 DOI: https://doi.org/10.12349/iser.v6i4.5300

Research on the application of blockchain technology in the botnet detection of the Internet of Things

Ying Xing[1] Yaxin Yang[2] Yushu Li[1]

1. School of Cyberspace Security, Zhongyuan Institute of Technology, Zhengzhou, Henan, 450007, China
2. School of Software, Zhongyuan Institute of Technology, Zhengzhou, Henan, 450007, China

Abstract

With the exponential growth of the number of Internet of Things devices, the traditional centralized botnet detection methods pose severe challenges in bandwidth consumption, single point of failure and data privacy protection. This paper systematically analyzes the innovative application of blockchain technology in botnet detection and protection, builds the decentralized C & C channel detection model through smart contract, designs distributed collaborative detection with digital signature and Byzantine fault-tolerant algorithm, and uses the lightweight blockchain architecture to optimize the storage and computing overhead in the Internet of Things environment. Blockchain technology can effectively solve the trust problem of detection nodes, ensure the integrity and privacy, and its tamper-proof features provide reliable support for attack traceability.

Keywords

blockchain technology; botnet detection; distributed detection

区块链技术在物联网僵尸网络检测中的应用研究

邢颖[1] 杨亚鑫[2] 李浴淑[1]

1. 中原工学院网络空间安全学院，中国 · 河南 郑州 450007
2. 中原工学院软件学院，中国 · 河南 郑州 450007

摘　要

随着物联网设备数量呈指数级增长，传统集中式僵尸网络检测方法在带宽消耗、单点故障和数据隐私保护等方面的严峻挑战。本文系统分析了区块链技术在僵尸网络检测与防护中的创新应用，通过智能合约构建去中心化C&C信道检测模型，利用数字签名和拜占庭容错算法设计分布式协同检测，采用轻量级区块链架构优化物联网环境下的存储与计算开销。区块链技术可有效解决检测节点信任问题，保障数据完整性与隐私安全，其不可篡改特性为攻击溯源提供可靠支撑。

关键词

区块链技术；僵尸网络检测；分布式检测

1 引言

随着大数据、云计算、区块链、人工智能、5G/6G 通信等新兴技术的快速发展与深度应用，人类社会迈入了名副其实的“数字时代”，以智能家居、智慧医疗、智慧城市、智慧农业、车联网、无人机系统等应用场景为代表的物联网（Internet of Things，IoT）技术已成为新型动态网络发展的核心技术之一。据全球领先的数据统计公司 Statisa 预测，IoT 设备的数量将呈爆炸性增长，预计到 2025 年全球将达到近 750 亿台。在日趋复杂的国际关系和地缘政治斗争的大背景下，网络空间安全俨然成为大国博弈的对抗领域。僵尸网络通常由控制者（Botmaster）、命令与控制信道（Command and Control Channel，C&C）以及僵尸主机（Bot）共同组成。作为数字化攻击的“超级武器”，Botmaster 可以通过控制服务器操控 Bot 对关键节点和网络基础设施发起复杂的网络攻击活动，包括勒索软件、分布式拒绝服务攻击、加密货币挖掘以及信息泄露等。僵尸网络作为重要的攻击平台，可对关键节点和网络基础设施进行直接打击，其影响和危害远远超过了传统恶意软件，对互联网生态安全构成了严重威胁。随着互联网的持续演化，僵尸网络在信道构建、消息传播等方面出现了更高级手段，呈现出平台多样化、通信隐蔽化、控制智能化等特点。以 5G、智能终端、云存储、社交平台为代表的公共服务资源逐渐成为僵尸网络滋生的沃土，特别是，物联网、车联网等物理信息基础设施的拓展为僵尸网络的传播提供了全新空间。

