文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于区块链的扫地机器人固件检测算法分析

潘亚峰
北京石头创新科技有限公司
DOI:10.12238/acair.v3i2.13493

[摘　要] 随着智能家居设备的普及,扫地机器人固件的安全性与可靠性日益受到关注。传统的固件检测方法存在数据篡改、检测结果不可信等问题,难以满足现代智能设备的安全需求。本文提出一种基于区块链的扫地机器人固件检测算法,通过区块链技术的去中心化、不可篡改特性,构建一个可信的固件检测框架。具体包括基于权威证明(PoA)的区块链网络架构设计、固件哈希值生成与上链机制、智能合约的检测逻辑与异常处理、检测结果的可追溯性与可视化实现,以及算法的性能优化与扩展性设计。
[关键词] 智能家居；扫地机器人；固件检测；区块链
中图分类号：TP18　文献标识码：A

Analysis of a Blockchain-Based Firmware Verification Algorithm for Robotic Vacuum Cleaners

Yafeng Pan
Beijing Stone Innovation Technology Co., Ltd.

[Abstract] With the widespread adoption of smart home devices, ensuring the security and reliability of robotic vacuum cleaner firmware has become increasingly important. Traditional firmware verification methods are susceptible to data tampering and untrustworthy detection results, making them inadequate for meeting the security requirements of modern intelligent devices. This paper proposes a blockchain-based firmware verification algorithm for robotic vacuum cleaners, leveraging the decentralized and tamper-resistant properties of blockchain technology to establish a trustworthy firmware verification framework. The proposed approach includes the design of a blockchain network architecture based on Proof of Authority (PoA), the generation and on-chain storage of firmware hash values, the implementation of verification logic and anomaly handling via smart contracts, the traceability and visualization of detection results, and algorithmic performance optimization and scalability enhancements.
[Key words] Smart home; Robotic vacuum cleaner; Firmware verification; Blockchain

引言

扫地机器人作为智能家居的重要组成部分,其固件的安全性与可靠性直接影响用户隐私与设备功能稳定性。传统固件检测方法依赖中心化机构,存在数据篡改、检测结果不可信等问题,难以满足现代智能设备对安全性和可追溯性的高要求。区块链技术以其去中心化、不可篡改和透明可追溯的特性,为固件检测提供了新的解决思路。本文旨在设计一种基于区块链的扫地机器人固件检测算法,通过构建基于区块链的分布式检测网络、引入智能合约与分片技术,实现固件数据的高效验证与不可篡改记录,为智能家居设备的安全运行提供技术保障。

1 扫地机器人固件检测需求分析

随着扫地机器人功能的日益复杂化,固件中可能存在的漏洞、恶意代码或未经授权的修改对设备安全构成潜在威胁[1]。传统的固件检测方法通常依赖于中心化的检测机构或本地验证机制,存在数据篡改、检测结果不可信、缺乏透明性等问题,难以满足现代智能设备对安全性和可追溯性的高要求。此外,扫地机器人的固件更新频率较高,检测过程需要具备高效性、实时性和可追溯性,以确保每次更新的固件均经过严格验证。区块链技术以其去中心化、不可篡改和透明可追溯的特性,为固件检测提供了全新的解决方案[2]。通过构建基于区块链的检测网络,可以实现固件数据的分布式存储与验证,确保检测结果的真实性和可信度。同时,智能合约的引入能够自动化执行检测流程,提高检测效率,并为用户提供透明、可信的检测结果。因此,基于区块链的扫地机器人固件检测算法不仅能够满足固件完整性验证的需求,还能为智能家居设备的安全运行提供有力保障。

2 基于区块链的扫地机器人固件检测算法

2.1基于PoA的区块链网络架构设计

为满足扫地机器人固件检测的去中心化和透明性需求,本文设计了一种基于PoA共识机制的区块链网络架构[3]。该架构由三类节点组成：扫地机器人设备节点、检测节点和用户节点。其中,设备节点负责固件数据的上传,检测节点负责哈希值的验证和共识过程,用户节点则用于查询检测结果。每个节点通过数字签名技术(如ECDSA)进行身份认证,确保网络的安全性。共识过程中,检测节点通过式(1)验证设备节点的签名,其如下所示：

$$C = \text{Verify}(S, K_{\text{pub}}) \tag{1}$$

其中K_{pub}为公钥；C为验证结果,通常是一个布尔值(True或False)； Verify()表示验证函数,用于验证数字签名的有效性,确保数据来源的可靠性。通过轻量级共识机制,网络在保证安全性的同时显著降低了计算和存储开销,为固件检测提供了高效、可靠的分布式环境。

