



基于区块链的 SDN 物联网部署安全

谢萍, 刘孝颂

(中国电信股份有限公司研究院, 上海 200122)

摘要: 与传统互联网相比, 由于基于 SDN 的物联网覆盖面更广、连接的设备更多、传输的数据更复杂等原因, 还存在很多安全方面的技术挑战。提出了在 SDN 物联网中加入一个基于区块链的安全层作为安全网关, 对进入物联网的数据进行一次性的精确验证, 各安全网关作为平等的区块链节点加入区块链系统, 结合区块链系统的可追踪和不可篡改性, 提高了 SDN 物联网部署的安全性能和效率。

关键词: 网络安全; 物联网; 区块链; SDN; 网络攻击; 分布式计算

中图分类号: TN915.9

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020323

Security of the deployment of SDN-based IoT using blockchain

XIE Ping, LIU Xiaosong

Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: Compared with the traditional internet, the SDN-based internet of things (IoT) has a wider coverage, more connected devices, more complex data transmission. There are many security technical challenges. The security challenges of SDN-based IoT deployment were firstly analyzed, and then the advantages of blockchain technology in solving those security issues were introduced. Finally, to add a blockchain-based security layer was proposed, which acted as a security gateway, data entering the IoT was verified accurately one time. Each security gateway was added to the blockchain system as an equal blockchain node, combined with the traceability and non-tampering of the blockchain system, the security performance and efficiency of SDN-based IoT deployments was improved.

Key words: network security, IoT, blockchain, SDN, network attack, distributed computing

1 引言

近年, 随着物联网技术的飞速发展, 物联网设备的使用规模呈现爆炸式增长。据统计, 2017 年物联网设备同比增长 31%, 达到 84 亿。预计到 2020 年, 这个数字将增长至 300 亿^[1]。物联网技术的广泛应用为物理世界更直接地整合到计算机

网络世界创造了机会, 从而减少人力消耗, 提升生产效率和经济效益, 但是, 物联网在带来开放性、包容性的同时也不可避免地引入了安全隐患, 而且, 物联网连接的对象数以十亿计, 其管理和控制对于大型分布式网络而言是一项极其复杂的任务。SDN 的引入使物联网的部署和管理更加简化和灵活, 同时也解决了物联网的一些安全问题。



但是,以 SDN 为基础网络架构的物联网依然存在着一安全隐患,而且还引入了 SDN 基础网络架构的一些新的安全挑战。由于物联网技术在各个领域的广泛应用,其安全性也引起了人们的高度关注。

由于区块链具有去中心化和很难篡改等特点,它可以在多种实际的业务场景中,用来建立信息,提升透明性、可靠性与安全性。区块链的巨大潜力引起了很多行业的注意,其中以金融领域和物联网领域最为火热,金融领域以支付系统和数字代币为代表,出现了很多成功的结合案例,而目前在物联网领域还处于比较早期的研究阶段,能看到物联网的建设与发展确实受到了安全隐私问题的制约^[2]。关于区块链技术改造升级物联网的研究,目前国内外学者已经做了一些有意义的尝试,这些研究大多集中在智能家居、物流和供应链等物联网数据隐私的高压区,提出了各种各样的模型,这些模型在安全性、交易处理效率、可用性等方面都有比较好的表现^[3-6]。

因此,如何结合区块链技术提高 SDN 物联网的安全性能是一个非常值得关注的研究课题。

2 基于 SDN 的物联网部署及其安全挑战

2.1 基于 SDN 的物联网部署

物联网是一项新兴技术,可利用异构技术实现智能生态系统。通常,配备有 RFID 标签、执行器、无线传感器或无线通信设备的物理设备连接到 Internet,以形成 IoT 网络。

SDN 是一种新型的网络架构,可通过编程而不是传统的系统管理方法管理网络节点,从而实现网络的虚拟化、可编程。其分层如图 1 所示。SDN 与物联网的结合具有非常大的潜力^[7]。首先,SDN 可以根据不同的 IoT 应用程序,设置不同的数据传输策略。这个来源于 SDN 的集中式管理和全局视野。其次,SDN 的许多方面都是动态的,包括服务质量(QoS)。交换器可以通过发出请