【基金项目】2024 年度河南省科技攻关项目“基于轻量级区块链的物联网僵尸网络智能检测方法研究”（项目编号：242102210136）。

【作者简介】邢颖（1985–），女，中国河南沈丘人，博士，讲师，从事网络安全研究。

与传统互联网环境相比，物联网环境具有一些独特的特点，如物联设备的小体积和有限内存容量，使其成为资源受限型系统；同时，设备旧化、系统防护较弱、安全设计缺失等问题都是众多安全漏洞频现的原因，容易受到破解和远程控制的威胁；再者，物联网的高度动态性导致设备之间的交互通常没有固定的模式，使得攻击手段多样且难以预测，增加了安全防护的复杂性。2021 年全球最大肉类供应商 JBS 遭遇了由 REvil 僵尸网络发起的勒索攻击，导致跨国冷链系统瘫痪 72 小时；2023 年，V3G4 恶意软件通过劫持百万级智能摄像头，构建了一个攻击金融交易中心的“视界黑洞”僵尸网络；2024 年，由 CNCERT 物联网安全研究团队与 ADLab 联合发布了一块具备诱捕及反探测能力的物联网僵尸网络，命名为“僵尸蜜网”。2025 年，僵尸网络对 DeepSeek 公司发起了分布式拒绝服务攻击，导致 DeepSeek 的核心服务器瘫痪，无法正常提供服务。

2 典型的僵尸网络检测关键技术

2.1 僵尸网络检测方法分类

大量文献从不同角度对检测技术开展研究，蜜罐技术通过模拟网络环境吸引恶意代码，利用逆向分析技术提取威胁特征，但面对加密数据传输时存在识别盲区，难以应对零日攻击及利用社会工程手段扩散的僵尸程序。传统特征码检测体系采用预定义规则库进行流量匹配（如 Snort 系统），虽能高效识别已知威胁，但其检测效能完全依赖特征库完备性，对新型攻击存在固有缺陷，且需投入大量资源进行规则库迭代维护。在异常行为检测领域，研究者主要聚焦于网络行为偏离度分析。该方法通过建立正常网络行为基准模型，对端口通信流量、数据包传输时延、协议交互频率等维度进行实时监测，通过计算当前行为与基准模型的统计学差异或与已知僵尸程序行为模式的相似性，实现潜在威胁的识别。这种动态检测机制虽能突破特征匹配的局限性，但在实际应用中仍需解决误报率控制、行为建模精度等技术挑战。

机器学习、深度学习等智能化方法为僵尸网络复杂特征工程提取及分类任务提供了新的模式。Jung 等人 [1] 通过侧信道功耗信息，如电量消耗等，来区分物联网设备是否受到恶意行为的影响，提出了一个基于卷积神经网络的深度学习模型来感知功耗数据的细微差异。McDermott 等人 [2] 提出了一种检测物联网设备中僵尸网络活动的解决方案，将 Mirai 的四种攻击向量作为特征向量，建立了基于双向长短期记忆的递归神经网络的检测模型。Bot Catcher 针对网络流量，从时间和空间两个维度，利用不同类型的深度神经网络模型进行检测，空间特征选取采用 CNN 将数据流转换成灰度图像，时间序列特征选取 BiLSTM 神经网络模型。XG-BOT 是一种利用图神经网络针对僵尸网络拓扑结构进行检测的方法，并给出了可解释性分析。GNN-WGAN 方法是一种融合图神经网络与 Wasserstein 生成对抗网络的，用于在智能城市物联网中有效检测僵尸网络攻击，提高了检测精度和模型的鲁棒性。GraphSAGE 是一种基于图神经网络的物联网攻击检测框架，通过捕捉图的边缘特征和物联网数据流信息来检测网络入侵。但是静态的图神经网络方法缺乏动态攻击场景下的僵尸网络攻击行为建模，多数方法处理单一维度数据，模型的自适应更新能力差，不适用于物联网场景下的检测，亟需新的动态解决方案。

2.2 集中式的僵尸网络检测方法分析

集中式僵尸网络检测的主要优势包括以下几点：首先，管理集中化，通过统一平台实现数据收集、分析与策略制定的集中管控，从而降低多节点运维的复杂性。同时，全局视角有助于系统性识别攻击模式，并优化防护策略。其次，部署便捷性，基于中心化架构，简化了硬件配置与软件协调流程。最后，算力集约化，依托中心化的算力资源，实现海量数据的快速处理与复杂模型的运算，通过集中式流量分析提升僵尸网络行为的识别效率。

