计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191000157

面向5G的命名数据网络物联网研究综述

谢英英[1] 石 涧[1] 黄硕康[1] 雷 凯[1,2]
1 北京大学深圳研究生院信息工程学院深圳市内容中心网络与区块链重点实验室 广东 深圳 518055
2 北京大学互联网研究院(深圳) 广东 深圳 518055
(1701213646@sz.pku.edu.cn)

摘 要 在5G时代,大规模物联网应用对网络架构提出了异构性、可扩展性、移动性和安全性四大挑战。基于TCP/IP的网络架构存在IP标识与位置绑定的二义重载问题,难以应对这四大挑战。命名数据网络(Named Data Networking,NDN)将内容作为第一语义,具有网络层和应用层逻辑拓扑一致性。NDN对这四大挑战的支持分别体现在:网络层命名屏蔽了底层异构细节,端到端解耦及网络层缓存使得NDN天然支持多对多通信和广播,消费者驱动的通信模式为消费者移动性提供原生支持,面向内容的内生安全更轻量可信。文中总结了基于NDN构建物联网亟待解决的问题,并对NDN与边缘计算、软件定义网络和区块链结合来构建边缘存储和计算模型、集中式与分布式结合的控制模型、分布式安全模型提出了展望。

关键词:物联网;命名数据网络;5G;边缘计算;软件定义网络;区块链
中图法分类号 TP393

Survey on Internet of Things Based on Named Data Networking Facing 5G

XIE Ying-ying[1],SHI Jian[1],HUANG Shuo-kang[1] and LEI Kai[1,2]
1 Shenzhen Key Lab for Information Centric Networking & BlockChain Technology,School of Electronic and Computer Engineering,Peking University Shenzhen Graduate School,Shenzhen,Guangdong 518055,China
2 Internet Research Institute(Shenzhen),Peking University,Shenzhen,Guangdong 518005,China

Abstract Large scale Internet of Things (IoT) applications in the 5G era pose sever challenges on the network architecture in terms of heterogeneity,scalability,mobility and security. Due to the identification and location overloading problem of IP,TCP/IP based network architecture appears inefficient in addressing the challenges mentioned above. Named Data Networking (NDN) makes named content as the primary sematic and has consistency in logical topologies between network layer and application layer. The advantages of NDN in addressing these four challenges are reflected in the fact that naming shields the underlying heterogeneity,end-to-end decoupling and network layer caching provide native support for many-to-many communication and multicast,consumer mobility is supported natively by consumer driven communication pattern and content-based security is more lightweight. In this paper,future research directions of NDN based IoT were summarized. Especially,the combination of NDN and technologies including edge computing,blockchain and Software Defined Networking (SDN) to construct edge storage and computing model,centralized and distributed control model,distributed security model were proposed.

Keywords Internet of things,Named data networking,5G,Edge computing,Software defined networking,Blockchain

1 引言

物联网(Internet of Things,IoT)包含大量低能耗、低成本、存储与计算能力受限、经常休眠的设备,因此需要保证不同种类的感知设备和控制设备在异构环境下高效互联互通[1]。物联网应用的大规模部署与服务质量保障,不仅依赖于5G底层接入与传输技术的升级,还需要上层网络架构设计在异构性、可扩展性、移动性、安全性方面给予支持与适配。

(1)异构性。物联网异构性包括设备异构性和网络异构性。设备异构性指物联网终端设备在计算能力、存储空间、通信方式、能耗等方面存在差异性。网络异构性主要表现在[2]:不同无线频段的特性导致的频谱资源使用的异构性;设备所处不同网络间的组网接入技术所使用的空中接口及相关协议的差异性和不可兼容性;不同运营商所实施的不同运营管理策略等。

(2)可扩展性。可扩展性指随着设备数量、地址空间的增加,系统性能不会快速下降。其主要包括设备接入的可扩展性、命名及寻址的可扩展性、数据传输的可扩展性等。根据IDC的预测,2020年全球IoT设备将超过500亿台,全球IoT设备产生的数据将增长到4.4ZB[3]。海量IoT设备接入和海

到稿日期:2019-10-23 返修日期:2019-12-24 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
通信作者:雷凯(leik@pkusz.edu.cn)

量 IoT 数据传输，对物联网网络架构的可扩展性提出了严峻挑战。

(3)移动性。设备移动在物联网应用场景中呈现出普遍性和多样化的特点[4]，如车联网、无人机等。由于物联网终端设备具有异构性和性能受限性，物联网需要信令开销更小的移动性管理方案。

(4)安全性。物联网是信息世界与现实世界融合的重要渠道，在智能家居、健康监控等涉及大量个人隐私数据的物联网场景，安全和隐私保护尤为重要。IoT 设备的异构性和性能受限性进一步增大了 IoT 数据在完整性校验、用户访问控制、入侵防御等物联网安全和隐私保护方面的难度。

