基于区块链的无线 Mesh 网络安全认证研究

李俊涛

（中共青海省委党校，青海西宁 810001）

【摘要】无线 Mesh 网络作为无线通信的一个重要分支，越来越受到人们的重视，它的自组织性、自愈性、多跳性和分布性等特点不仅是其受到关注的原因，也导致了一些常见的安全风险。利用区块链技术中的密码学技术和智能合约技术，可以有效地消除网络认证过程中的单点依赖和位置依赖，使得无线 Mesh 网络更加安全、高效、简洁，对今后无线 Mesh 网络的研究和应用也有一定的借鉴意义。

【关键词】无线 Mesh 网络；区块链；智能合约
【doi:10.3969/j.issn.2095-7661.2021.02.007】
【中图分类号】TN929.5　　【文献标识码】A　　【文章编号】2095-7661(2021)02-0026-03

Research on Security Authentication of Wireless Mesh Network Based on Blockchain

LI Jun-tao
(Party School of Qinghai Provincial Committee of CPC, Xining, Qinghai, China 810001)

Abstract: As an important branch of wireless communication, wireless mesh network attracts more and more attention. Its self-organization, self-healing, multi hop and distributed characteristics are not only the reason for its attention, but also for its security risks. Using cryptography technology and intelligent contract technology in blockchain technology can effectively eliminate the single point dependence and location dependence in the process of network authentication, and make wireless mesh network more secure, efficient and concise. It has certain reference significance for the future research and application of wireless mesh network.

Keywords: wireless mesh network; blockchain; smart contract

随着移动网络的不断发展，人们可以在移动的状态下进行网络办公、生活等。无线 Mesh 网络作为一种新的无线通信技术，近年来越来越受到人们的关注，它是一种高互联、高容量、高可靠性、高灵活性的分布式网络，这些特点是优势的同时，也带来了一定的安全隐患。为此本文在无线 Mesh 网络的认证过程中，加入了区块链的相关技术，来增强它的安全性。

1 区块链技术

区块链技术是由密码学、智能合约、分布式数据链式存储等组合而成的一种新技术合集[1]，它为数据的交换和存储提供了高效、安全的保证。区块链网中整个节点的分布是对等的，它只要半数以上的节点达成共识，便可以创建一个有效的数字签名来完成认证。

1.1 区块链的基本架构

一般区块链由 5 层组成，各层之间相互独立又不可分割，如图 1 所示。

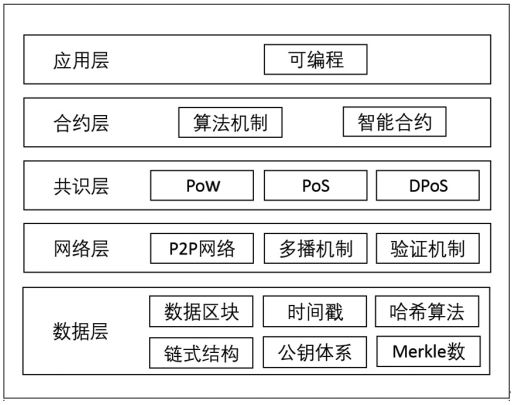

图 1　区块链技术结构图

1）数据层，是一种链式结构，表现形式为“链表 +

[收稿日期] 2021-01-20

[作者简介] 李俊涛(1982-)，男，河南淅川县人，中共青海省委党校高级工程师，本科，研究方向：网络信息安全。

区块”。主要由数据区块、非对称加密算法、时间戳、哈希运算、链式结构等组成,用于数据的不可篡改和不断增长。

2)网络层,是一种点对点的对等式分布结构,即去中心化的网络模式。在该网络中每个节点无需通过中心节点进行通信[2]。当网络中有认证行为时,认证信息会被作为候选区块随机广播到全网各个节点上,当同意节点超过半数时,该候选区块就会增加到共同维护的区块链上,实现数据的分布式管理。

3)共识层,其目的是使各个节点之间能对某一项提案达成共识,缩短交易时间。该层封装了区块链创建信用技术的各类共识算法,如 PoW、PoS、Raft 等。

4)合约层,是区块链实现自由编程的基础,包含各类算法机制和智能合约等。用户可以根据需求自定义编程,自动灵活地实现相应功能。

5)应用层,主要为用户提供多种场景和案例应用的接口,服务对象可以是 Web 端、移动端等。

1.2 区块链的分类

根据数据使用权限的不同可以分为:

1)公有链,数据完全公开,结构完全去中心化,没有加密、审计等访问控制手段,任何用户都可以使用并维护区块链。如比特币网络和以太坊网络。

2)私有链,具有一定的中心化,只允许用户自己和部分组织机构使用,并且在数据访问时需具备相应的权限。如内部审计。

3)联盟链,介于上述两者之间,网络结构可以认为是多中心化的,数据访问必须经过授权,由若干个组织或机构共同协商使用和维护[3]。普通用户只能参与交易过程, 验证和记账则由共识机制来完成。如 R3、超级账本等。

