物联网医疗系统安全和隐私保护方法研究*

陈庆龙 石春花 郝文延

（长治医学院附属和平医院 长治 046000）

〔摘要〕 提出一种基于 Holochain 的物联网医疗系统安全与隐私保护方法，阐述方案设计以及具体模型构建，分析安全机制性能，指出基于 Holochain 的物联网医疗系统时间和空间复杂度显著降低，更具优势。

〔关键词〕 区块链；Holochain；医疗保健；物联网；分布式网络；安全威胁

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2022.01.013

Study on the Security and Privacy Protection Method for Internet of Things Medical System

CHEN Qinglong, SHI Chunhua, HAO Wenyan, Heping Hospital Affiliated to Changzhi Medical College, Changzhi 046000, China

〔**Abstract**〕 The paper proposes a holochain－based security and privacy protection method for Internet of Things (IoT) medical system based on Holochain, expounds the scheme design and specific model construction, analyzes the performance of security mechanism, and points out that the time and space complexity of Holochain－based IoT medical system is significantly reduced and has more advantages.

〔**Keywords**〕 blockchain; Holochain; healthcare; Internet of Things (IoT); distributed network; security threat

1 引言

1.1 物联网概述

物联网（Internet of Things，IoT）是物理设备网络，包括嵌入式传感、处理和通信技术，主要通过互联网收集和传输感官数据。随着异构技术的进步，物联网应用迅速发展，包括智能城市、医疗、家居、农业、教育、食品工业等领域[1－2]。在医疗保健领域引入物联网应用有可能彻底改变行业，如果实现医疗保健系统各实体之间的集成连接以及准确和及时的互操作，大量敏感医疗数据将得以共享并具有即时可访问性。基于物联网的医疗保健网络数据容易受到未经授权访问和其他恶意活动攻击[3－4]。由于物联网医疗设备有资源限制，传统加密技术如高级加密标准（Advanced Encryption Standard，AES）和不对称密码演算法（Rivest－Shamir－Adleman，RSA）不适合保护大量敏感医疗数据。所以轻量级加密算法被用于物联网医疗保健应用中，从而降低时间复杂度[5]并在安全性和服务之间进行了权衡。然而由于物联网医疗技术的异构性和动态环境攻击者仍然可以发布各种威胁，系统容易受到数据窃取和篡改。实时分布式安全方法（如基于区块链的方法）成为一种有前景的替代方法，可有效应对物联网医疗系统中的各种隐私、安全和认证挑战。

〔修回日期〕 2021－06－18

〔作者简介〕 陈庆龙，工程师，发表论文2 篇。

〔基金项目〕 山西省高校科技创新项目（项目编号：No. 2019L0672）。

1.2 Holochain 概述

Holochain 是一种新兴技术，它提供一种开源的分布式网络基础设施，可以在不继承区块链等巨大存储和数据交换需求的情况下进行安全通信[6]。Holochain 通过结合两种底层技术执行任务：分布式哈希表（Distributed Hash Table，DHT）和哈希链。分布式哈希表关注的是数据传播问题，而哈希链用以保持数据完整性。Holochain 旨在构建完全分布式的网络，DHT 可以在物联网医疗网络中实现和使用，用于在每个节点中存储转换数据链，以确保基于 Holochain 的网络自治性[7]。本文针对应用安全和隐私问题，基于 Holochain 的物联网医疗方法提出一种低复杂性、高安全性的区块链替代方案。

2 轻量级可扩展安全解决方案设计

2.1 增强扩展性

区块链是一种以数据为中心的分布式安全方法，其主要目的是在网络中所有授权用户之间创建一个单一的共享数据块。数据大小将随着每个交易涉及的网络实体数量增加而增加并且不可扩展。相反每个 Holochain 应用程序由一个代理维护，该代理可以独立参与数据加密，将交易存储在 Holochain 网络的唯一源链中并与对等代理共享所需数据，这种以代理为中心的 Holochain 方法具有高度可扩展性。