求并在网络内创建对数据包的优先处理来响应 QoS。这个特点对于物联网尤为关键。通过使用 SDN,网络可以弹性地处理这些变化的需求,从而动态地提供带宽。

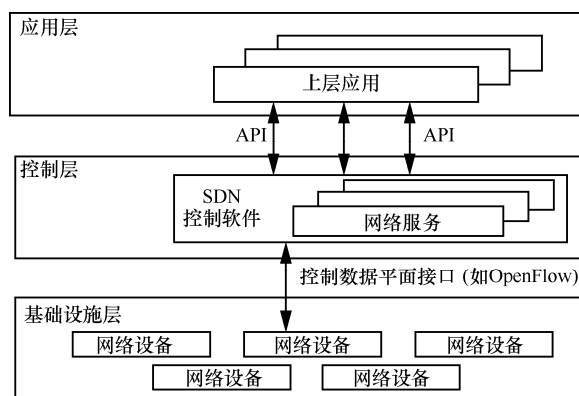


图 1 SDN 通用架构示意图

UbiFlow 框架^[14]实现了基于 SDN 的物联网部署,如图 2 所示,该框架使用 SDN 分布式控制器在移动性物联网多网络中进行有效的流量控制和移动管理。在 UbiFlow 架构中,物联网网络被划分为小的网络块/群集,其中每个分区都由一个物理上分布的 SDN 控制器控制,每个分区中的 IoT 设备可以连接到不同的访问点以进行不同的数据请求。这些分布式控制器协调工作,以一致、可靠和可扩展的控制顺序提供网络流的调度、移动性管理、最佳的接入点选择。同时,分布式控制器可以为多域 IoT 网络提供容错和负载平衡。SDN 控制器使用 UbiFlow 架构中的网络演算对网络进行分区,具备多网络管理能力,从而实现这些复杂的网络功能。

2.2 基于 SDN 的物联网部署的安全挑战

基于 SDN 的物联网由传统互联网发展而来,因此,与传统互联网相比较,它不仅继承了传统互联网时代遗留的安全问题,还有 SDN 物联网特有的安全问题。因此,基于 SDN 的物联网的安全问题更加复杂。