此外,本文采用分片技术将网络划分为多个子链,每个子链独立处理部分检测任务,进一步提高了网络的扩展性和处理效率。分片过程中,通过将网络节点N划分为K个子链,每个子链负责特定范围内的固件检测任务,其如式(2)所示：

$$\text{Shard}(N, K) \tag{2}$$

其中,Shard( )为分片函数,固件检测数据以区块的形式存储,并通过哈希链连接,形成不可篡改的检测记录链。每个区块包含固件哈希值 H、版本信息 V、设备标识符 D 以及时间戳 T,通过式(3)构建,如下所示：

$$\text{Block} = (H, V, D, T, \text{PrevHash}) \tag{3}$$

其中,PrevHash 为前一个区块的哈希值,确保数据的连续性和不可篡改性。这种设计不仅满足了固件检测的高效性和可追溯性需求,还为大规模扫地机器人设备的固件检测提供了技术保障。

2.2固件哈希值生成与上链

在扫地机器人固件检测过程中,固件数据的完整性验证是关键环节。首先,扫地机器人的固件二进制数据通过哈希算法(如SHA-256)生成唯一的哈希值[4]。在具体实现中,固件数据 F 被分割为固定大小的数据块 $F_1, F_2, \ldots, F_n$,每个数据块通过SHA-256算法生成中间哈希值 $H_i = \text{SHA} - 256(F_i)$,最终将所有中间哈希值合并并通过二次哈希计算生成全局哈希值,如式(4)所示：

$$H = \text{SHA} - 256(H_1 || H_2 || \ldots || H_n) \tag{4}$$

其中 $\|$ 表示字符串连接操作。该哈希值 H 作为固件数据的数字指纹,能够唯一标识固件内容。为确保检测的全面性,哈希值与固件版本信息、设备标识符等元数据绑定,形成完整的检测记录,如式(5)所示：

$$M = (H, V, D) \tag{5}$$

这些数据通过智能合约上传至区块链网络,智能合约在上传过程中对哈希值进行初步验证,确保其格式正确且未被篡改。具体验证逻辑包括检查哈希值长度是否为64字符、是否包含非法字符以及是否与历史记录冲突。通过将固件哈希值上链,实现了固件数据的不可篡改存储,为后续的完整性验证提供了关键依据。此外,区块链的分布式特性确保了检测记录的透明性和可追溯性,任何对固件数据的修改都会被记录并公开,从而有效防止恶意篡改行为,为扫地机器人的安全运行提供了可靠保障。

2.3智能合约的检测逻辑与异常处理

智能合约作为区块链网络的核心组件,负责固件检测的自动化执行,其检测逻辑包括哈希值验证、固件版本比对和异常处理[5]。当固件数据上链后,智能合约自动触发检测流程,首先,通过公式(6)验证当前固件哈希值 H 与区块链中存储的历史哈希值 H' 是否一致,其中 H' 为历史记录中的哈希值,如下：

$$\text{Verify}(H, H') \tag{6}$$

若 $H \neq H'$,则表明固件数据可能被篡改,智能合约将触发警报机制。其次,智能合约通过公式(7)比对当前固件版本 V 与历史版本 V' ,如下：

$$\text{Compare}(V, V') \tag{7}$$

其中 V' 为历史记录中的版本信息。若 V 与 V' 不匹配或 V 为未经授权的版本,智能合约将记录异常信息,如式(8)所示：

$$E = (H, V, D, T) \tag{8}$$

其中 E 为异常记录,并将 E 存储于区块链中,供后续追溯和分析。

为进一步提高检测的准确性,智能合约还引入了多节点验证机制,即多个检测节点对同一固件数据进行独立验证,并通过共识机制确定最终检测结果。这种设计不仅提高了检测的可信度,还增强了系统的容错能力。此外,智能合约通过事件驱动机制实时通知用户检测结果,用户可通过区块链浏览器或专用工具查看详细检测报告。通过智能合约的自动化执行和多节点验证机制,固件检测过程高效且可追溯,为扫地机器人的安全运行提供了可靠保障。

2.4检测结果的可追溯性与可视化实现

为实现检测结果的可追溯性,本文在区块链网络中引入了时间戳机制,确保每条检测记录均与具体时间点绑定[6-7]。在具体实现中,每条检测记录 R 包含固件哈希值、版本信息、设备标识符以及时间戳,如式(9)所示：

$$R = (H, V, D, T) \tag{9}$$

时间戳是通过函数 GetTimestamp（） 生成,确保每条记录的时间点精确且不可篡改,其如式(10)所示：

$$T = \text{GetTimestamp}() \tag{10}$$

用户可通过区块链浏览器或专用可视化工具查询固件检测的历史记录,并追溯检测过程中的关键节点。可视化工具通过检索设备标识符在时间区间 $[T_1, T_n]$ 内的检测记录,并以图表形式展示检测结果的变化趋势,例如,表1展示了设备 D_1 在时间区间 $[T_1, T_n]$ 内的固件检测结果,包括固件版本、哈希值、检测状态及时间戳。由表1可知,固件版本 V_1 在时间 T_1 检测通过,而在时