表 1 总结了应对物联网对网络架构提出的异构性、可扩展性、移动性和安全性这四大挑战时，传输控制协议/网际协议(Transmission Control Protocol/Internet Protocol，TCP/IP)网络架构的局限性和命名数据网络[5]具有的优势。为传统计算机网络设计的 TCP/IP 协议采用基于端到端连接的通信方式，IP 寻址方式将标识与位置绑定在一起。基于 TCP/IP 协议的 IoT 网络架构对异构性、可扩展性、移动性、安全性的支持是通过打补丁的方式实现的，解决方案的效率低下。IP 采用单一最佳路径路由来防止循环，而且一个由五元组标识的 TCP 连接只能绑定到单个 IP，因此 TCP/IP 不支持异构网络接口的并行转发；IP 下的多播依赖拓扑维护机制，应用层缓存可用性差，因此传输效率低下，可扩展性差；标识与位置绑定的特性导致 IP 难以支持移动性，依赖路由全网更新来反映节点移动存在滞后性；TCP 基于通道的安全机制无法保障内容本身的安全性，而且存在建立和维护安全通道的开销问题。

表 1 应对物联网四大挑战时 TCP/IP 网络架构的局限性和 NDN 网络架构的优势的对比

Table 1 Comparison of TCP/IP and NDN facing four major challenges of IoT

5G IoT 挑战	TCP/IP 网络架构的局限性	NDN 网络架构的优势
异构性	不支持异构网络接口并行传输：1)IP 采用单一最佳路径路由，只能单接口转发；2)TCP 连接由五元组标识，只能绑定到单一 IP	支持异构网络接口并行传输和异构设备共存：1)Nonce 字段防止循环，可以多接口转发；2)命名隐藏底层异构细节，提供统一接口
可扩展性	传输效率低下：1)多播依赖于拓扑维护机制；2)应用层缓存可用性差	兼容异构网络和异构设备，且传输效率高：1)天然支持多播和多对多通信；2)高可用的网络层缓存
移动性	无直接的移动性支持能力：1)IP 地址将标识与位置绑定；2)路由全网更新周期长，反映节点移动滞后	天然支持消费者移动，移动切换时延小：1)命名将标识与位置解绑；2)消费者驱动的通信模式，天然支持消费者移动；3)网络层缓存有利于降低移动切换时延；4)路由和转发平面分离，及时反映节点移动
安全性	基于通道的安全机制：1)建立安全通道存在时延；2)维护安全通道给受限 IoT 设备带来了计算和存储负担；3)无法保障内容离开通道之后的安全性	基于内容的安全机制：1)保障内容本身的安全；2)内容可信性与主机可信性、通道可信性分离；3)语义化细粒度安全

NDN 作为一种以内容为中心的新一代网络体系架构，摒弃了类似于 IP 地址的位置标识，直接对数据本身进行命名和寻址，具有应用层语义和网络语义一致性[6]。在 5G 大规模物联网业务下，NDN 可以提供对异构性、可扩展性、移动性和安全性的高效支持，具体表现在以下 4 个方面。(1)Interest 包的无环路路由保障和命名机制对底层异质网络的差异性屏蔽，使得 NDN 支持异构网络接口和异构 IoT 设备；(2)在未来上百亿 IoT 设备接入和海量 IoT 数据传输压力下，网络层缓存和端到端解耦使得 NDN 天然支持多播和多对多通信，有利于提高 IoT 数据的传输效率，进而提高可扩展性；(3)NDN 用数据命名取代 IP 地址，标识与位置的解绑使得 NDN 天然支持 IoT 设备移动；(4)NDN 遵循安全与数据绑定原则，相比基于通道的安全机制，基于内容的安全机制更加轻量级和可靠，并且支持语义化定制安全策略。

基于 NDN 的物联网的未来研究可以分为两个方面：(1)应对 NDN 多维命名检索、轻量级路由和分布式同步等功能性方面的研究挑战。多维命名检索相比最长命名前缀匹配，增加了命名匹配的难度；轻量级路由对于无基础网络设施的物联网环境至关重要；NDN 实现分布式同步的挑战在于，分布式同步中推送数据的通信需求与 NDN“拉”数据的通信原语相矛盾。(2)探索 NDN 与其他技术的结合，在计算和存储模型、控制模型、安全模型上进行创新。在计算和存储模型方面，边缘计算(Edge Computing，EC)[7]利用靠近网络边缘侧设备的计算和存储能力，在提供低时延保障的同时，减轻主干网带宽压力，这将成为物联网体系架构中必不可少的部分，而边缘计算中的服务发现可以受益于 NDN 基于命名的寻址方式；在控制模型方面，NDN 采用完全分布式控制，而软件定义网络(Software Defined Networking，SDN)[8]提供了网络的集中控制能力，两者的结合有利于平衡控制时效性与全局最优性；在安全模型方面，区块链[9]作为一种去中心化的可信任分布式系统，可以与 NDN 基于内容的安全机制相结合，从而加强基于 NDN 的物联网安全性。

