

基于区块链的轻量化移动自组网认证方案

张勖^{1,2}, 马欣³

1. 北京邮电大学网络空间安全学院, 北京 100876;
2. 移动互联网安全技术国家工程实验室, 北京 100876;
3. 北京邮电大学网络教育学院, 北京 100876

摘要: 为了解决现有认证方式无法追踪恶意节点、集中式认证中心易受攻击的问题, 基于区块链技术的去中心化、防篡改、可追溯特点, 提出了一种分布式轻量化移动自组网认证方案。该方案包括对等网络建立、认证账本设计和共识机制选择, 并分析讨论了智能合约的作用。在所提方案中, 当给定对等节点之间最大传输时延 $\tau_{\max}$ 时, 节点认证时间 δ 和网络规模 N_t^{all} 间的关系满足 $\left(\frac{N_t^{\text{all}}}{3} + 7\right)\tau_{\max} \leq \delta \leq 3(N_t^{\text{all}} + 1)\tau_{\max}$ 。

关键词: 移动自组网; 区块链; 认证; 对等网络; 账本; 共识机制

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020040

Lightweight mobile Ad Hoc network authentication scheme based on blockchain

ZHANG Xu^{1,2}, MA Xin³

1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. National Engineering Lab for Mobile Network Security, Beijing 100876, China
3. School of Network Education, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: In order to solve the problem that the existing authentication method can't track the vulnerable of malicious nodes and depends on the centralized authentication center, based on the de-centralization, tamper-proof and traceable characteristics of blockchain technology, a distributed lightweight mobile Ad Hoc network authentication scheme was proposed. It included the establishment of peer-to-peer network, the design of certification ledger and the choice of consensus mechanism. Then the role of smart contracts was analyzed and discussed. In this scenario, when the maximum transmission delay $\tau_{\max}$ between a pair of peers is given, the relationship between node authentication time δ and network size N_t^{all} is satisfied with $\left(\frac{N_t^{\text{all}}}{3} + 7\right)\tau_{\max} \leq \delta \leq 3(N_t^{\text{all}} + 1)\tau_{\max}$.

Key words: mobile Ad Hoc network, blockchain, authentication, P2P network, ledger, consensus mechanism

收稿日期: 2020-01-20; 修回日期: 2020-03-06

通信作者: 张勖, selina_zhangx@bupt.edu.cn

基金项目: 国家重点研发计划 (2018YFB1402704)

Foundation Item: The National Key R&D Program of China (2018YFB1402704)

论文引用格式: 张勖, 马欣. 基于区块链的轻量化移动自组网认证方案[J]. 网络与信息安全学报, 2020, 6(4): 14-22.

ZHANG X, MA X. Lightweight mobile Ad Hoc network authentication scheme based on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 14-22.

1 引言

移动自组网 (MANET, mobile Ad Hoc network) 从早期的军事战场环境逐步扩展至应急通信、机器通信、车联网等场景, 其应用领域日渐广泛和开放。与具有基础设施的移动通信系统不同, 移动自组网中的节点都具备参与组网的能力。在此前提下, 对节点的认证结果不仅关系到是否允许该节点接入网络并按权限规定使用网络资源, 更为重要的是对节点能否成为组网成员进行确认。为改进传统认证机制的集中式、无法追踪恶意节点的缺陷, 基于区块链的认证技术应运而生。虽然在互联网应用中已有研究人员^[1-3]将区块链技术引入认证过程, 但在 MANET 中的相关研究还在进行。

在 MANET 中, 通过应用层覆盖协议 (overlay approach), 可以增强服务传输能力。Liebeherr 等^[4]的研究表明了覆盖网络可以为自组网中的应用数据提供正向和反向保密。他们提出了一种密钥管理和加密方案“邻域密钥方法”。自组网中的每个节点与它已经认证的邻居节点共享一个密钥。当网络成员改变或网络被分区时, 邻域密钥方法能够避免代价高昂的全局密钥重置操作。通过新开发的应用层自组网路由协议, 即基于 Ad Hoc 网络的 P2P 技术, 对文中提出的数据加密方法进行了评估。在应用层覆盖网络的软件系统中, 实现了自组网路由协议和安全方案。通过使用手持无线设备进行的大量室内和室外测量实验, 评估了该方法的有效性和应用层自组网的性能。