2.2 减少网络流量

Holochain 将数字签名和 DHT 相结合，可以作为区块链的有效替代方案，以改善分布式对等网络（Peer - to - Peer，P2P）中信息检索的性能。Holochain 网络中的每个代理都在本地存储其单独数据。在物联网网络中，由于内存和计算能力有限制，许多设备使用雾节点或云来存储其数据库。然而每个代理都能够计算各自的哈希值并使用 DHT 与其他对等方共享敏感医疗数据。相反区块链网络所有对等点存储的是无法区分的传输副本，这需要节点之间进行更多通信交换。此外每个实体都需要额外带宽，会显著增加网络带宽消耗并影响可扩展性。在 Holochain 中代理不需要与网络所有其他节点共享各自交易信息，可以显著减少网络中的带宽需求量和流量。

2.3 低复杂度交易验证

在区块链中矿工负责通过解决数学问题以验证新交易。任何网络节点都可以充当矿工并随时启动挖掘。例如有 20 个网络节点，其中 10 个节点开始挖掘以验证交易，最早找到数学问题解决方案的节点将验证交易。矿工可以与其他节点协同工作，同时进行挖掘。Holochain 允许各节点验证其自身交易，在将交易信息与某些其他预先确定信息一起发送给它们时，允许具有预定距离的邻居节点对该交易进行 2 次验证[8]。只有少数节点保留交易副本，因此内存空间和信息交换量明显低于区块链。

2.4 高效的共识机制

与区块链不同，Holochain 不需要全球共识机制。Holochain 旨在为每个用户或 1 组用户提供自主权，这些用户可以在不需要任何全局协商一致的情况下验证交易[9]，见图 1。显然 Holochain 比区块链效率更高。为验证交易，区块链将当前交易发送到所有节点以存储完整节点信息，而 Holochain 只需要几个参与运行同一应用程序的主机验证当前交易，不需要全局一致性。此外验证过程、数据所有权和网络治理仅由代理和创建者管理。在某些情况下可能用于验证节点或交易的数据本身没有被授权，为解决此问题可使用哈希指纹帮助检测交易身份验证[10]。

2.5 操作时间和存储效率

区块链固有属性之一是所有节点中具有相同交易信息，以便在整个哈希树中提供数据完整性。在许多实际应用中 1 个特定用户数据可能不会引起其他人兴趣，但区块链网络强制所有用户存储所有信息，增加数据处理时间和内存空间[11]。鉴于许多物联网医疗设备都是轻量级，这不利于其设计目标的实现。在 Holochain 中只有一些选定代理会存储数