5G 和 IoT 相关的综述请见文献[10-12]，这些综述的重点在于对比和分析了适用于 IoT 的各种 5G 通信层技术。IoT 和 NDN 相关的综述请见文献[13-15]，这些综述的重点在于总结了面向 IoT 的 NDN 命名、转发策略、缓存策略、信任模型等方面的研究。与上述工作相比，本文的创新之处体现在两个方面：1)面向 5G 通信技术的升级，本文从网络层的角度系统性地分析了 IoT 网络架构设计面临的挑战，并分析和总结了 TCP/IP 网络架构的局限性与 NDN 网络架构的优势，为 IoT 网络架构的选择提供了理论性指导；2)近年来，边缘计算、SDN、区块链得到了广泛且成功的应用，本文分析了将边缘计算、SDN、区块链应用于基于 NDN 的物联网的可能研究方向。

首先，简要介绍了面向 5G 的物联网、NDN 的背景知识；然后，针对 5G 大规模物联网应用对网络架构提出的异构性、可扩展性、移动性、安全性这四大挑战，分析了 TCP/IP 网络架构应用于物联网的主要缺陷及现有解决方案；接着，对应分

析了基于 NDN 构建的物联网在应对以上四大挑战时的主要优势和研究进展；最后，总结了基于 NDN 构建物联网亟待解决的研究问题，并提出了 NDN 与边缘计算、SDN 和区块链技术结合的必要性以及可能的研究方向。

2 背景

2.1 面向 5G 的物联网

下一代移动通信网络——5G 应服务的三大应用场景包括增强移动宽带（enhanced Mobile Broadband，eMBB）、大规模机器类通信（massive Machine Type Communications，mMTC）和超高可靠低时延通信（ultra-Reliable and Low Latency Communications，uRLLC）[16]，其中后两者都属于物联网应用场景，如图 1 所示。物联网是指通过信息传感设备，按照约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络[2]。

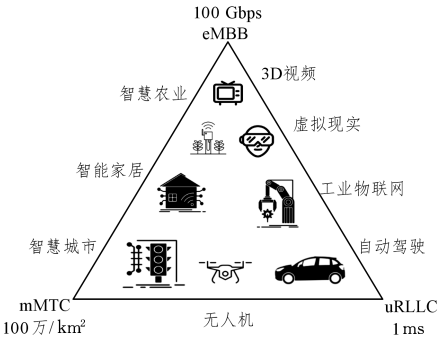

图 1 5G 的三大应用场景

Fig. 1 Three application scenarios of 5G

5G 的发展和实际部署使得实现真正意义上的“万物互联”具备了接入和传输的通信层基础。在 5G 支持大规模物联网应用的技术标准进展方面，2018 年 6 月完成的 Rel-15 5G 标准支持 eMBB 和 uRLLC，而满足 ITU 全部应用场景要求的 Rel-16 5G 标准预计于 2020 年完成[17]。2018 年 3 月召开的 3GPP 无线接入网第 79 次全会，针对 Rel-16 的提案明确了将通过继续演进窄带物联网（Narrow Band Internet of Things，NB-IoT）[18] 和增强机器类通信（enhanced Machine Type Communications，eMTC）[19] 来支持 5G mMTC 应用场景。NB-IoT 和 eMTC 都属于低功耗广域网技术（Low Power Wide Area，LPWA），在授权频谱上工作，基于移动蜂窝网络部署，关注物联网设备大连接、广覆盖、低功耗、低成本的通信需求[20]。eMTC 在数据传输速率和移动性支持方面具备优势，而 NB-IoT 在部署灵活性、成本、功耗方面更胜一筹，两者互补。不同 IoT 应用可以根据对移动性、功耗、传输速率的需求选择相应的 LPWA 技术。

2.2 命名数据网络

针对当今用户对互联网的核心需求从端到端连接转变为内容分发这一现状，NDN 在整体架构上以内容本身为中心，可寻址对象不仅包括设备终端，还包括内容对象、服务程序、用户指令等。如图 2 所示，NDN 网络架构沿用了 TCP/IP 网络架构的“沙漏”模型，但是“瘦腰”部分（IP 层）在 NDN 中被命名数据所代替，通过检索和匹配数据命名来转发和获取数据。NDN 采用 Interest 包和 Data 包一一对应的“拉”数据通信原语，每个转发节点维护转发信息表（Forwarding Information Base，FIB）、请求等待表（Pending Interest Table，PIT）和内容仓库（Content Store，CS）3 种数据结构。