当移动自组网的任务或系统实现目标 (如可靠性、可用性、可伸缩性和可重构性) 侧重在协作、协同方面, 当中的信任管理就颇具挑战性。Cho 等^[5]在定义和管理军用自组网的信任问题时, 考虑的内容包括复合认知、社交网络和信息网络之间的交互、严苛的资源限制 (算力、能源、带宽、时长) 和网络的动态性 (拓扑结构的变化、节点的移动性、节点失效、传播信道的条件)。他们把来源于社交网络的“社会信任”的概念和源于消息与交流网络的“服务质量”的概念结合起来, 得到复合信任度量。接着, 提供了对移动自

组网中信任管理机制发展的调研情况, 并讨论了移动自组网中被普遍接受的分类、潜在攻击、性能度量和信任度量的内容。最后, 就未来移动自组网中基于社交和复合网络的信任管理的研究领域进行讨论和说明。

以组 (group) 为中心的計算和通信的激增, 激发了对提供组访问控制机制的需求。Saxena 等^[6]对 Ad Hoc 网络中基于身份的组接入控制进行了研究。组接入控制包含组成员接纳和撤销/驱逐机制。尤其在自组网中, 如系统等和移动自组网, 安全的成员接入机制是必需的, 以便引导其他组提供安全服务。除此之外, 问题成员和恶意成员的撤销也需要安全的成员撤销机制。与集中式的组 (多播) 不同, 自组织的组在运行上呈现去中心化的特征, 这类组能够容纳动态的成员资格。这样的特性使在网络中实施接入控制变得有趣且富有挑战性。尽管在成员接纳的问题上已有一些工作取得了初步进展, 但成员资格撤销的问题尚未得到解决。他们设计了一种基于身份的组接入控制技术, 这个技术避免了以前 (基于证书的) 方法的缺陷, 还提出一种同组成员资格撤销的机制。实验结果证明, 解决方案是健壮的、完全分布式的、可扩展的, 同时具有合理的效率。

传统的互联网组网服务和技术并不总是能很容易地移植到无线自组织环境中。Winter 等^[7]介绍了专门针对移动自组织环境的对等网络, 通过引入对等覆盖网络技术, 移动自组网中许多原先呈现出性能问题的应用几乎不存在了, 或者原问题可以被完全忽略。这种方法利用邻近信息有效地生成覆盖结构, 同时可反映出基础物理层网络拓扑。此方法减少了因覆盖网络的路由查找导致的物理层路由路径长度的增长。覆盖网络的新颖性在于它不依赖于固定的节点集, 并且能够适应物理层网络拓扑的变化。覆盖网络构造过程中一个显著的特征是将通信开销缩减至最低。除此之外, 现有的对等网络保持了一套均匀分布的覆盖 ID, 这种方式曾经在有线网络的开发解决方案中被故意放弃。新的覆盖网络的基础是基于分布式哈希表的对等网络 Pastry。文献[7]发展和分析了两种不同的引导策略, 它们都被设计用于动态网

络和移动网络（如 Ad Hoc 网络）

从上述文献中可知，在移动自组网上构建对等网络已有研究成果，即具备了将区块链技术引入的网络前提条件。但是，移动自组网的动态特性和区块链技术共识过程耗时的问题都对认证方案设计构成了挑战。在移动自组网中引入基于区块链的认证机制需要解决网络动态拓扑与对等（P2P, peer to peer）网络建立间的融合问题、轻量级认证账本结构和共识机制设计，以适应移动节点资源受限的需求。本文提出的方案在上述问题上作出如下贡献。

1) 通过跨层设计，降低对等网络生成维护开销。认证账本和共识算法轻量化。由此设计的基于区块链的移动自组网认证方案能够满足安全认证需求高的应用场景。

2) 通过理论分析，在本文方案基础上，给出了认证时间和网络规模间的关系，有助于网络设计或认证方案选择。

2 方案设计

基于区块链技术的轻量化认证方案至少应包括 P2P 网络、认证账本和共识算法这 3 部分功能模块，如图 1 所示。

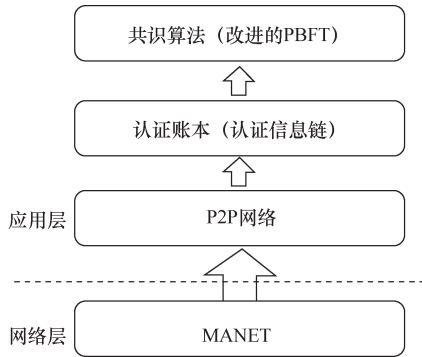


图 1 轻量化认证方案功能组成

Figure 1 Functional components of lightweight authentication scheme

2.1 跨层对等网络 P2P 生成算法

MANET 拓扑可以建模为静态有向图 $G=(V,E)$ ， V 表示节点集， E 表示边集。但对其中的源节点 S 和目的节点 D 间的通信路径来说，静态建模意义有限，原因是 MANET 路由协议无论是预设式还是反应式，每个节点都会维护从自己到目的节点的路由信息，所构成的路由表可用