2.2.1 感知控制层

感知控制层的设备种类繁多,体积从小到大,

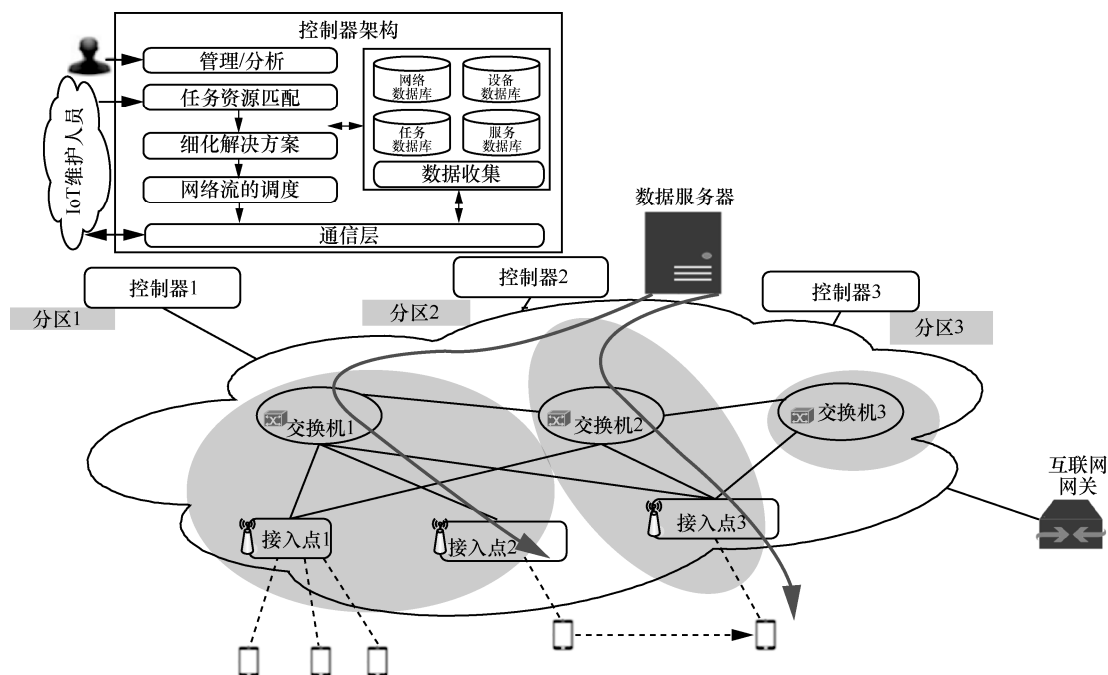


图2 UbiFlow 框架系统示意图

功能各异，状态或联网或断开，在其上面部署安全软件或者高复杂度的加解密算法会增加运行负担，甚至可能导致无法正常运行，加之许多物联网设备部署在无人监控场景中，攻击者更容易对其实施攻击。感知控制层的常见安全威胁包括：

- 窃听，它是一种未经授权的实时攻击；
- 节点捕获，攻击者获得对关键节点（如网关节点）的完全控制，这种攻击行为可能使所有信息被泄露，包括用于进行安全通信的密钥以及存储在内存中的信息；
- 恶意节点攻击，攻击者在其中向系统添加一个节点并输入虚假数据，旨在停止传输真实信息，攻击者添加的节点消耗了真实节点的宝贵资源，并可能进行控制以破坏整个网络；
- 定时攻击，通常发生于计算能力较弱的设备中，攻击者通过观察系统对不同查询的响应、输入密码算法所花费的时间等，发现设备漏洞并进行攻击。

2.2.2 网络互联层

网络层是感知层和应用程序层之间的桥梁，采用多种异构网络，通信传输模型与互联网相比更为复杂，因此，攻击面更广，攻击方式更多样化。而且，SDN 物联网架构采用 SDN 处理其复杂的网络基础架构，SDN 的控制逻辑集中化和可编程性也为网络层带来了新的安全挑战。网络层的常见安全威胁和问题如下。

- 拒绝服务（DoS）攻击，一种阻止真实用户访问设备或其他网络资源的攻击。通常，通过使用冗余请求向目标设备或网络资源泛洪实现此目的，以使某些或所有真实用户无法或很难使用网络资源。
- 中间人（MiTM）攻击，攻击者秘密地拦截并更改了发送方和接收方之间的通信，由于攻击者控制了通信，因此可以根据他们的需求随意更改消息，这对系统安全造成了严重威胁。
- 泄露/漏洞攻击，攻击者利用应用程序、系统或硬件中的安全漏洞，获得系统的控制



权并窃取存储在网络中的信息；

- SDN 控制器攻击，作为基础网络架构的 SDN 允许第三方在控制器上部署应用程序，有缺陷或有害的应用程序将具有重新配置整个网络的能力，一旦攻击者控制了 SDN 控制器，其后果将不堪设想。

2.2.3 物联网应用层

物联网的应用层可以提供诸多应用（如智慧城市、智慧家庭、智慧医疗、智慧交通等），从总体功能结构方面定义了所有采用 IoT 技术或者已经部署的 IoT 应用程序。不同的应用程序根据应用场景提供不同的应用服务，具体的服务内容又取决于传感器所采集的信息。

安全问题是物联网应用层中的核心关键点，常见的如下。

- 跨站点脚本注入攻击，它使攻击者能在其他用户查看的受信任站点中插入客户端脚本，例如 Java 脚本。这样，攻击者可以根据自己的需要完全更改应用程序的内容，并以非法方式使用原始信息；
- 恶意代码攻击，使用软件任何部分中的代码对系统进行破坏和攻击。这是一种可能无法通过使用防病毒工具阻止或控制的威胁。它既可以激活自己，也可以像需要用户注意才能执行动作的程序一样。