与集中式数据库相比,私有链具有可追溯性和不可篡改的特点,成本更低,效率更高,同时保护了相关的隐私,为此本文将采用这种方式。

2 无线 Mesh 网络

无线 Mesh 网络是在 802.11a/b/g 的标准上结合 Ad-hoc 网络优势发展而来的一种新型网络[4],其核心优势在于: 网络中各节点之间进行数据包交换时,采用无线多跳来实现与相邻节点之间的通讯[5],以此来增强网络的覆盖能力。传统无线网络中,终端设备的网络服务必须链接 AP,而在无线 Mesh 网络中终端设备除了连接 AP,自身还可以作为路由和 AP 使用。

2.1 无线 Mesh 网络的组成及结构

无线 Mesh 网络主要是由:终端、路由器和网关三种类型的节点组成[6]。首先将路由器节点作为关键点组成网络的骨架;其次将终端节点分布到路由器节点的底层,用于网络的扩展和交互;最后整体网络通过网关节点连接因特网。在实际的应用中,根据网络需求的不同,网络中的节点类型也有所变化,这三种类型的节点不一一包含在内。按无线 Mesh 网络的使用方式其结构可分为:

1)平面式,是一个点对点对等的分布式网络,由具备路由和转发功能的终端节点组成,节点具有相同的路由协议,可以直接通信,并且可以随时加入或退出网络,具有较高的灵活性。

2)多级式,是一种总分结构的网络,由 Mesh 路由器组成骨干总网络,具备收发功能的终端设备组成分层网络。网络结构中,分层节点之间不能直接通信,需由上层路由器作为桥梁。

3)混合式,由平面式和多级式结合而成,包含了二者的优势。同层节点可以直接通信,还可以通过路由器与它层节点通信,并可以作为中间节点实现通讯路径的选择和数据传输。

2.2 无线 Mesh 网络存在的问题

由于无线 Mesh 网络采用了中间节点转发的方式实现数据交换,如果没有合理的安全认证方式,会导致较大的安全隐患,主要安全隐患如下:

1)由于它是一个分布式的、对等的、去中心化的网络,这就意味着其决策的分散性,为不法攻击者提供了便利。

2)该网络的数据传输采用了开放的无线通道,在同一个无线覆盖范围内,不同频段的网络之间必定会产生干扰。当进行无线多跳中间节点传输时,就有可能遭受中间人攻击。

3)在该网络结构中,当发生节点的加入或退出时,网络拓扑图就发生了变化,相关节点将会自动更新路由表信息,在这个过程中,如果非法节点发送了错误的路由表信息, 就有可能占用大量的网络资源,影响整个网络的可用性。

3 基于区块链的无线 Mesh 认证方案

无线 Mesh 网络在接入过程中面临的威胁有:消息的截获、篡改、重放等。拒绝服务可以造成网络的瘫痪,非法访问可以造成信息资源的泄露。为了防范这些攻击手段,本文结合密码学与智能合约技术相关理论,提出了一种基于区块链的无线 Mesh 网络身份认证体系,确保网络通讯更高效、更安全、更可靠。

3.1 设计体系结构

其体系结构如图 2 所示。首先申请者发出实时认证请求,认证系统收到请求后,使用哈希算法加密技术对其身份信息进行加密处理,IPC 通知区块链核心模块进行验证。核心模块内,已授权用户会对新申请的用户信息进行安全认证, 如果通过则使用 ioctrl 函数调用 Wi-Fi 模块来实现网络的接入,如果不通过则