$RT=\{rt_{ij}|P(rt_{ij})\}$ 表示，其中 $i \in S, j \in D$ 。

MANET 中对等网络建立的实质是每个节点能够发现并维护自己的逻辑邻居，构成 Peer 对。如上所述，由于每个节点已经通过路由协议获知与其他节点的可达路径，因此本文采用直接通过节点自身维护的路由表生成 Peer 节点对列表 $PT=\{au_{mn}|\langle au_m, au_n \rangle, m \in S, n \in D\}$ 的方法形成 P2P 网络。显然地， au 表示的是已认证的 MANET 成员节点。这样，在移动自组网中，应用层 P2P 网络的建立与网络层路由查找融合在一起，可减小协议开销。

但是，该跨层对等网络生成算法依赖于已通过认证获得入网权限的节点。而认证过程则是节点入网的必要条件，如果节点认证失败，该节点就无法成为网络成员节点，也就不能参与路由生成。为解决该问题，本文作如下定义。

定义 1 存在已认证节点集 $V_{au}=\{au_k|au_k \in V, k=0,1,2,\dots\}$ ， V_{au} 可以运行本文提出的分布式认证程序，最小集合至少包含一个节点。

以最小集合为例，MANET 的构建起始于待认证节点向最小集合中的节点发起认证请求。与传统认证方案不同的是，随着入网节点的增加，各个节点通过跨层 P2P 生成算法形成区块链认证的基础网络结构，对后续节点的入网认证则是依据分布式账本结构、共识算法达成的一致性结果为准。

2.2 轻量级认证账本设计

账本作为区块链中的核心功能，其结构设计不仅要满足特定需求，还要能够支持分布式数据存储。比特币的账本结构较以太坊和 HyperLedger Fabric 更为简略，比特币数据块（Block）结构包括 $\{\text{magic_number}, \text{block_size}, \text{block_header}, \text{transaction_cnt}, \text{transaction}\}$ ， magic_number 是区块之间的分隔符，其值为 $0xD9B4BEF9$ ； block_size 是区块大小； block_header 是区块头，其中包含版本号、上一区块的哈希值、Merkle 根节点哈希值、时间戳、难度值、随机数； transaction_cnt 是交易数量； transaction 是交易详情。以太坊账本结构中除了交易树外，还引入了状态树和收据树。Fabric 的结构与以太坊类似，但为了提升查找效率，在数据库设计上进行了改进。

本文方案应用于移动自组网，节点资源受限，因此账本需要轻量化。构建和保存认证节点的区块链结构被称为认证信息链，结构如图2所示。参考比特币账本结构，轻量化设计体现在以下3方面。

1) 仅保留与认证和追踪过程有关的必要字段。

2) 由于不采用工作量证明 (PoW, proof of work) 共识算法，相应的字段予以删除。

3) 分隔符采用重复概率低的编码方案，可用1个字节表示，提升识别速度，减少存储开销。

具体来说，认证信息链由首尾相连的区块构成，以第 N 区块为例，完整的区块包括区块头和区块体，区块头保存区块的元数据{前一区块hash，认证信息 MPT Root hash，时间戳}，相应的字节长度分别是32 B、32 B和4 B，总计68 B。区块体内容包括{分隔符，区块大小，认证详情}，长度分别是1 B、4 B和可变长度。其中，认证详情中存储{索引 index，共识结果 Proof}，共识结果中保存参与共识的节点回复消息，用于后续追踪恶意节点。

2.3 共识算法

共识是指通过消息传递使系统中所有节点均以相同顺序执行一个命令序列，即保证全网各节点数据记录一致性。在实际环境中，节点可能出错产生异常行为，或者消息无法被正确传递，也可能存在恶意节点使系统无法达成一致。由此产生的容错问题分为两类：宕机容错 (CFT, crash fault tolerant)，是指无恶意节点情况下的容错；拜占庭容错 (BFT, Byzantine fault tolerant)，即有恶意节点情况下的容错。移动自组网中虽然因无线信道和网络拓扑动态变化会引起 CFT 类问题，但本文方案主要解决安全类问题，希望通过区块链技术能够追踪恶意节点，因此共识算法采