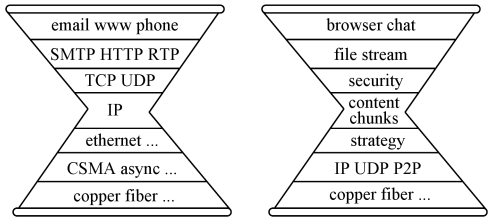

图 2 TCP/IP 及 NDN 沙漏模型的比较[21]

Fig. 2 Comparison of hourglass model of TCP/IP and NDN[21]

NDN 体系架构的设计遵循以下原则[21]。

（1）保留“沙漏”模型。TCP/IP 网络架构设计的成功之处在于其“沙漏型”体系。在“沙漏型”网络架构设计中，通用的网络层以最少的功能实现全局的互联互通，上层和下层的技术创新不需要考虑不必要的网络层限制，因此 NDN 延续了“沙漏型”网络架构设计。

（2）内置的安全机制。TCP/IP 网络架构在设计之初并没有考虑安全性问题，安全机制是以打补丁的方式补充到网络架构中的。NDN 提供内置的基于内容的安全机制，通过数据签名和验证来保障数据的可靠性和完整性，应用程序可以建立细粒度、定制化的认证、授权和信任模型。

（3）流量自调节机制。TCP/IP 网络架构中，网络层 IP 协议的数据交付方式是开环的，需要传输层 TCP 协议提供流量调节功能。在 NDN 中，Data 包和 Interest 包是一一对应的，而且每个网络节点都可以根据转发策略进行智能转发，从而在不依赖传输层的情况下，NDN 也可以提供单跳粒度的网络流量控制。

（4）路由和转发平面分离。NDN 采用路由和转发分离的设计，这使得路由和转发可以分别提供不同粒度的网络调控能力。这种设计的另一个优点是降低了系统耦合度，有利于路由机制和转发机制分别独立创新。

3 基于 TCP/IP 构建物联网的局限性

目前的物联网架构大多基于 TCP/IP 协议（特别是 IPv6），国际互联网工程任务组（Internet Engineering Task Force，IETF）为使 TCP/IP 协议适应物联网场景而对其做了许多扩展，但没有从根本上解决问题。为了使 IPv6 适配物联网低功耗链路层协议（如 IEEE 802.15.4，Bluetooth LE 和低功耗 Wi-Fi）的 MTU 限制，在链路层和网络层之间加入了适配层，即 6LoWPAN 协议[22]，以提供 IPv6 头部压缩和链路层分片功能；TCP 协议提供基于通道的按序和可靠传输服务，但是 TCP 执行按序交付所造成的重传会进一步增大时延，而且 TCP 维护传输通道的开销相对于要传输的 IoT 数据量来说太大，因此目前许多 IoT 应用在传输层采用 UDP 协议，而由应用层协议（如 CoAP[23]）选择性地实现定制化可靠传输功能。本节将分别从异构性、可扩展性、移动性、安全性 4 个方

面，来分析将 TCP/IP 应用于 5G 大规模物联网业务的挑战，并对 IETF 的多种解决方案进行评价。

3.1 异构性

在物联网场景中，任何一种单一的无线接入网络都无法提供无处不在的网络覆盖和全方位的服务，因此终端往往配置了多个网络接口来实现多模化，以保证全网接入性。在网络异构性方面，主要考虑 TCP/IP 协议对多网络接口并行使用的能力。对于 IP 协议，IP 下的路由机制通常采用单一最佳路径路由来防止循环，因此不能将一个 IP 包同时从多个网络接口转发出去。多路径路由[24]解决了多路径发现、多路径选择和多路径流量分配三大问题，提供了多路径转发能力，但是多路径转发通常比单一最佳路径路由选择的路径更长，且多路径发现和多路径维护需要引入额外的控制信令开销，中间节点无法识别并丢弃重复 IP 包。对于 TCP 协议，TCP 连接由源 IP、源端口、目的 IP、目的端口、上层协议五元组标识，因此一个 TCP 连接同时只能利用单个网络接口的传输能力。传输层多路径协议可以同时利用多个网络接口进行多路径传输，多路径 TCP(Multi-path TCP，MPTCP)[25]是目前主流的传输层多路径协议，在兼容 TCP 协议的基础上，在 TCP 层和应用层之间加入 MPTCP 层，用于提供多路径管理、数据包调度、拥塞控制服务，并对应用层透明。综上，需要在 TCP/IP 协议的基础上引入复杂的控制机制才能实现对多网络接口的并行使用，这会对性能受限的物联网终端设备造成额外的开销。

3.2 可扩展性

伴随着上百亿物联网设备的接入，网络信息的传输压力将进一步增大。网络架构对可扩展性的支持主要体现在传输效率上，多播和缓存是提高传输效率的两大方式，然而 TCP/IP 协议下的多播效率低，应用层缓存可用性差。