据以确保数据完整性和本地存储交易，节省内存和处理时间。

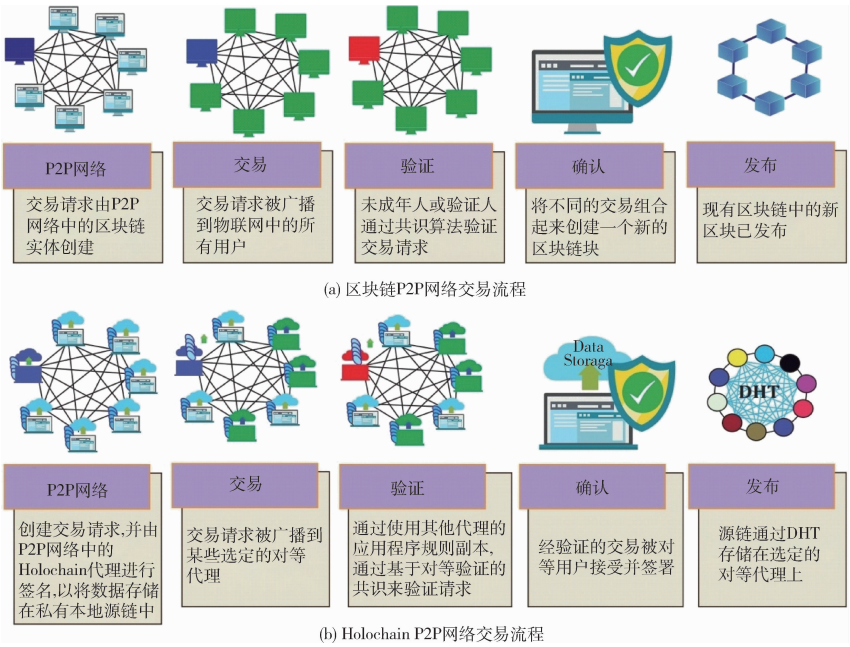

图 1 区块链和 Holochain 交易验证流程

2.6 大规模网络效率

由于区块链技术监控和存储连接到网络中每个节点上的所有交易，随着用户数量增加网络负载迅速增加，导致大规模网络中效率低下[12-13]。如果 1 个网络由 100 个节点组成，由于每个交易都增加数据冗余和时间复杂度，网络效率将降低 100 倍。相反 Holochain 处理任务只是线性升级并在网络其他节点之间分配处理负载。如果 1 个 Holochain 网络包含 100 个代理，整个网络负载将被分配到 100 个节点，每个节点只处理总交易的一小部分，大多数节点将节省大量网络效率。实现比特币结构的区块链网络的平均时间复杂度[14-15]为：

$$\Omega_{blockchain} \in O(n^2 * m) \quad (1)$$

其中，n 为节点数，m 为所需的网络交易数量。Holochain 方法的平均时间复杂度为：

$$\Omega_{Holochain} \in O(m * (\log(n) + c)) \quad (2)$$

其中，c 为应用程序特定的复杂度参数。

利用上述时间复杂度定义可比较分析区块链和 Holochain 网络的时间复杂度与节点数，见图 2。区块链网络时间复杂度随节点数增加呈指数级增长[16-17]，而 Holochain 网络平均时间复杂度随节点数的增加在很大程度上保持不变。

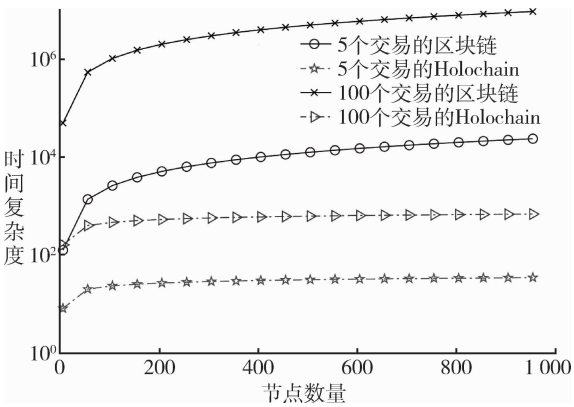

图 2 区块链和 Holochain 网络时间复杂度

3 基于 Holochain 的物联网医疗保健模型构建

3.1 模型结构

提出一种基于 Holochain 的新型智能物联网医疗系统，该系统保证了严格的数据完整性和高水平网络安全性。提出的物联网医疗保健模型由 4 个层次组成：感知层、网络层、云层或处理层、应用层，见图 3。

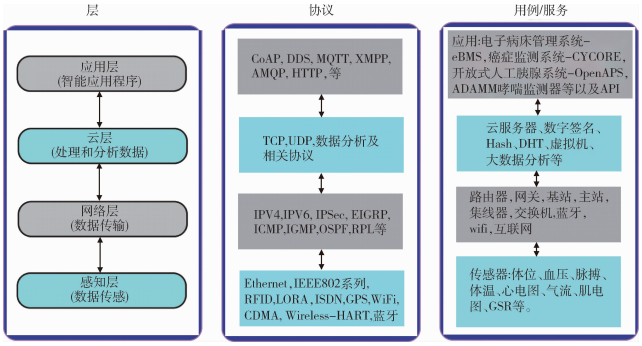

图3 物联网医疗体系结构分层协议和技术

3.2 感知层

鲁棒信任评估系统仅用于从授权用户收集数据。基于 Holochain 的物联网医疗方法将患者、医生、医务人员、技术专家、护士以及感知层中的医疗设备等各种医疗实体互连，医疗保健系统的每个实体都可能发生多个事件，通过 1 组独特的、基于逻辑的规则来使用这些应用程序，以提供特定服务，见图 4。