然而，传统的僵尸网络检测方法存在诸多不足，例如带宽消耗大、单点故障风险高以及数据隐私问题。这些缺陷导致集中式方法在处理大规模物联网设备时效率低下，并且容易成为攻击者针对中心节点发起攻击的目标。此外，实时性方面也存在明显缺陷，在设备频繁接入或退出的动态环境中，数据采集与分析链路的延迟会影响攻击响应的及时性，难以有效应对时空演化型僵尸网络的隐蔽渗透行为。在智能化检测模型方面，大多数深度学习模型都假设网络处于静态状态，未能充分考虑时间演化因素，缺乏模型的自适应更新能力。因此，迫切需要开发新的动态解决方案。

3 区块链技术构建僵尸网络

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，可以实现分布式非可信环境下的数据完整性、一致性、可追溯性和不可篡改性。Omer Zohar 构建了一个完全在以太坊区块链上运行的僵尸网络，其所有通信都通过智能合约实现。新一代混合型两层僵尸网络 LNBot 利用闪电网络（Lightning Network，LN）作为命令控制信道的，利用链下概念实现近乎即时的比特币交易。Fbot 僵尸网络分析报告指出其通过 EmerDNS 实现抗逆向分析，利用 EmerCoin 的分布式域名系统动态解析 C&C 服务器 IP，替代传统 DGA 域名生成算法。华为 Noah’s Ark 实验室发现 Mirai 变种利用 MQTT 协议控制智能家居设备将 C&C 指令嵌入物联网协议，如 CoAP 的观察模式、MQTT 的发布订阅，伪装成设备正常通信。

4 区块链技术在僵尸网络检测中的应用

4.1 分布式检测

智能合约、数字签名、激励机制等技术也为分布式僵尸网络检测提供了新的视角。区块链在僵尸网络识别中的核心机制在于整合智能合约、密码学签名及激励体系等技术，依托分布式节点协同工作机制，通过共识机制推动节点间威胁情报共享及联合决策行为。具体表现为构建多代理协作架构下的可信交互平台，借助区块链的不可篡改特性实现检测数据溯源，并运用经济激励模型保障分布式检测节点的有效参与。

AutoBotCatcher[3] 利用拜占庭容错（Byzantine Fault

Tolerance，BFT）共识算法，在大型网络上执行动态和协作式的僵尸网络检测，使用社区检测算法 Louvain 方法检测僵尸网络社区。Wu 等人 [4] 提出了一种由区块链智能合约、PoW（Proof of Work）共识方案驱动的激励平台 SmartRetro，可以吸引更多的分布式检测器参与检测，并共享检测结果。分布式的基于区块链技术的僵尸网络检测方法可以为具有去中心化和频繁移动特点的物联网场景提供可信、弹性、自进化的智能检测框架，在保护隐私的前提下实现多节点协同的僵尸网络检测与防御，为构建安全可信的物联网生态系统提供理论支撑与技术保障。

4.2 轻量级架构

物联网设备通常存在计算能力和存储资源有限的问题，传统的区块链架构往往因其存储和计算开销过大，难以适应物联网的需求。轻量级区块链架构通过简化区块存储、优化共识算法、减少计算和存储开销，使得区块链能够更好地适应物联网设备的资源限制。例如，Javid 等人 [5] 提出的区块链解决方案通过智能合约设定设备的 gas 限制，对设备的行为进行监控。Zhang 等人 [6] 提出了一种基于联盟链的系统架构，将联盟链引入智能家居系统，通过改进拜占庭容错的 PBFT 共识机制，提出了 DTSG-PBFT 算法。Fan 等人 [7] 通过改进拜占庭容错算法提出了一种适用于车联云任务调度的轻量级区块链架构，将任务的调度过程与区块链紧密结合。