另外，目前很多的物联网应用采用云端部署的方式，物联网的终端通过网络连接云端服务，并上报相应的数据信息为云端应用层提供分析和管理的。对网络和设备的安全管理，以及在攻击发生时能够及时地响应和主动预警，是目前物联网云端部署模式下非常关键的技术点。对物联网应用层的威胁来自于内部管理或者外部的渗透、攻击等，若在管理流程和机制方面存在漏洞，尤其是近年来外部较多利用社会工程学发起非传统网络模式的攻击，如果应用层的系统被攻击，将可能带来整个生态链的危机。

3 区块链技术

3.1 区块链基本原理及架构

区块链本质上是一个数据不断增长的分布式交易账本^[9]，系统中存在的所有客户端节点的关系都是完全对等的，都保存一份相同的账本，账本中包含区块链系统中所有被确认过的交易，如图 3 所示，每个区块都指向上一个区块的哈希值，这样，所有的区块连成一条长长的链，这条区块连接成的链被称为区块链。区块链技术通过去中心化共识机制保证整个网络承认同一条链。由于每个区块都指向上一个区块的头哈希值，要想篡改一个区块的交易记录，必须重新计算该区块之后的所有区块。根据网络的算力以及现有的计算设备，一般一个区块后如果有 6 个区块，就很难被篡改了。

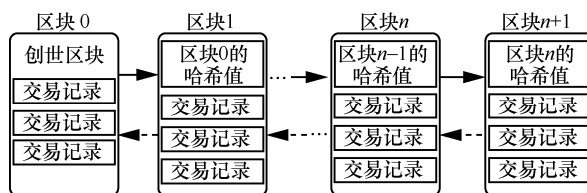


图3 区块链数据结构

区块链技术在架构上^[10]可以分为 5 层的层次结构，区块链的层次架构如图 4 所示。

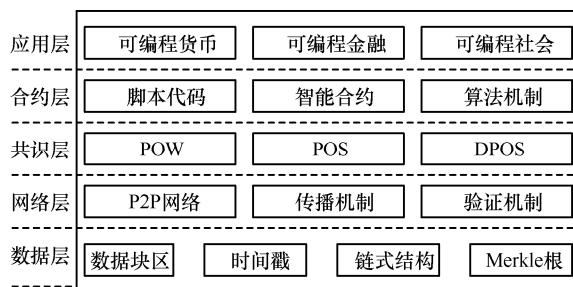


图4 区块链的层次架构

- 数据层：区块链是一个去中心化的、大规模复制的数据库（分布式分类账），其中交易按块排列，并放置在 P2P 网络中。所有账户的当前状态都存储在这样的数据库中。

- 网络层：也称为 P2P 层，负责节点间通信的层，它负责发现、事务和块传播。P2P 层确保节点之间可以发现彼此，可以彼此通信、传播和同步，以维护区块链网络的有效当前状态。
- 共识层：共识层是区块链最关键的层。共识负责验证块、订购块并确保每个节点都同意。共识方法因不同类型的区块链而异。这种共识保证了分类账的一致性，尽管各种参与者可能对区块有不同的看法。
- 合约层和应用程序层：封装了各类脚本语言、算法机制以及智能合约。合约层和应用层具有最终用户来与区块链网络进行交互的应用程序。对于这些应用程序，区块链网络是后端系统，它们通常通过 API 与区块链网络连接。合约层是构成智能合约、基础规则和链码的子层。该子层具有要执行的实际代码和已执行的规则。

3.2 区块链的特点

首先，区块链是一个分布式系统，这意味着不需要也没有中心机构可以控制该系统，这样可以防止攻击者通过访问和损坏存储在中心机构的特定计算机系统的内存和磁盘中的数据来攻击整个系统。而且，区块链的去中心化也可以消除聘请专家人员使用密码技术预防或阻止对系统的攻击的成本。区块链的去中心化可确保即使某些节点处于脱机状态或受到攻击时，系统也将照常运行。第二，区块链是透明的，区块链中的任何数据对于任何用户都是可见的，在区块链中进行的任何更改，系统中的所有用户都可以查看。第三，区块链中的交易是可追溯的，因为区块链中的所有交易均具有数字签名和时间戳，因此系统中的所有用户可以轻松地追踪历史。第四，区块链中的信息很难被篡改，一旦信息通过验证被加到区块链，这个信息就会永久地存储起来，除非能够同时控制系统中超过 51% 的节点，否则单个节点

