换请求作为切换认证的起始点(即对于用户切换来说,在向切换卫星发起的切换请求之前所发生的通信都相当于准备工作),则本协议的区域内认证响应时间在 300 ms~400 ms 的级别,跨域认证响应时间在 200 ms~300 ms 的级别.

同时,分析可得,本文所提认证协议,对于原有正常卫星认证协议,只需要有记录用户权限相关的 token 即可,因而也具备高可扩展性.另一方面,如果采用本协议的 LEO 卫星网络轨道数与卫星数目足够多,那么对于每一颗卫星来说其付出的代价越低,且本文所提出的认证协议的性能也会因为星间的轨内与轨间通信延时进一步的降低而获得更高的性能.综上,可以得出本文所提出的区域合作共识认证协议依赖于区域内与区域间的共识,具备高效、稳定、可扩展与安全等特点.

6 总 结

本文提出了一种基于区块链共识思想的区域合作认证协议,包括区域内与区域间 2 种切换协议.区域内利用 DHT 的方式,通过较低的存储与通信代价使得用户可以在区域内卫星处快速的进行切换,区域间的跨域切换则利用卫星与 NCC 组成的群签名群组,同时结合 Hash 锁定的方式,完成跨域情况下用户在星间的快速切换.最后通过理论与仿真结果表明,本文提出的基于区块链共识思想的区域合作认证协议在保证安全性的前提下,性能方面优于许多已有的卫星认证协议,同时兼具可扩展、高效与稳定性.

参 考 文 献

[1] Cruickshank H S. A security system for satellite networks [C] //Proc of the 5th Int Conf on Satellite Systems for Mobile Communications and Navigation. London: IET, 1996: 187-190

[2] Hwang M S, Yang Chaochen, Shiu C Y. An authentication scheme for mobile satellite communication systems [J]. ACM Sigops Operating Systems Review, 2003, 37(4): 42-47

[3] Chang Yafen, Chang Chinchen. An efficient authentication protocol for mobile satellite communication systems [J]. ACM Sigops Operating Systems Review, 2005, 39(1): 70-84

[4] Zheng Guibin, Ma H T, Cheng C, et al. Design and logical analysis on the access authentication scheme for satellite mobile communication networks [J]. Iet Information Security, 2012, 6(1): 6-13

[5] Wu Xinghua, Zhang Aixin, Li Jianhua, et al. A lightweight authentication and key agreement scheme for mobile satellite communication systems [C] //Proc of the Int Conf on Information Security and Cryptology. Berlin: Springer, 2016: 187-204

[6] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: A distributed operating system for permissioned blockchains [C] //Proc of the 13th EuroSys Conf. New York: ACM, 2018: 1-15

[7] Yuan Yong, Wang Feiyue. Development and prospect of blockchain technology [J]. Journal of Acta Automatica Sinica, 2016, 42(4): 481-494 (in chinese)
(袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494)

[8] Zhu Liehuang, Gao Feng, Shen Meng, et al. Review of researches on privacy protection of blockchain [J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186 (in chinese)
(祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186)

[9] Wang Xiang. A group signature scheme based on NTRUSign [J]. Journal of Computer Engineering and Application, 2010, 46(34): 99-101 (in Chinese)
(汪翔. 基于 NTRUSign 的群签名方案[J]. 计算机工程与应用, 2010, 46(34): 99-101)

[10] Chen T H, Lee W B, Chen H B. A self-verification authentication mechanism for mobile satellite communication systems. [J]. Computers & Electrical Engineering, 2009, 35(1): 41-48

[11] Yoon E J, Yoo K Y, Hong J W, et al. An efficient and secure anonymous authentication scheme for mobile satellite communication systems [J]. Eurasip Journal on Wireless Communications & Networking, 2011, 2011(1): 86-95

[12] Chang C, Cheng T, Wu H. An authentication and key agreement protocol for satellite communications [J]. International Journal of Communication Systems, 2015, 27(10): 1994-2006

[13] Zhang Yuanyuan, Chen Jianhua, Huang Baojun. An improved authentication scheme for mobile satellite communication systems [J]. International Journal of Satellite Communications & Networking, 2015, 33(2): 135-146

[14] Zhang Xiaoliang, Liu Heyu, Lu Yong, et al. A Novel End-to-End Authentication Protocol for Satellite Mobile Communication Networks [M] //Foundations and Applications of Intelligent Systems. Berlin: Springer, 2014: 755-766

Wei Songjie, born in 1977. PhD. Associate professor. His main research interests include information security and intelligent computing.

Li Shuai, born in 1994. Master candidate. His main research interests include cryptography, blockchain and network security.

Mo Bing, born in 1981. PhD. Associate professor. His main research interests include Internet of things, integrated circuits and blockchain (mobing@njust.edu.cn).

Wang Jiahe, born in 1994. Master candidate. His main research interests include network security, network traffic confusion and satellite network (jhwang@njust.edu.cn).