相比互联网，TCP/IP 协议在物联网场景下高效地支持多播是一个更大的挑战，原因包括以下 4 点[26]。(1)很多无线链路层协议并不支持对多播的确认帧(ACK)，因此丢包在链路层无法恢复；(2)物联网的设备异构性及网络异构性，使得节点设备可能分别运行在不同链路层协议之上，而各链路层协议数据的传输速率各有差异，因此要求多播发送者使用所有接收者中的最低传输速率进行传输；(3)物联网中的设备可能经常进入休眠模式以提高续航能力，这些休眠节点可能错过多播包；(4)多播包要在多条路径上进行转发，可能会唤醒路径上的休眠节点，这会显著降低物联网节点的续航能力。

传统的 IP 多播协议通常依赖拓扑维护机制，使多播组所有订阅用户发现和维护路由[27]。由于低功耗和有损无线网络的资源约束和网络拓扑动态变化，维持多播路由拓扑的代价难以接受。一种解决思路是将多播域限制在指定的某些节点，如 IETF ROLL WG 提出的 MPL(Multicast Protocol for Low-Power and Lossy Networks)[28]协议(该协议已被列入 Zigbee 的 IP 协议标准)。指定某些节点为 MPL 转发器，无须构建或维护任何多播路由拓扑，MPL 使用可控的泛洪将多播消息通过同步机制传播到 MPL 域中的所有 MPL 转发器。另一种解决思路是用点对点传输代替多播，代表算法有 IPv6 邻居发现(Neighbor Discovery，ND)算法的物联网适配版。节点需要发送多播包时，将多播数据包临时存储在某些已知位置的节点上，接收者基于休眠时间表选择合适的时间从这些已知位置的节点提取多播包。设备节点希望通过多播包进行查询时，可将查询发送到一些被预先配置为通过收集信息来回复查询的指定节点。这两种解决方式以损失多播效率为代价来实现多播功能，而且中间节点的引入带来了安全性问题。

物联网时断时续的动态网络环境使得通信双方难以维持稳定的连接，其通常依赖应用层缓存和代理来实现有效的数据交换。在被代理节点休眠期间，代理节点可以代表休眠节点请求资源、临时缓存数据和应答其他节点的请求，这有利于缩短响应等待时间。但在物联网环境中实现应用层缓存存在以下限制：(1)代理节点是预先配置的，随着网络环境的动态变化，这些预先配置的代理节点可能并不是当前环境下的最佳选择；(2)节点需要利用资源发现机制按需找到附近的代理节点，这种资源发现机制带来了额外的复杂性和开销；(3)在动态网络环境中，预先选择的代理节点可能变得完全不可达，这时节点需要重新发现和配置代理节点；(4)代理节点的引入存在极大的安全问题。为了增强物联网环境中缓存的可用性和灵活性，网络架构需要在网络内提供普遍的高速缓存，允许应用在不造成额外配置和通信开销的前提下使用它们。这要求网络层可以感知应用层资源并将缓存集成到转发过程中，还需要对网络安全模型进行根本性修改，以保障网络层缓存的安全可靠。

3.3 移动性

移动性问题大量存在于物联网场景中，如车联网、物流管理等。IP 地址将标识与位置绑定，获取内容时必须首先通过标识找到内容源，若内容源移动，根据原来的标识将无法找到该内容源。移动 IP 协议(Mobile IP，MIP)是 TCP/IP 网络架构的移动性解决方案。当移动终端从归属地移动到另一地点时，移动节点需要将其转交地址注册到归属地代理。发往该移动终端的数据包首先被路由到归属地代理，再由归属地代理路由到转交地址。移动终端在发送数据时可以将数据直接路由到网络中，也可通过归属地代理完成。MIP 协议这种移动性解决方案采用映射机制，存在数据报转发低效的问题，同时终端移动过程中的安全性得不到保证，易产生三角路由问题(Triangle Routing Problem)。

3.4 安全性

TCP/IP 网络架构通过在通信双方之间提供安全的端到端通信通道(如 TLS[29]和 DTLS[30])来保障数据传输的安全性，如 CoAP 协议[23]允许受限节点选择代理节点访问和缓存数据，在代理节点与资源所有者之间建立基于 DTLS 的安全通道。基于通道的安全模型不适合物联网场景的原因包括 3 点：(1)在发送数据之前，需要几轮握手以认证信道并协商安全参数，建立安全通道的开销对于低延时数据传输将是难以容忍的；(2)安全通道的两端必须维持通道的状态直到通道关闭，维护通道的开销会对存储和计算能力受限的物联网设备造成巨大的压力，特别是当物联网节点需要同时与多个节点保持通信时；(3)基于通道的安全不能保证数据离开通道之后的安全性，例如当数据被缓存时，数据归属者失去了对数据的