用改进的实用拜占庭容错 PBFT 算法，称之为 MANETBFT。

PBFT 通过准备和确认两大阶段的消息同步，在节点数量较小情况下，可以实现高交易量 (TPS, transaction per second) 且分叉概率很低。将 PBFT 应用于移动自组网认证，需要解决以下问题。

1) 请求认证的节点只能利用公共信道与相邻的 P2P 网络节点通信。

2) 参与共识的 P2P 节点数量是变化的。

3) 多个节点同时请求认证的共识。

针对问题 1)，MANETBFT 在 P2P 节点中增加了认证代理身份，设发起认证请求的普通节点集 $V_{\text{req}} = \{v_i | v_i \in V, i = 0, 1, 2, \dots\}$ ， v_i 先将 REQUEST 消息发送至相邻节点之一的 P2P 节点 au_k ，该 au_k 则成为代理，在代理和其他剩余 P2P 共识节点中执行 PBFT 流程，如果 au_k 收到的 Reply 消息确认了申请节点的认证请求，则更新账本，并将 Reply 和最新的账本返回给 v_i ，节点身份变更为 V_{au} 元素。

针对问题 2)，依据 PT 表计算 N_t^{all} ，即 t 时刻的 P2P 节点总数，也就是此时刻参与 MANETBFT 共识的全部节点数。通过引入变量 N_t^{all} ，在每一轮共识过程中，PBFT 算法中代表节点数量的参数 $R = N_t^{\text{all}}$ ，以适应本场景需求。

问题 3) 多节点同时请求认证，分两种情况：一是多个普通节点在同一时刻分别发起各自的代理进行共识，这种情况 PBFT 采用<客户端 ID，时间戳，序列号>信息进行区分；二是多个普通节点申请的代理节点相同，本文以异步方式进行共识处理，并结合全网账本信息同步过程实现数据的一致性。

图3中以1个普通节点和4个P2P网络节点为例，说明MANETBFT的消息类型和处理流程。具体的消息类型如下。

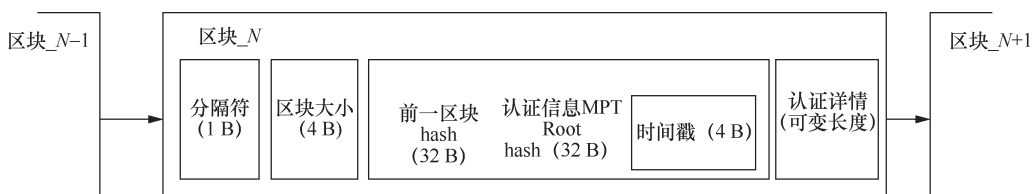


图2 轻量化认证信息链结构

Figure 2 Structure of lightweight authentication information chain

终每个 P2P 节点会把自己对本次请求的结果写入 REPLYPROXY 消息, 返回给 au_k 这个代理客户端。

4) au_k 检查收到的 REPLY, 如果有 $f+1$ 个具有不同签名且 t 和 r 都相同的回复时, 证明客户端的请求已达到全网共识。其中, f 是恶意节点数量。

5) au_k 通过映射的 REPLY 消息向 v_i 回复共识结果。

3 认证流程及性能分析

图 4 是待认证普通节点 v_i 的认证过程状态机, 图 5 是 P2P 网络节点相应的状态机。通过对两类节点状态机的分析, 完整展示本文方案。

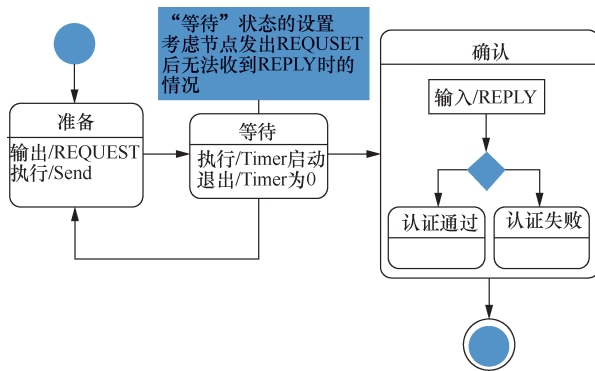


图4 普通节点认证状态机
Figure 4 State machine of ordinary node authentication

对于待认证的普通节点 v_i , 处理流程包括 {准备, 等待, 确认} 3 类状态。准备状态中节点发出 REQUEST 消息; 设置等待状态, 除了考虑异常情况外, 还出于流程和程序扩展的考量; 确认状态中输入是节点接收到的 REPLY 消息, 根据消息中携带的认证通过或认证失败确认本次认证结果并结束认证流程。