拒绝访问。

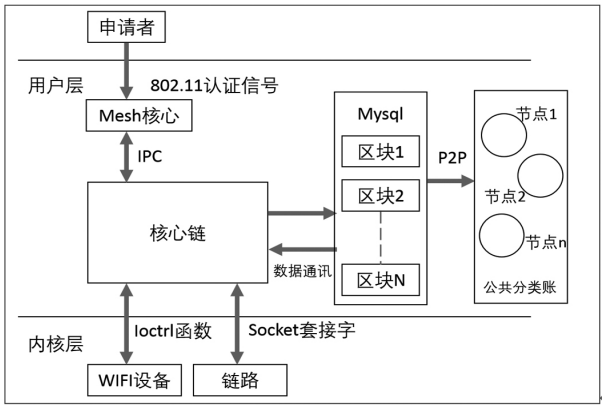

图 2 基于区块链的 Mesh 架构设计图

每个新接入的用户信息，都会被记录在账本中，并由所有节点共同来维护，一旦发现有可疑用户进入，便可发起安全认证和共识，将非法用户踢出网络。

3.2 MSA 认证

无线 Mesh 网络接入认证协议主要是 MSA 认证方法，它可以限制未授权的用户直接访问，并确保数据在 Mesh 网络中的快速和安全传输。在 MSA 认证方案中，首先定义了 Mesh 密钥分发者 MKD 和认证者 MA，并将两者合称为密码持有者 MKH。MSA 密钥体系结构分为链路安全和密匙分发两部分。在链路安全部分，申请者 MP 和认证系统 AS 成功认证后生成 MSK，PSK 是它们的预共享密钥，每个不同的申请者通过 MSK 生成不同的 PMK-MKD，并存储在 MKD 上，同样对应生成的 PMK-MA 将存储在 MA 上；在密钥分发部分，MKD 使用 MSK 生成 KDK，此时需要使用 MA 的 MAC 地址，通过 KDK 生成 PTK-KD，并生成随机数。

MSA 定义了四种安全通信协议来确保密钥持有者的通信安全。一是安全握手协议，用于 MA 和 MKD 直接建立安全链路；二是 EAP 消息传输协议，用于 MA 和 MKD 直接传输 EAP 消息；三是密钥传输协议，用于 Mesh 密钥体系中分发和管理密钥；四是安全拆解协议，用于 MA 和不同 MKD 之间改变所属关系的交互协议。

3.3 基于区块链的认证过程

认证过程如图 3 所示，首先申请者将认证申请发送给 AP 进行审批，AP 验证客户端证书能否在本地进行审批，如果可以，AP 将执行身份验证。如果不能申请者就会提交预共享秘钥 PSK 给认证者 AP 进行审批，并通过 4 次握手获得 PMK，最终自动获取到 IP 地址并接入到网络。

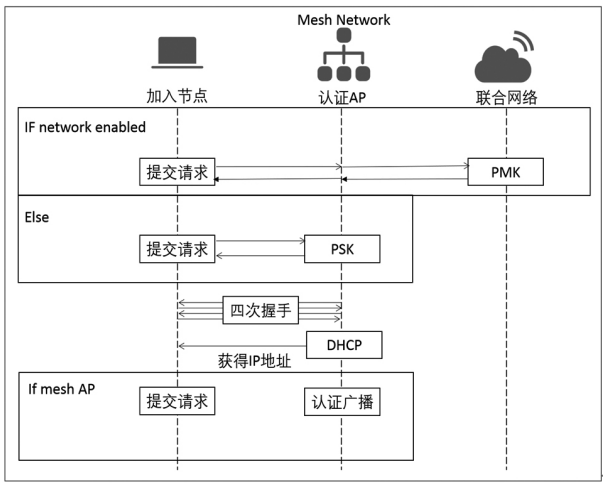

图 3 基于区块链的认证过程图

认证过程中，用户的信息是作为公钥使用，因此不需要存储和签署。这样系统网络配置相对简单，认证过程不需要证书，系统运维成本也相对较低，运行效率自然提高。认证过程中消息传递的具体描述如下：

第一步系统初始化，成功认证的用户信息将被单独封装，并通过时间戳进行戳记生成单独区块，将这些区块按时间顺序从一端连接到另一端形成区块链。

第二步生成临时公钥，申请者 A 将其公钥 PubA、身份 IDA 和数字签名 SignA 发送给认证系统 S，在收到相关请求后，系统提取摘要并生成随机数 Ns。在生成随机数的基础上结合 DH 秘钥交换算法，生成临时公钥 aPubs。

第三步生成共享密钥，将认证系统临时节点上的公钥 cPubs 和第 2 步生成的临时公钥 aPubs 通过密钥函数计算，得出认证者和系统的共享密钥 MSK，单播会话密钥 UMK，并计算出系统的消息签名 M1。

$$MAK=H_{KD}(acPub_m, n_s)$$

$$UMK=H_{KD}(SAPub, Ns \mid Na)$$

$$M1=\{IDs\}_{MSK} \mid ID_A \mid ID_s \mid N_s \mid N_a \mid Pub_A \mid Pub_S$$

第四步身份验证，系统通过扩展消息认证密钥 MAK，生成消息认证码 MACA，并对申请者的消息进行验证。如果成功，则生成散列认证码。

$$Signs=Signs(H_2(Pub_S \mid Pub_A))$$

$$HashA=SHA-1(MAK, M2 \mid Sign_A \mid Sing_S)$$

最后将申请者的身份验证状态改为成功，并通过 P2P 技术将哈希码和其他信息发送到整个区块链中，至此整个消息传递过程完成。

3.4 智能合约

本文设计的认证系统，各个节点都是利用 P2P 连接服务器，进行节点之间的消息队列循环和数据传输，实现智能合约的自动执行和自我验证。具体的智能合约交易流程包含：连接交易，是指当合法的用户在通过验证后，设备信息、网络信息、（下转第 70 页）