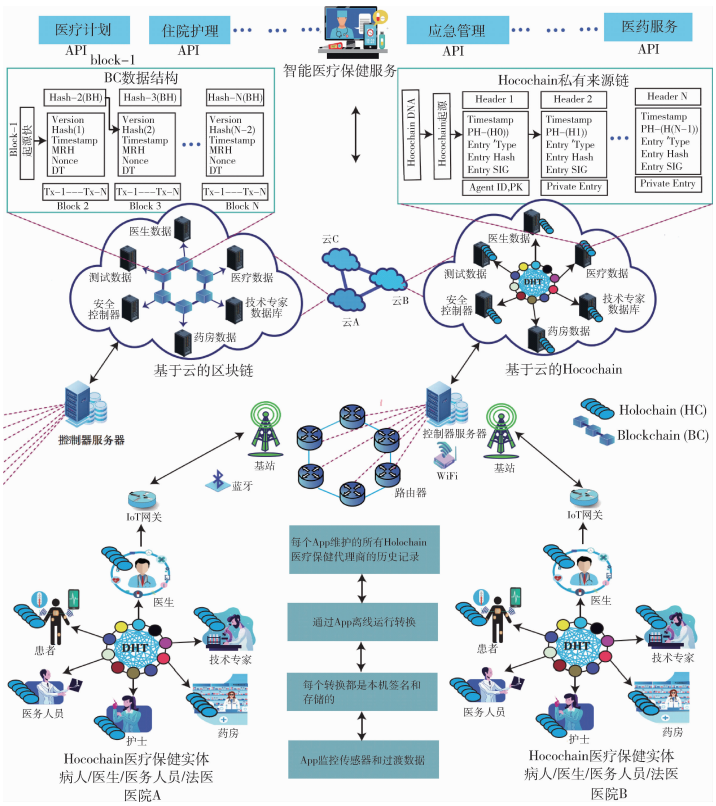

图4 基于 Holochain 的物联网医疗体系结构

感知层负责感知和收集必要信息，如患者医疗数据[18]。物联网节点通过以太网，IEEE802 系列，无线传感器网络（Wireless Sensor Network，WSN），全球定位系统（Global Positioning System，GPS），无线 HART 和蓝牙等各种协议感知、收集并传输数据。

3.3 网络层

接收来自感知层的转发医疗数据，这些医疗数据是由各种应用程序处理的用于 IP 寻址的信息。该层使用各种常见协议，如 IPV4、IPV6、IPSec、ICMP 等多种通用协议，确保可靠的传输路径。网络层使用路由器、网关、基站、主站、集线器、交换机、蓝牙和 WiFi 等异构设备和技术处理交易并提供服务。这一层对数据包进行处理后将可信信息传输给上层云层，云层负责以分布式方式管理 IoT 节点之间可信值的存储和共享。

3.4 云层

由于物联网设备资源有限，敏感医疗数据可以

存储在云端，授权方（如医生、保险公司、医务人员、药房等）可以方便地共享医疗数据。患者及其他实体可以将医疗数据存储在云中并与授权对等方共享该数据以增强医疗保健服务的性能。传输控制协议（Transmission Control Protocol，TCP），用户数据报协议（User Datagram Protocol，UDP），ML，数据分析和预测协议是该层的常用协议。为保证云层安全性和数据完整性，在云设备中使用分布式 Holochain。

3.5 应用层

负责医疗数据的格式化和表示，这一层定义了1 组用于传输医疗数据的规则。受限应用协议（Constrained Application Protocol，CoAP），数据分发服务（Data Distribution Service，DDS），消息队列遥测传输（Message Queueing Telemetry Transport，MQTT），可扩展消息传递和状态协议（Extensible Messaging and Presence Protocol，XMPP），高级消息队列协议（Advanced Message Queuing Protocol，AMQP）和超文本传输协议（Hyper Text Transfer Protocol，HTTP）是专用于应用层的协议。应用层通过与用户直接通信提供基于应用程序的服务。