v_i 的认证需要在 P2P 节点共识基础上完成, 因此认证流程还包括如图 5 所示的运行于各个 P2P 节点的状态机。作为自组网成员节点, 图 3 中涉及的代理节点、主节点、对等节点的功能是每个 P2P 网络节点都要具备的, 结合共识消息, P2P 节点状态包括 {代理请求, 主节点, 对等节点, 共识, 回复, 代理确认}, 状态的输入不限于来自本节点上一状态的输出, 如“共识”状态的输入消息“PREPARE”, 既可以是来自本节点的“对等节点状态输出”, 也可以是其他 P2P 节点的“对等节点状态输出”。每个状态都设置了定时退回到上一状态的机制, 以避免因 MANET 拓扑变化或恶意认证导致的消息长时间等待。

在 2.3 节中提到 MANETPBFT 通过引入 N_t^{all} 解决因新加入的 P2P 节点而产生的参与共识节点总数变化的问题。在图 5 中“代理确认”状态中

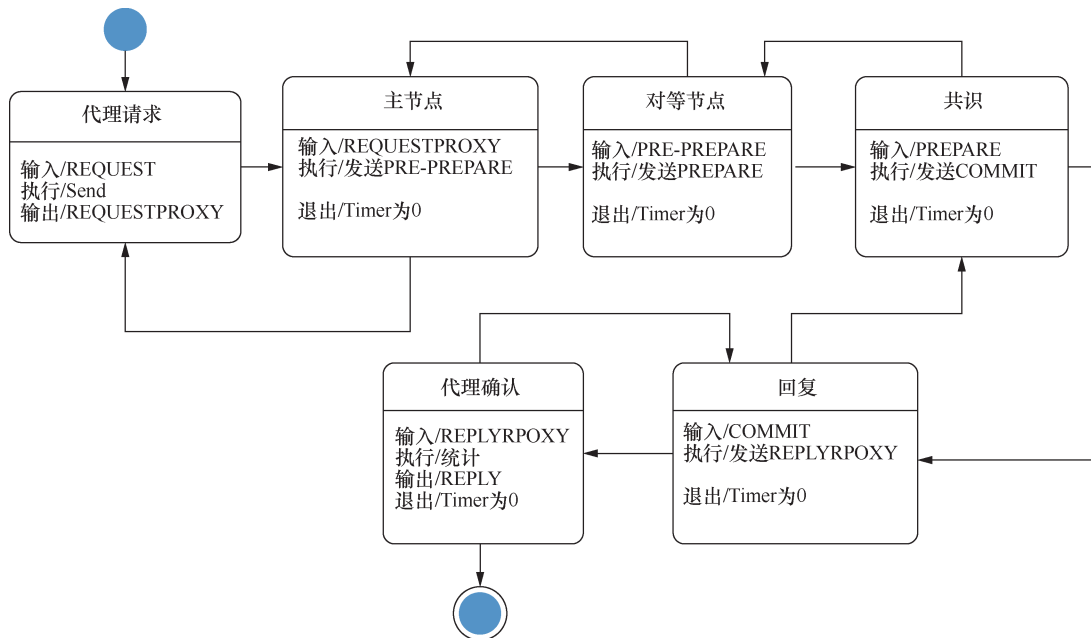


图5 P2P 网络节点状态机
Figure 5 State machine of P2P network node

的统计操作涉及该变量,代理根据收到的 $f+1$ 个具有不同签名且 t 和 r 都相同的回复 REPLYPROXY 产生对认证请求的应答,这里 f 是恶意节点数量 $f = \frac{N_t^{\text{all}}}{3}$ 。

认证结果以及相应的共识节点回复作为上链数据由代理节点写入区块链。如果 v_i 通过认证,其节点属性将变更为 au_k ,它将从代理节点处获取完整的区块链,并更新 N_t^{all} 值。P2P 节点间的账本数据一致性操作可采用周期性广播方式进行。