表 1 （续）

知识内容	思政元素及融入点	预期成效
模块 7 液、气、电控制应用	观察，思考，推理	比较液、气、电控制的异同点，找到事物的规律；锻炼学生观察能力，能在事物中找到规律
模块 8 PLC 通信与网络应用	团队意识，资料查阅，创新精神	通过网络的搭建，培养学生收集分析资料的能力、集体配合的能力，思考不同的控制方案，激发创新意识
模块 9 触摸屏和变频器综合应用	工匠精神，团队协作，诚信	通过集体协作分工完成较复杂的应用设计任务，锻炼学生做事的各项能力，同时教育学生诚信做事

3.2 专业课课程思政实施情况

本研究自 2018 年起至今，在可编程控制器应用技术课程中进行课程思政育人的探索，涉及机电一体化专业的 200 多学生。课程结合知识目标和育人目标重新制定了课程标准，进行教学设计。通过项目式教学、演示教学、案例分析、讨论协作和分组学习等多种教学手段在专业知识技能教学的同时融入思政教育。改革课程的考核体系，将学习过程考核、综合能力考核、职业素养考核等思政元素纳入到课程考核体系中，在考察学生专业知识技能掌握情况的同时考查课程思政的育人效果。通过教师自我总结、互相听评课、学生问卷测评等多种途径评价教学过程，促进可编程控制器应用技术课程中思政元素的有机融合。通过以上措施，该课程的学生学习主动性积极性明显提高，相关的职业资格考证通过率明显提高，取得了良好的育人效果。

4 结语

总之，将专业课课程思政有规划、有设计地融入到专业课的教学过程中，使学生潜移默化地受到影响，是实现全程、全方位协同育人的有效途径，也是思想政治教育的有利补充，同时，也促进了专业课程教学质量的提升。可编程控制器应用技术课程在教学过程中有机地融入思政元素，不仅提高了教学质量，还提高了学生的道德素养和综合素质，取得良好的育人效果，对其他专业课程的思政教学展开有一定的借鉴意义。

【参考文献】

[1]教育部新闻办.教育部长陈宝生在 2021 年全国教育工作会议上的讲话[EB/OL].https://mp.weixin.qq.com/s/Xb_WnrvxPyeJMrL39CV5tg,2021-2-04.

[2]罗佳琪.高职院校理工科专业课课程思政有效路径研究[J].湖南邮电职业技术学报,2021(1):82-85.

[3]包立远.新形势下高职院校营销专业课程思政化路径探索研究[J].湖北函授大学学报期刊,2018(12):135-136.

[4]岳洪江.财经院校课程思政推进状况及建设策略[J].高等学刊期刊,2020(3):49-51.

[5]牟芳芳,国海东,郭春霞,邵水金,张黎声.医学专业课程思政工作中教学目标设置与实施的探索[J].中医教育,2019(11):63-66.

[6]叶莲.课程思政与素养教育同向同行的内在逻辑及实践路径[J].大学教育,2020(2):121-123.

（上接第 28 页）

接入认证等交易信息就会存储到区块链的账本中；离开交易，是指用户超过了网络覆盖范围或者主动离开了网络后，联网或中断时长等交易信息就会被存储到区块链的账本中；更新交易，是指合法用户重新连接网络会被视为一次交易；断网交易，当某个节点的网络断开时，另外的节点就会自动连接网络，以确保整个网络的持续联网，这种情况下的交易称为断网交易。

将上述交易过程的协议内容部署在智能合约中，在不影响其安全的前提下，能够使整个区块链节点的连接变得更加高效和简洁。

4 结语

为规避安全风险，提出将区块链技术应用到无线 Mesh 网络的认证中，利用密码学技术和智能合约技术，消除了认证过程的单点依赖和位置的依赖，使认证过程更加安全和高效。随着技术的不断进步，相信无线 Mesh 网络的应用也会越来越广泛。

【参考文献】

[1]成诺.基于区块链的无中心网络身份认证技术的研究与实现[D].西安：西安电子科技大学,2018.

[2]王崇宇.区块链技术与其价值展望[J].经济动态与评论,2018(2):149-164.

[3]袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016(4):481-494.

[4]张瑜.信息安全技术综述[J].电子技术与软件工程,2020(1):249-250.

[5]孙华林,盛昀瑶,苏宝莉.“区块链 + 在线教育”的现状分析与研究[J].湖南邮电职业技术学院学报,2019(2):16-18.

[6]马春光,安婧,毕伟等.区块链中的智能合约[J].信息网络安全,2018(11):8-17.