访问控制能力，只能依赖于缓存节点提供安全保障机制。

针对基于通道的安全模型的局限性，IETF 提出了一种基于对象的安全模型(Object Security of CoAP，OSCOAP)[31]。该方案不保护数据传输通道，而是直接保护 CoAP 协议应用层的数据单元。每个数据对象携带必需的认证信息(如数字签名)，使得数据接收者可以核实数据的有效性。数据归属者可以加密数据内容，使得只有合法的接收者可以对数据进行解密和访问。OSCOAP 与 NDN 基于内容的安全机制的区别在于，NDN 将安全机制构建到网络层，网络中的转发和路由设备也可以对数据进行安全鉴定，而 OSCOAP 属于应用层安全机制。

4 基于 NDN 构建物联网的优势

从网络架构设计角度分析，NDN 可以更高效地应对 TCP/IP 网络应用于物联网所面临的技术挑战。如图 3 所示，物联网网络的“瘦腰”从 TCP/IP 网络中的以位置为中心转变为 NDN 中的以数据为中心，通信方式从面向连接转变为面向内容。NDN 构建物联网的优势已被实际部署效果所验证。文献[32-33]基于 NDN 网络构建了家庭物联网 demo，通过与基于 TCP/IP 的物联网协议栈 6LoWPAN/RPL/UDP 比较，证明了基于 NDN 构建的物联网在能耗、传输数据包数量、内存效率等方面具有优势。文献[34]在单跳和多跳场景下将 NDN 分别与基于 IP 的物联网应用层协议 CoAP 和 MQTT 进行比较，结果发现基于 NDN 的部署方案更加轻量级，而且在多跳场景下具有更强的可靠性。下文将分别从网络异构性、可扩展性、移动性、安全性 4 个方面具体分析将 NDN 网络应用于物联网场景的主要优势，并总结相关研究进展。

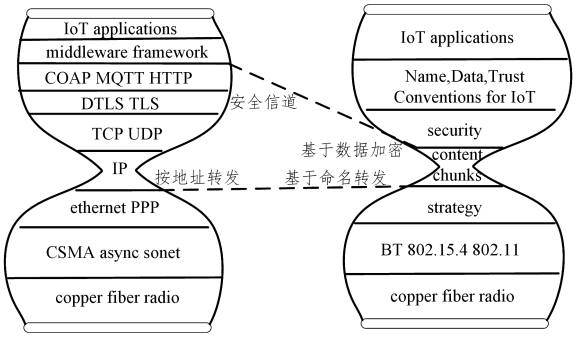

图 3 基于 IP 与基于 NDN 的物联网协议栈对比[13]

Fig. 3 Comparion of IoT protocal stack based on IP and NDN[13]

4.1 异构性

NDN 对物联网网络异构性和设备异构性的支持主要体现在以下两个方面。(1) NDN Interest 包的 Nonce 字段保证了 Interest 包的传输不会出现回路，由于 Data 包沿着 Interest 包的反向路径传输，因此也不可能形成环路，这使得 NDN 无需额外的协议补充就可以支持多路径传输，这也是 NDN 能够同时利用多网络接口转发的原因；(2)NDN 的命名机制隐藏了底层的异构设备和异构网络细节，暴露给上层的是统一的接口，因此上层应用设计者无须关心底层设备和网络的异构性，只须调用 NDN 提供的统一接口便可实现通信。物联网中存在大量异构设备及异构网络，NDN 支持异构设备、异构网络协同工作的这一特性有利于实现物联网中不同设备和网络之间的互操作性，进而提高可扩展性。Interest 包和 Data 包的直接交互不增加额外的协议数据传输开销，相比 TCP/IP 为支持物联网异构性而增添许多复杂控制机制的实现方式，NDN 对物联网异构性的支持不增加额外的网络传输负担，网络整体效率更高。

4.2 可扩展性

可扩展性体现在对异构设备和异构网络的兼容能力和传输效率两方面。4.1 节指出 NDN 天然支持多播并支持异构设备和网络，这两大特性有助于提高可扩展性。此外，NDN 的网络层缓存有助于提高传输效率，进而增强可扩展性。NDN 的网络层缓存功能使得节点可以根据缓存策略缓存经过它的内容，后续的相同请求可以迅速地在就近节点获取内容副本[35]。NDN 还可以为数据提供长期托管存储的持久性数据存储库[36]。网络内的缓存虽然有利于减少数据的重复传输，但是在 IoT 节点运行缓存策略和缓存替换策略时必然使得 IoT 设备在存储、计算、能耗等方面付出代价。针对 IoT 场景下部署网络内缓存的有效性问题，文献[37]在真实 IoT 设备上评测和比较了若干现有 NDN 缓存策略。实验结果表明，在 IoT 环境下，即使是最简单的无状态缓存策略，也能达到与其他复杂缓存策略近似的效果，从而证明了在 IoT 节点上部署有效网络内缓存的可行性。