本文基于该认证方案,分析 MANET 规模 N_t^{all} 与认证时间 δ 间的关系。

设 $\langle v_i, \text{代理节点} \rangle$ 间 REQUEST 消息传输时延为 τ_1 , $\langle \text{代理节点}, \text{主节点} \rangle$ 间 REQUESTPROXY 消息传输时延为 τ_2 , $\langle \text{主节点}, \text{对等节点} \rangle$ 间 PRE-PREPARE 消息传输时延为 τ_3 , $\langle \text{对等节点}, \text{主节点或对等节点} \rangle$ 间 PREPARE 消息传输时延为 τ_4 , $\langle \text{对等节点}, \text{主节点或对等节点} \rangle$ 间 COMMIT 消息传输时延为 τ_5 , $\langle \text{主节点或对等节点}, \text{代理节点} \rangle$ 间 REPLYPROXY 消息传输时延为 τ_6 , $\langle \text{代理节点}, v_i \rangle$ 间 REPLY 消息传输时延为 τ_7 , 其中,每一类消息在两个相邻 P2P 节点间传输一次所需时延分别用 τ_{request} 、 $\tau_{\text{requestproxy}}$ 、 $\tau_{\text{pre-prepare}}$ 、 τ_{prepare} 、 τ_{commit} 、 $\tau_{\text{replyproxy}}$ 和 τ_{reply} 表示,根据认证流程可得

$$\begin{aligned}\tau_1 &= \tau_{\text{request}} \\ \tau_2 &= \tau_{\text{requestproxy}} \\ \tau_3 &= \tau_{\text{pre-prepare}} \\ \tau_{\text{pre-prepare}} &\leq \tau_4 \leq (N_t^{\text{all}} - 1) \tau_{\text{prepare}} \\ \tau_{\text{commit}} &\leq \tau_5 \leq N_t^{\text{all}} \tau_{\text{commit}} \\ \left(\frac{N_t^{\text{all}}}{3} + 1 \right) \tau_{\text{replyproxy}} &\leq \tau_6 \leq N_t^{\text{all}} \tau_{\text{replyproxy}} \\ \tau_7 &= \tau_{\text{reply}}\end{aligned}$$

不失一般性,设该 MANET 网络中构成的 P2P 节点对之间最大传输时延为 τ_{max} ,可推出

$$\begin{aligned}\delta &= \tau_1 + \tau_2 + \tau_3 + \tau_4 + \tau_5 + \tau_6 + \tau_7 \\ \delta &\leq \tau_{\text{max}} + \tau_{\text{max}} + \tau_{\text{max}} + (N_t^{\text{all}} - 1) \tau_{\text{max}} + \\ &N_t^{\text{all}} \tau_{\text{max}} + N_t^{\text{all}} \tau_{\text{max}} + \tau_{\text{max}}\end{aligned}\quad (1)$$

$$\begin{aligned}&\tau_{\text{max}} + \tau_{\text{max}} + \tau_{\text{max}} + \tau_{\text{max}} + \tau_{\text{max}} + \\ &\left(\frac{N_t^{\text{all}}}{3} + 1 \right) \tau_{\text{max}} + \tau_{\text{max}} \leq \delta\end{aligned}$$

即

$$\left(\frac{N_t^{\text{all}}}{3} + 7 \right) \tau_{\text{max}} \leq \delta \leq 3(N_t^{\text{all}} + 1) \tau_{\text{max}} \quad (2)$$

由于式(2)中认证时间 δ 的上下边界只是对 MANET 节点数量进行范围估计,所以此处没有进行严格的分析推导。如果考虑无线信道、链路层协议、路由协议、节点运动模型等因素,可以建模和分析出更为精准的端到端时延条件下, N_t^{all} 与 δ 间的关系。通过该结论,可以估计 MANET 规模或者评估认证时间范围,有助于网络设计或认证方案选择。

根据式(2),当对节点认证时间 δ 有指标要求,在已知 τ_{max} 时,可以估计出 MANET 节点数量的范围。例如,假设已知 $\tau_{\text{max}} = 100 \text{ ms}$, $\delta \leq 1 \text{ s}$, $N_t^{\text{all}} \in \mathbb{Z}^3$, $N_t^{\text{all}} < 9$,即假设 P2P 节点对间的最大传输时延是 100 ms,如果对节点的认证时间要求在 1 s 以内,则采用本文认证方案的 MANET 节点数量应控制在 3~9 个内。也可以在已知 τ_{max} 和节点数量的情况下,对 δ 进行估计,如 τ_{max} 仍然假设为 100 ms, N_t^{all} 取 6,则此时节点认证时间 δ 的范围是 $[0.9 \text{ s}, 2.1 \text{ s}]$ 。

本文算法的性能分析如表 1 所示,待认证普通节点向其代理节点发送单播消息 REQUEST,并等待接收 REPLY 消息。假设此时网络中有 α 个待认证节点,则此阶段通信开销为 $O(\alpha)$; P2P 节点通过 5 种消息完成请求、共识和应答,其中,共识过程采用广播方式,在 α 个待认证节点情况下,其消息复杂度达到了 $O(\alpha N_t^{\text{all}})$ 。