上对数据库的修改是无效的。第五，区块链更加安全，因为区块链使用了很复杂的密码学，所以区块链比其他第三方系统能更安全地存储数据^[11]。

3.3 区块链技术与物联网技术的结合

随着区块链技术和物联网技术的不断发展，人们注意两者可以形成有效的互补关系。区块链被设计用于跟踪传感器测量的数据并防止任意恶意数据在系统中被复制^[12]。IoT 设备的部署可能很复杂，而分布式账本非常适合提供 IoT 设备标识、身份验证和无缝的安全数据传输。IoT 设备可直接通过区块链进行寻址，提供连接设备的历史记录以进行故障排除。物联网传感器也可以通过区块链交换数据，分布式账本消除了系统内的单一故障源，从而保护了物联网设备的数据免遭篡改。由于没有中介，因此可以通过区块链降低 IoT 的部署和运营成本。更进一步的，在物联网架构优化方面，Samaniego 等^[13]提出了将区块链技术整合至物联网网络的方法，并对此进行了分析；Dorri 等^[14]则提出了一个将区块链运用在物联网网络上的轻量级的架构。

4 采用区块链提升 SDN 物联网部署安全

4.1 安全网关在 SDN 物联网安全中的重要性

SDN 物联网云部署架构采用 SDN 处理其复杂的网络基础架构，同时还分布计算、控制和存储功能分配给最终用户设备。该部署架构的性能不仅受每个子系统的性能影响，还要看单独部署之间的跨云通信的效率和安全性。

具有 SDN 物联网支持的云部署都包括 3 个主要部分：执行核心 IoT 应用程序的 IoT 应用服务器（IoT 服务器）、SDN 和安全网关节点。只要通信通道可以在任意规定时间内运行，以稳定而连续地传输数据，那么将安全网关节点设置为连接可能位于拓扑视图中任何位置的传感器，传感器和 IoT 服务器之间的所有通信都首先通过安全



网关进行遍历，然后重定向到 SDN 节点，作为整个部署架构的第一道防线的安全网关处理所有的入口流量，以检测所有数据包的有效性。只要通过安全网关节点的消息流被完全信任，允许其在整个部署架构中通信，那么单个云部署内部通信和云部署间的通信就会更有效率。因此，如果安全网关节点能够以某种方式精确确认入口流量的真实性，那么该安全网关节点可以作为整个架构的第一道防线，所以提高安全网关节点的检测准确率在 SDN 物联网中至关重要。这就是新的区块链技术发挥作用的地方。

4.2 基于区块链的安全网关在 SDN 物联网部署的应用

使用区块链作为 SDN 物联网系统的主要分布式存档，无论该系统有多少个节点，一旦作为授权节点被记录在此数据结构中，均可立即跟踪和验证由物联网设备生成的数据。由于加密的分布式数据库具有弹性，且系统使用最新区块进行定期更新，因此访问该系统的任何活动节点可确保正确更新信息。一旦创建区块链，由于区块链技术的时间不可逆性和不可篡改性，采用算法可以对区块链的有效性进行连续验证和校准，同时立即标记尝试进行的对系统某一节点的篡改行

为。该特征使数据篡改攻击无效，从而保障了系统的安全性，因为恶意节点必须获得创世区块才能解密来自区块链的任何信息，而获得创世区块是一项基本上不可能的任务。

使用区块链的安全物联网云间通信如图 5 所示，在 SDN 物联网中加入一个基于区块链的安全层作为安全网关，该安全层使用区块链作为主要分布式存档。安全网关作为节点加入区块链系统如图 6 所示，各个安全网关以区块链成员的身份加入此区块链系统中，在该区块链系统中没有中心节点，每一个安全网关作为一个节点，所有节点都是平等的、并以去中心的方式达成共识，共同维护整个系统中的分布式账本。网关作为网络的入口点，对进入该网络的数据进行一次性的精确验证，当其验证通过时，即为其创建新区块并共识到整个区块链系统中，由此利用区块链系统的可追踪、不可篡改特性来保证整个物联网的通信安全。由于所有的传感器和节点都有访问创世区块的权限，当一个无害的数据包进入安全网关时，只需要检查其最新的区块，就可以即刻被归类为属于本区块链，这样使安全网关的身份验证工作变得非常直接，而不需要广泛的数据包审查（比较消耗 CPU 的一个动作），整个流