物联网环境下 NDN 缓存策略和缓存替换策略的设计需要结合物联网特性(包括节点休眠特性、数据时效性特征、节点性能受限性和差异性等)，平衡缓存命中率与节点能耗。缓存算法 CoCa[38]的设计结合了节点休眠周期，在降低节点能耗的同时使缓存命中率达到 90%以上。物联网数据的时效性一般较强，例如在传感器周期性监测环境参数的场景下，随着新传感数据的产生，需要对缓存的历史数据做失效处理，缓存替换策略的设计应该将数据时效性考虑在内。在同一个物联网部署环境中，各个物联网终端设备的计算、存储、能耗可能存在差异，缓存节点的选择在考虑单个节点特征的同时还应该平衡各个节点的能耗，从而最大化全网节点的平均寿命。

4.3 移动性

NDN 的命名将标识与位置解绑。NDN 对移动性的原生支持体现在以下 3 个方面：(1)消费者驱动的通信模式，NDN 通信由消费者通过 Interest 包发起，消费者移动之后可以发起新的通信来获取数据包；(2)网络内缓存，Interest 包可以由最近的缓存所满足，不需要被转发到生产者，这有利于降低切换时延；(3)路由和转发平面分离，节点移动触发路由机制全网更新路由表的周期较长，而 NDN 的转发可以更及时地更新策略以反映节点的移动。NDN 移动性研究分为消费者移动和生产者移动两个方面。

4.3.1 消费者移动

为了缩短消费者移动后重新发起通信带来的切换时延，文献[39]提出基于代理的方案来解决消费者移动问题。移动节点显式地指明代理节点，并且只需与代理节点相连，代理节点负责管理移动节点。移动节点向代理节点请求数据，当检测到移动节点移动后，代理节点将缓存原移动节点请求的数

据包。移动节点完成移动后，向代理节点发送 Interest 包，以请求之前缓存的数据包。代理节点处于移动节点原路径与移动路径的相交位置，协助移动节点实现了移动后数据的获取。文献[40]提出基于主动缓存请求信息的思想来选择邻居节点缓存(Selective Neighbor Caching，SNC)的方案，以处理消费者移动问题。移动消费者在移动之前，选择恰当的邻居节点主动缓存其请求的数据。当消费者移动到预测节点后，可直接从已经缓存数据的邻居节点中获取数据，降低了切换时延。

4.3.2 生产者移动

当生产者移动时，物联网中路由节点 FIB 表中对应此生产者的表项失效，Interest 包将根据失效的 FIB 表项路由到生产者原位置，因此无法获得数据。生产者移动问题的解决方案可以分为两大类：数据仓库型和追踪生产者型。数据仓库型方案的基本思想是将移动生产者生产的数据存储到一个不移动的数据仓库，消费者的数据请求由数据仓库满足。文献[41]通过维护 CET(Custodian-to-Endpoint Table)映射，实现了对数据仓库的移动性支持。追踪生产者型方案又细分为 3 种：基于映射的方案、基于追踪的方案和基于路由的方案。基于映射的方案中，由映射服务器维护数据命名前缀和移动生产者可路由命名前缀之间的映射，生产者移动仅改变可路由命名前缀，而数据命名前缀不变，因此消费者可以通过数据命名前缀向代理服务器请求可路由命名前缀，重新构造 Interest 包；基于追踪的方案中，代理服务器维护路由到移动生产者的路由信息，并且代理服务器向网络广播移动生产者的数据命名前缀，消费者的 Interest 包路由到代理服务器之后再路由到移动生产者；基于路由的方案由移动生产者在移动到新位置之后通过 NLSR 协议向全网广播名字前缀，更新 FIB 表，触发全网路由表重新收敛[42]。

4.4 安全性

NDN 将内容可信性与主机可信性、通道可信性分离，通过维护名字与内容的安全绑定来保证内容本身的安全。这种基于内容的安全模型从根本上解决了内容安全问题，不存在维护内容安全传输通道的开销，是构建网络层缓存的基础。NDN 强制要求生产者对发送的每个 Data 包签名，消费者对接收到的每个 Data 包进行签名验证，NDN 路由器是否执行签名验证是可选的。Data 包的签名范围包括名字、内容主体和一些对签名验证有用的信息(Singned info 域)。Data 包的 KeyLocator 域指示了执行签名验证的公钥名称。除了获取指定的公钥和执行签名验证之外，消费者还对数据名称和密钥名称进行匹配校验，以验证密钥的合法性。