表 1 算法性能开销分析

Table 1 Overhead analysis of algorithm performance

复杂度	开销类型		
	通信开销	计算开销	说明
复杂度上界	$O(\alpha N_t^{\text{all}})$	$O(N_t^{\text{all}} \tau)$	α 为同时待认证节点的个数; τ 为 P2P 节点间的广播所需时长; N_t^{all} 为 MANET 节点数量

认证时间复杂度由通信所需时间和节点共识计算时间决定。设每次广播需要的时间为 $O(\tau)$ ，通信时间复杂度为 $O(N_i^{\text{all}}\tau)$ 。节点计算时间开销集中在区块查询和插入，采用 MerkleTree 的时间复杂度为 $O(\log N)$ ， N 为字符串长度。综上，认证时间复杂度的主要影响因素还是通信时间，故上界为 $O(N_i^{\text{all}}\tau)$ 。

4 系统安全模型与安全性分析

MANET 应用以军事、应急通信等需要高可信环境的场景为主。本文方案以节点硬件信息和口令作为注册身份信息，MANET 成员已预存组网的全部节点身份信息。注册节点通过加密算法（如 SM2）产生私钥 d_A 和公钥 P_A ， d_A 加密存储于本地。通过哈希算法（如 SHA-256 或 SM3）对身份信息进行哈希运算得到身份哈希值 H_{ID} 。采用签名算法对 H_{ID} 和注册时间戳 T_{Reg} 进行签名，得到注册身份签名值 SIG_{Reg} 。将消息 $\{P_A, H_{ID}, T_{\text{Reg}}, \text{SIG}_{\text{Reg}}\}$ 封装在 REQUEST 消息中发送至代理 P2P 节点。代理 P2P 节点计算用户的 H_{ID} ，通过 P_A 计算验证 SIG_{Reg} 。若验证通过，则用哈希算法（如 SHA-256 或 SM3）对 P_A 进行计算，生成区块地址，作为该节点的身份认证区块标识，在该区块体中记录用户的 $H_{ID}, T_{\text{Reg}}, \text{SIG}_{\text{Reg}}$ 。通过共识机制确认后，代理节点将该区块加入区块链中，并给待认证节点回复 REPLY。

移动自组网节点的注册过程包含首次认证，如需再次登录认证，执行过程是节点使用 d_A 对 H_{ID} 与时间戳 T_A 进行实时签名，产生动态身份签名值 SIG_{Dyn} 。节点将消息 $\{P_A, H_{ID}, T_A, \text{SIG}_{\text{Dyn}}\}$ 封装在 REQUEST 中发送给 P2P 代理节点。P2P 节点通过 T_A 判断消息时效性，使用 P_A 计算验证动态身份签名值 SIG_{Dyn} ，签名验证通过后，通过 P_A 计算区块地址，访问身份认证区块，对比消息中包含的 H_{ID} 和区块中的 H_{ID} ，计算验证 SIG_{Dyn} ，从而确定认证节点身份是否合法。

本文认证方案中的安全模型将传统集中式认证服务器或者 CA 三方认证模式，通过区块链技术转变为分布式、无中心的多方参与模型，并与 MANET 组网过程结合，为有预先组织设置、高可信要求的应用场景提供了安全的认证方案。

安全性分析如下。

常见的攻击方法包括网络侦听、重放攻击、口令猜测、跟踪地址攻击等，传统认证方式还面临单点失效和多 CA 信任难的问题。本文方案采用区块链技术，从而具有了以下几方面安全性。

1) 无中心化：通过 MANET 节点共同参与认证，并将密态账本信息在各节点中同步，可有效实现认证功能从集中式转变为分布式；待认证节点可以从相邻的 P2P 节点直接发起认证请求，在避免单点失效、多 CA 信任难问题的同时，能够实现快速认证接入。

2) 防篡改：经过共识后的认证信息记录在区块链中，具有严格顺序关系的链式结构以及父/子哈希值变动关联的特性，保证了链上数据的不可篡改性。

3) 恶意节点追踪：每个参与共识过程的 P2P 节点将回复信息返回给主节点后，根据方案设计，结果值会记录在区块体中，如果网络中存在恶意节点，根据区块链的不可篡改性，其操作和时间戳信息都可通过链中信息进行溯源，从而实现恶意节点追踪功能。