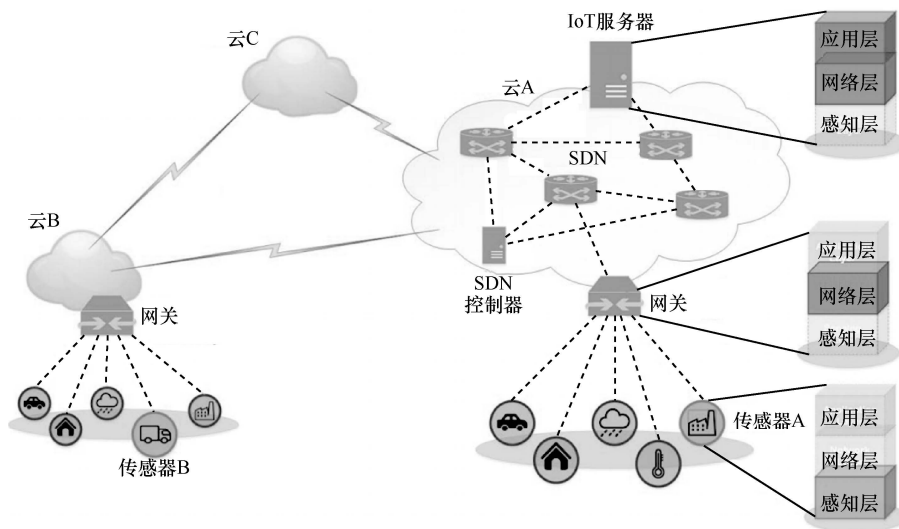


图 5 使用区块链的安全物联网云间通信

程可以很快结束,在安全得到了完全保障的前提下提高了通信效率。由于只要提供必要的创世区块的副本就能被授予对相邻云部署的访问权限,云间通信也将变得更加高效。因为区块链支持零信任网络,这种层面的透明和信任度甚至允许让云 A 的 IoT 服务器获取云 B 的传感器 B 信息。

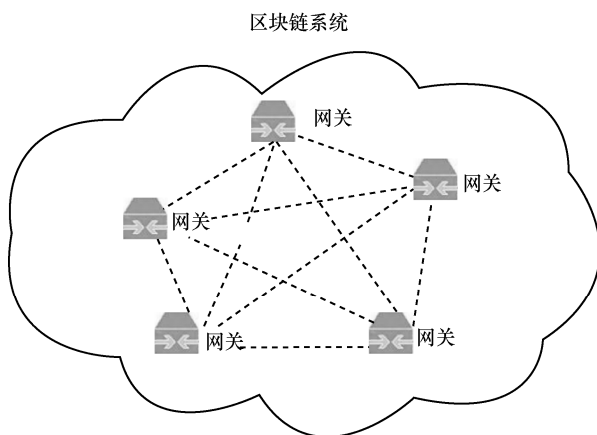


图 6 安全网关作为节点加入区块链系统

5 结束语

随着数字驱动的互联网世界高速发展,万物互联的概念越来越接近现实。在物联网设备数量呈爆炸式增长、同时 SDN 技术和区块链技术日益进步的情况下,SDN 物联网与区块链技术的结合已经成为非常值得关注的研究问题。

本文论述了基于 SDN 的物联网部署存在的安全挑战和区块链技术在解决安全问题方面带来的优势,并提出了在 SDN 物联网中加入一个基于区块链的安全层作为安全网关,以在提高 SDN 物联网部署安全性能的同时,提高整个物联网的通信效率。但目前区块链和 SDN 物联网仍处于起步阶段,因此,针对如何具体地在 SDN 物联网中设计一个基于区块链的安全层以及区块链的底层技术,尤其是共识算法研究等这些关键技术,还有待进一步深入探索,使区块链技术在 SDN 物联网安全领域可以得到更好的应用与发展。