4.3 安全防护

4.3.1 节点信任

分布式检测架构中不同参与者之间的信任问题难以解决，存在数据共享与隐私保护之间的矛盾。物联网环境具有地理分布广泛、设备容量小、实时更新快等特点，而现有分布式检测架构缺乏可信数据共享与协同验证机制。跨域数据协同易引发敏感信息泄露，例如设备指纹和用户行为数据，现有区块链方案因高通信开销与低扩展性难以适配资源受限设备。此外，当前的基于区块链的分布式检测方法未充分考虑设备身份验证和敏感数据访问的安全验证等问题，容易遭受数据注入攻击，从而降低了整体的安全防护性能。检测设备都可以通过数字签名和智能合约来认证其身份，从而保证设备在网络中的可信度。例如，Ahmed 等人 [8] 提出的方案利用区块链技术来存储和共享设备的 IP 地址，通过比较设备生成的数据包数量与预设的阈值来检测是否存在僵尸网络行为。该方案采用区块链技术存储设备的认证信息，并且通过智能合约确保每个设备都通过合法验证后才允许加入网络，通过这种方式，每个设备的身份得到了唯一标识和认证，避免了传统集中式系统中由于单点信任导致的安全隐患。

4.3.2 数据安全

区块链技术不仅保证了数据不可篡改的特性，为数据交换提供了安全保障。在传统的集中式检测系统中，所有的网络流量数据通常都需要传输到中心节点进行处理，这可能导致数据泄露、篡改或中间人攻击的风险。而区块链通过其加密和去中心化存储的方式，确保了数据在传输过程中不被篡改或泄露。例如，BCIoT 框架在使用区块链进行设备身份认证时，所有的通信和数据交换都受到智能合约和加密算法的保护。该框架通过在区块链上记录设备的认证信息和流量数据，确保了数据交换的安全性，并且通过加密和数字签名技术，保障了流量数据的隐私安全。

5 结语

本文系统探讨了区块链技术在物联网僵尸网络检测中的创新应用与挑战。研究表明，区块链通过智能合约构建去中心化 C&C 信道检测模型，结合数字签名与拜占庭容错算法设计分布式协同检测，有效解决了传统集中式检测存在的单点故障、数据隐私泄露及节点信任问题。轻量级区块链架构的优化显著降低了物联网环境下的存储与计算开销，其不可篡改特性为攻击溯源提供了可靠技术支撑。然而，现有方案在链下数据可信性验证、动态检测模型构建及跨链协同机制等方面仍存在不足。未来研究应着重突破轻量级区块链与边缘计算的深度融合，构建基于跨链技术的分布式检测体系，同时结合 AI 算法实现动态自适应检测模型，为应对物联网僵尸网络的新型攻击范式提供更完善的安全防护解决方案。

参考文献

[1] Woosub Jung Hongyang ZhaoMinglong Sun Gang Zhou. IoT botnet detection via power consumption modeling. Smart Health. Smart Health 15 (2020) 100103 https://doi.org/10.1016/j.smhl.2019.100103.

[2] McDermott C D， Majdani F， Petrovski A V. Botnet detection in the internet of things using deep learning approaches[C]//2018 international joint conference on neural networks (IJCNN). IEEE，2018: 1-8.

[3] Gokhan Sagirlar, Barbara Carminati, Elena Ferrari. AutoBotCatcher: Blockchain-based P2P Botnet Detection for the Internet of Things[J], arXiv: Cryptography and Security, 2018: 1-8.

[4] Wu B，Li Q，Xu K，et al. Smartretro: Blockchain-based incentives for distributed iot retrospective detection[C]//2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE，2018: 308-316.

[5] Javid M, Khan S, Ahmad F. Blockchain-Based IoT Resource Optimization via Smart Contract Gas Limits[C]//Proceedings of the 12th IEEE International Conference on Blockchain and Cryptocurrency. New York: IEEE Press, 2023: 245-257.

[6] Zhang L, Li M, Wang F. Consortium Blockchain-Based Smart Home System with DTSG-PBFT Consensus[R]. Beijing: Tsinghua University Press, 2023: 1-25.

[7] Fan J, Li R, Zhang Y. Lightweight Blockchain Architecture for Vehicular Cloud Task Scheduling[R]. Beijing: Tsinghua University Press, 2020: 1-25.

[8] Ahmed, Z.; Danish, S.M.; Qureshi, H.K.; Lestas, M. Protecting IoTs from Mirai botnet attacks using blockchains. In Proceedings of the IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD,2019, Limassol, Cyprus, 11–13 September 2019; pp. 1–6