4) 防欺骗伪造：采用改进的 PBFT，MANET 内部最大节点欺骗个数是总节点数的 $\frac{1}{3}$ ；对于外部攻击，假设攻击者掌握用户的身份哈希值，但因其不具备用户私钥，无法对消息进行签名，因此无法伪造用户的动态身份签名值。在上述两种状态下，认证过程具有一定的防欺骗和伪造攻击能力。

5) 抗重放攻击：在认证过程中，每次传送的消息都包含了时间戳信息。由于每个区块头中包含时间戳和随机数，如果攻击者将消息重放，收方可通过时间戳判断该消息为重放消息，拒绝其认证请求。由此可以有效防止创建区块过程中的重放攻击。

6) 可靠性：分布式账本是一种分布式数据库，即使网络中某个节点损坏，也不影响全网账本的高可用性，且同时满足账本失效转移同步和备份恢复等安全要求。

5 智能合约讨论

智能合约是一种在满足特定条件时，自动执行的计算机程序。它是代码和数据的集合，

可以部署在区块链网络上运行。其可事先制订规则,让网络中节点按照规则完成预先设计好的合约功能。节点或者用户的认证过程通常同时包含授权功能,触发/执行条件不同、权限等级不同、这些需求都可以在智能合约中设计和实现。另外,通过智能合约,还可以考虑对权限定义中的一部分操作(如对不同等级命令的执行)实现自动执行关联,以减少人为控制带来的风险。

本文方案侧重区块链技术在MANET节点认证中的应用,从轻量化角度出发,认证流程中不引入智能合约技术。对授权的设计是下一步工作。

6 结束语

本文通过国内外文献首先分析了区块链技术与移动自组网结合的现状。MANET的自组织特性具有和区块链基础结构对等网络天然融合的优势,但自组网的动态性、资源受限又对冗余度高的区块链技术方案设计提出了挑战。针对可信环境要求高的MANET场景,本文提出了一种基于区块链的轻量化节点认证方案,详细说明了跨层对等网络P2P生成算法、认证账本设计、基于PBFT的适应性改进共识算法,并给出了状态机描述的节点认证流程。通过消息分发流程的分析,估算了当给定对等节点之间最大传输时延 $\tau_{\max}$ 时,节点认证时间 δ 和网络规模间的关系是 $\left(\frac{N_t^{\text{all}}}{3} + 7\right)\tau_{\max} \leq \delta \leq 3(N_t^{\text{all}} + 1)\tau_{\max}$ 。作为

区块链核心技术之一的智能合约技术,本文规划了其应用于授权权限管理的方向,并将作为下一阶段的工作重点继续推进区块链技术在MANET网络中的应用。

参考文献:

[1] 朱建明,付永贵. 基于区块链的供应链动态多中心协同认证

模型[J]. 网络与信息安全学报, 2016, 2(1): 27-33.

ZHU J M, FU Y G. Supply chain dynamic multi-center coordination authentication model based on block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(1): 27-33.

[2] 吴邱涵,胡卫. 基于SM2算法和区块链的移动端身份认证协议设计[J]. 网络与信息安全学报, 2018, 4(9): 60-65.

WU Q H, HU W. Design of identity authentication agreement in mobile terminal based on SM2 algorithm and blockchain[J]. Chinese Journal of Network and Information Security, 2018, 4(9): 60-65.

[3] 宋宇波,戚姗姗,胡爱群. 权限可控传递的物联网共享设备委托授权访问机制[J]. 网络与信息安全学报, 2019, 5(2): 40-49.

SONG Y B, QI S S, HU A Q. Delegation authorization mechanism with controllable permissions propagation for IoT devices sharing[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 40-49.

[4] LIEBEHERR J, DONG G. An overlay approach to data security in Ad-Hoc networks[J]. Ad Hoc Networks, 2007, 5(7): 1055-1072.

[5] CHO J H, SWAMI A, CHEN I R. A survey on trust management for mobile Ad Hoc networks[J]. IEEE Communications Surveys & Tutorials, 2011, 13(4): 562-583.

[6] SAXENA N, TSUDIK G, YI J H. Identity-based access control for Ad Hoc groups[C]//7th International Conference on Information Security and Cryptology - ICISC 2004. 2004.

[7] WINTER R, ZAHN T, SCHILLER J. Dyna MO: a topology-aware P2P overlay network for dynamic, mobile Ad-Hoc environments[J]. Telecommunication Systems, 2004, 27(2-4): 321-345.

[作者简介]



张勳(1973-),女,上海人,博士,北京邮电大学副教授,主要研究方向为移动自组网安全、信息物理融合系统。



马欣(1996-),女,陕西榆林人,北京邮电大学硕士生,主要研究方向为区块链技术。