4 安全机制性能分析

4.1 概述

分布式分类技术在整个网络上以分布式方式复制、同步和传输医疗数据。Holochain 是一种安全保护的分布式分类技术，它实现了高级加密和加密货币概念，具有可靠、防篡改特点，能够抵抗各种攻击，例如拒绝服务（Denial of Service，DoS），假节点，中间人攻击等[19]。智能医疗服务会处理大量用户医疗数据，由于物联网医疗系统的异构技术，需要考虑安全漏洞[20]。

4.2 加密机制

4.2.1 *常用加密算法* 使用物联网中的医疗数据，根据两个关键性能指标（Key Performance Indicator，KPI），即每比特的内存使用量和 CPU 周期，评估和比较算法性能。同时还提供各种现有分布式分类技术针对 KPI 执行的比较分析。其中 AES 和数据加密标准（Data Encryption Standard，DES）是两种常用的对称密钥分组密码算法，RSA 是一种非对称密钥加密机制，能够检测并抵抗物联网中的各种常见攻击。泄漏提取（LEX）和光加密设备（LED）是 AES 的扩展版本。此外 LEX 是一种面向软件的流密码，使用递归过程修改 AES 密钥流。LED 更适用于硬件实现，使用简单的密钥调度抵抗各种攻击，尤其是 LED－80。

4.2.2 *轻量级分组密码* 如 RC5 和 Salsa20。RC5 在递归过程中利用可变数量的块大小、密钥大小和轮数，这取决于微处理器功能。Salsa20 利用 64 字节块大小的散列和异或函数优势。由于相对较低的内存需求，RC5 和 Salsa20 更适合基于物联网的医疗应用。而 SPECK 和 SIMON 用于密钥大小和块大小可变的多块密码。使用 SIMON 和 SPECK 的基本优势是提高速度和内存利用率，更适合轻量级医疗保健应用程序。

4.2.3 *物联网现有加密机制比较分析* 通过对现有物联网安全机制性能比较分析可知，与其他密码相比 LEX 的 CPU 速度最快。虽然 AES 和 DES 比 SPECK 略快，但就内存使用而言，SPECK 比 AES 和 DES 速度更快。综合考虑各种安全机制性能，SIMON 和 SPECK 在资源受限的物联网中具有更好性能。

4.2.4 *常用分布式分类技术物联网安全性能比较分析* 由于分布式分类技术功能不同于现有传统加密机制，因此内存需求比 CPU 周期更重要，软件定义网络（Software－Defined Networking，SDN）和区块链混合技术能够提供比传统区块链更好的性能。区块链包括来自任何用户的请求，但 SDN 确保安全连接并避免不必要请求，减少每个比特内存和 CPU 周期。尽管这项技术在区块链领域带来新突破，但内存需求和处理技术仍然是挑战。Holochain 和 Holochain RSM（Holochain 新版本）在物联网等动态实时实现中减少大量数据处理和存储负载，Holochain 内存利用率和速度远远优于区块链技术。

5 结语

本文提出一种基于 Holochain 的分布式物联网医疗应用安全保护方案，该方案充分利用 Holochain 体系结构和协议的固有自主性。与区块链相比 Holochain 通过在用户端运行应用程序，将通信代理从任何形式的集中控制中解放出来，因此不存在故障中心点。由于用户是主机，随着更多代理使用应用程序，主机和存储可用性更强，负载也会变得更轻。一旦代理更改其应用程序代码，它们会有效地将自身从共享分布式分类技术空间中分离出来，进入完全不同的应用程序。因此 Holochain 是分布式物联网应用中最有效的技术。比较分析性能结果表明与区块链方案相比 Holochain 方法的时间和空间复杂度显著降低，为大规模物联网医疗系统实际部署提供前景。基于 Holochain 的技术将在确保下一代大规模部署通信模型的安全性和私密性方面发挥重要作用，因为该技术允许具有分散式体系结构并且具有高可扩展性、轻量级、灵活性和透明性以及高安全性优势，可为 5G 或即将到来的 6G 标准中出现的高数据速率和低延迟通信系统提供支持。

参考文献

1 季敏. “互联网 +” 形势下应用微信平台改善医疗服务的实践与思考 [J]. 中国卫生产业，2020，17（31）：99 – 102.