间 T_2检测未通过,表明固件可能被篡改。此外,工具支持多设备管理,用户可实时监控多台扫地机器人的固件状态,进一步提升用户体验。通过时间戳机制和可视化工具的结合,检测结果的可追溯性和透明度得到了显著提升,为扫地机器人的安全运行提供了有力支持。

表1 设备 D_1的固件检测结果

时间戳 T	固件版本 V	哈希值 H	检测状态	设备标识符 D
T_1	V_1	H_1	通过	D_1
T_2	V_1	H_2	未通过	D_1
T_3	V_2	H_3	通过	D_1
T_4	V_2	H_4	通过	D_1

2.5算法的性能优化与扩展性设计

为提高算法的执行效率,本文对区块链网络进行了性能优化,具体通过引入分片技术将固件检测任务分配到多个子链中并行处理。分片技术将区块链网络划分为多个独立的子链,每个子链负责处理部分检测任务,从而显著提高了检测速度。在分片过程中,网络节点通过一致性哈希算法动态分配到不同的子链,确保负载均衡和任务分配的公平性。同时,为减少数据传输和存储的开销,本文采用了轻量级加密算法(如高级加密标准-128,Advanced Encryption Standard-128,AES-128)和压缩技术(如Zstandard压缩算法),在保证数据安全性的同时优化了网络资源的利用率。此外,本文设计的算法具有良好的扩展性,通过动态调整子链数量和节点分配策略,能够支持大规模扫地机器人设备的固件检测需求。例如,当网络中新增设备时,算法能够自动扩展子链数量,并通过智能合约动态分配检测任务,确保系统的高效运行。这种设计不仅满足了当前智能家居设备的安全需求,还为未来智能家居生态系统的扩展提供了技术保障,充分体现了区块链技术在固件检测中的优势。

在扩展性设计方面,本文通过动态调整子链的规模和处理能力,确保系统在高负载情况下仍能保持高效运行。例如,当检测任务量激增时,算法会自动增加子链数量,并通过智能合约重新分配任务,确保检测任务的及时完成。这种动态扩展能力使得算法能够适应不同规模的智能家居环境,为扫地机器人固件检测提供了高效、可靠的解决方案。通过性能优化与扩展性设计的结合,本文提出的算法不仅提升了检测效率,还为未来智能家居生态系统的扩展提供了坚实的技术基础。

3 结束语

本文提出的基于区块链的扫地机器人固件检测算法,通过构建基于区块链的检测网络、引入智能合约和分片技术,实现了固件检测数据的高效验证与不可篡改记录。算法通过哈希值生成与上链、智能合约的自动化检测逻辑、多节点验证机制以及时间戳绑定,确保了检测结果的透明性、可追溯性和高效性。此外,通过性能优化与扩展性设计,算法能够支持大规模设备的固件检测需求,为智能家居设备的安全运行提供了可靠的技术保障。未来,随着智能家居生态系统的进一步发展,本文提出的算法将为更多智能设备的固件检测提供技术参考,推动智能家居安全性的全面提升。

[参考文献]

[1]程福萍,周福昌,崔跃玉,等.扫地机器人噪声分析与控制[J].噪声与振动控制,2024,44(05):278-283.

[2]刘华懿.基于区块链技术的二手房交易监管服务系统研究与实现[D].辽宁省:辽宁大学,2023.

[3]常锦鹏.权威证明共识机制在区块链上的研究与应用[D].四川省:电子科技大学,2023.

[4]徐英朋.面向物联网安全芯片的SM3哈希算法IP核的设计与实现[D].河南省:中原工学院,2023.

[5]刘晓庆.基于智能合约的制造业供应链知识共享模式研究[D].山西省:太原科技大学,2023.

[6]赵宏平,方延学,高海艳,等.高值医疗器械替代物留样的可追溯性探讨[J].中国医疗器械信息,2024,30(23):45-48.

[7]张鹏,罗文华.基于布隆过滤器查找树的日志数据区块链溯源机制[J].信息网络安全,2024,(11):1739-1748.

作者简介：

潘亚峰(1983--),男,汉族,陕西渭南人,北京石头创新科技有限公司,硕士研究生,研究方向：软件开发。