参考文献:

- [1] DONOHO D L. Compressed sensing[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.
- [2] 黄泽源, 孔勇平, 张会炎. 基于区块链的物联网安全技术研究[J]. 移动通信, 2018, 42(12): 8-13.
HUANG Z Y, KONG Y P, ZHANG H Y. Research on security technology of internet of things based on blockchain [J]. Mobile Communication, 2018, 42(12): 8-13.
- [3] 李宣, 柳毅. 基于双区块链及物联网技术的防伪溯源系统[J]. 计算机应用研究, 2020, 37(11): 1-6.
LI X, LIU Y. Anti-counterfeiting traceability system based on dual blockchain and Internet of Things technology [J]. Application Research of Computers, 2020, 37(11): 1-6.
- [4] 花丽. 基于区块链技术的物联网安全探析[J]. 卫星电视与宽带多媒体, 2019(21): 39-40.
HUA L. Analysis of security of the internet of things based on blockchain technology [J]. Satellite TV and Broadband Multimedia, 2019(21): 39-40.
- [5] 陈烨, 许冬瑾, 肖亮. 基于区块链的网络安全技术综述[J]. 电信科学, 2018, 34(3): 10-16.
CHEN Y, XU D J, XIAO L. Summarization of network security technology based on blockchain[J]. Telecommunications Science, 2018, 34(3): 10-16.
- [6] 赵阔, 邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息安全, 2017(5): 1-6.
ZHAO K, XING Y H. A review of internet of things security research driven by blockchain technology[J]. Information Network Security, 2017(5): 1-6.
- [7] 王博伟, 谭劲, 蒋文斌. 一种基于 SDN 的物联网数据聚合方案[J]. 电信科学, 2019, 35(2): 27-34.
WANG B W, TAN J, JIANG W B. An SDN-based data aggregation scheme for the internet of things[J]. Telecommunications Science, 2019, 35(2): 27-34.
- [8] WU D, ARKHIPOV D I, ASMARE E, et al. UbiFlow: mobility management in urban-scale software defined IoT [C]//2015 IEEE Conference on Computer Communications (INFOCOM). Piscataway: IEEE Press, 2015: 208-216.
- [9] 张恩. 区块链技术原理、应用及建议[J]. 软件, 2016, 37(11): 51-54.
ZHANG C. Principles, applications and suggestions of blockchain technology [J]. Software, 2016, 37(11): 51-54.
- [10] 聂凯君, 曹侯, 彭木根. 6G 内生安全: 区块链技术[J]. 电信科学, 2020, 36(1): 21-27.
NIE K J, CAO B, PENG M G. 6G endogenous security: blockchain technology[J]. Telecommunications Science, 2020, 36(1): 21-27.
- [11] 袁煜明, 李骅熹, 蒋利峰. 区块链模式: 让多方协作实现共赢[J]. 清华管理评论, 2018(10): 64-69.



- YUAN Y M, LI Y X, JIANG L F. Blockchain model: let multi-party collaboration achieve a win-win situation [J]. Tsinghua Management Review, 2018 (10): 64-69.
- [12] 史锦山, 李茹, 松婷婷. 基于区块链的物联网访问控制架构[J]. 计算机应用, 2020(4): 1-13.
- SHI J S, LI R, SONG T T. Blockchain-based internet of things access control architecture[J]. Computer Applications, 2020(4): 1-13.
- [13] SAMANIEGO M, DETERS R. Blockchain as a service for IoT[C]//Proceedings of IEEE International Conference on Internet of Things. Piscataway: IEEE Press, 2017: 433-436.
- [14] DORRI A, KANHERE S S, JURDAK R. Towards an optimized BlockChain for IoT[C]//Proceedings of 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). Piscataway: IEEE Press, 2017: 173-178.

[作者简介]



谢萍（1989—），女，中国电信股份有限公司研究院工程师，主要研究方向为网络安全、网络大数据应用。



刘孝颂（1977—），男，中国电信股份有限公司研究院高级工程师，主要研究方向为网络数据分析/挖掘网络数据的应用安全。