2 蒋伟宏. 基于物联网的智慧城市固态废物垃圾卡车调度及路径规划方案研究 [J]. 湖南邮电职业技术学院学报，2019，18（1）：5 – 7.

3 杨洪民，王全景，仪维，等. 基于物联网的医疗健康大数据智能化采集系统及云管理系统 [J]. 智慧健康，2019，5（34）：1 – 3.

4 马磊. 基于物联网技术的医疗图像数据安全传输模型研究 [J]. 中国医疗设备，2021，36（2）：54 – 57.

5 钱涵佳，王宜怀，彭涛，等. 轻量级窄带物联网应用系统中高效可验证加密方案 [J]. 计算机研究与发展，2019，56（5）：1112 – 1122.

6 Janjua K，Shah M A，Almogren A，et al. Proactive Forensics in IoT：Privacy – Aware Log – Preservation Architecture in Fog – Enabled – Cloud Using Holochain and Containerization Technologies [J]. Electronics，2020（9）：1 – 39.

7 Zia M F，Benbouzid M，Elbouchikhi E，et al. Microgrid Transactive Energy：Review，Architectures，Distributed Ledger Technologies，and Market Analysis [J]. IEEE Access，2020，8（1）：19410 – 19432.

8 张永，和凯. 基于邻居节点间相互影响和改进概率的社交网络信息传播模型 [J]. 计算机应用研究，2018，35（3）：755 – 759，764.

9 方亮，刘丰年，苗付友. 基于秘密共享的组密钥协商方案 [J]. 计算机工程与应用，2018，54（12）：69 – 73，151.

10 刘轩甫，刘玉梅. 社会机会网络中基于局部敏感哈希的用户隐私保护方案 [J]. 应用科技，2019，46（3）：93 – 99.

11 葛利洁. 基于区块链技术的交易信息存储与查询系统的设计与实现 [D]. 北京：北京邮电大学，2018.

12 胡兆鹏，丁卫平，高瞻，等. 一种基于区块链技术的多阶段级联无线安全认证方案 [J]. 计算机科学，2019，46（12）：180 – 185.

13 汪金苗，谢永恒，王国威，等. 基于属性基加密的区块链隐私保护与访问控制方法 [J]. 信息网络安全，2020（9）：47 – 51.

14 方响，马笛，侯伟宏，等. 分布式新能源接入下的区块链共识机制研究 [J]. 浙江电力，2019（7）：1 – 6.

15 李涵，张晨，黄荷姣，等. 一种支持前向安全更新和验证的加密搜索算法 [J]. 西安电子科技大学学报，2020，47（5）：52 – 60.

16 袁敏夫，李引，陈胜俭，等. 基于云平台的区块链组网方案及数据共享存储机制 [J]. 计算机与现代化，2019（9）：46 – 52.

17 喻国明学术工作室. “数字劳工” 与权益平衡：区块链对网络平台机制的全新建构 [J]. 东南传播，2020（5）：1 – 4.

18 李春贺，陶帅. 基于大数据的采矿人员安全感知信息实时采集系统设计 [J]. 现代电子技术，2019，42（7）：27 – 31.

19 吴文丰，张文芳，王小敏，等. 一种安全增强的 LTE – R 车 – 地无线通信认证密钥协商方案 [J]. 铁道学报，2019，41（12）：72 – 80.

20 信海辉，张姗姗. 云计算背景下物联网数据挖掘技术分析与实验验证 [J]. 数字通信世界，2020（2）：115.