在物联网场景下，NDN 基于内容的安全机制研究还需要解决以下研究问题。(1)鉴于物联网设备的计算、存储和能耗限制，需要研究轻量级的签名生成和验证算法、加密和解密算法。椭圆曲线密码学[40](Elliptic Curve Cryptography，ECC)可以使用更短的密钥实现同等或者更高级别的安全性。相对于 RSA 算法[41]，ECC 在同等安全级别下进行加密和解密的速度更快，是一种更适合受限物联网设备的密码学算法。(2)目前 NDN 只对 Data 包进行签名和验证，缺少针对 Interest 包的安全保障机制。在工业物联网、智能家居等包含设备控制需求的物联网场景中，Interest 包通常包含了对物联网设备的控制请求，因此需要验证 Interest 包的合法性。将安全验证信息附加到 Interest 包名称中的方式增加了 Interest 包名称的长度，而且破坏了 Interest 包名称的语义性。

5 NDN 物联网未来的研究方向

鉴于物联网设备性能受限的特征以及普遍存在的多维度数据检索、数据同步需求，NDN 物联网研究未来需要应对轻量级路由、多维命名检索、分布式同步等方面的挑战。结合边缘计算、SDN、区块链在物联网中的广泛应用前景，表 2 总结了 NDN 物联网未来的研究方向及挑战。

表 2 NDN 物联网未来的研究方向及挑战

Table 2 Future research directions and challenges of NDN based IoT

研究方向	研究挑战
轻量级路由[43]	FIB 储存条目受限；NDN 命名的字符串匹配计算开销
多维命名检索[44-45]	命名组合数随维度的增加呈几何倍增长；多维命名任意组合的互相匹配
分布式同步[46]	基于 Interest-Data 通信原语的推送通信方式；轻量级数据集摘要数据结构
基于 NDN 的边缘计算[47-51]	PIT 超时时间与边缘计算响应时间不匹配；多 NDN 边缘计算节点协作的参数传递方案
集中式与分布式相结合的控制模型[52-53]	控制器的分布式部署方案；控制平面与数据平面的低时延通信
基于区块链的跨域分布式安全[54-55]	物联网数据的选择性上链；链上数据查询和物联网安全攻击识别的实时性；区块链系统在高动态性物联网环境下的稳定性

5.1 轻量级路由

NDN 有状态的路由转发机制要求每个节点维护 FIB 表、PIT 表和 CS 3 个数据结构。在多数 IoT 场景下，并没有专门的基础网络设施对路由提供支持，仅仅依靠计算和存储能力受限的物联网设备进行路由存在巨大的挑战，具体表现在两个方面。(1)由于节点存储能力的限制，物联网设备无法缓存大量数据，FIB 的条目也将受到限制。一种解决资源受限物联网节点路由问题的思路是将路由信息嵌入命名中，充分利用 NDN 命名的语义协助智能转发机制实现路由。(2)与基于 IP 地址路由相比，基于内容命名路由具有将应用层语义一定程度地下放到网络层的优势，但是将 IP 地址的比特位匹配转换成字符串匹配时增大了路由的计算开销。降低计算开销的可行方法是通过硬件方案或者软件方案进行字符串匹配加速，并根据内存容量、处理速度需求谨慎选择前缀树的粒度[43]。

5.2 多维命名检索

应用程序希望同时通过多个维度来检索数据，这一需求在物联网场景中普遍存在，如在智能家居场景中检索特定房间(位置维度)的特定温度数据(温度维度)，同时通过位置和温度两个维度检索数据可以简化上层应用的数据检索步骤。NDN 的最长命名前缀匹配机制支持一维命名检索，而在支持多维命名检索方面存在巨大挑战，其原因是：(1)多维命名检索中可能的组合数量随着名称中组件数量的增加呈几何式增长；(2)难以保证多维名称的任意组合在路由器 FIB 表中都存在，因此需要支持多维命名任意组合的互相匹配。NDN 多维命名检索研究的难点在于将多维信息嵌入 NDN 层次化命名中，并且设计支持命名多维信息匹配的转发和路由机制。

NDN 多维命名检索研究已经受到了部分学者的关注。文献[44]受 TagNet[45] 设计思想的启发，提出了一种基于关键字的 NDN-IoT 命名和路由设计方案，该方案支持利用多个关键字对物联网数据命名、请求、转发和路由，并且在物联网边缘对多个有关联的数据进行聚合。

5.3 分布式同步

分布式同步是生产和维护一个共享数据集的多方通信模式，是发布/订阅通信模式在多发布者情况下的升级。分布式同步在 NDN 中表现为多个生产者分别生产同一个命名前缀下的部分内容，并且保障每个生产者对全数据集同步。分布式同步在灾难场景的多传感器合作、工业物联网的多控制器协同等物联网场景中被广泛应用。

在 NDN 中实现适合物联网场景的分布式同步方案有两大挑战。(1)在不违背 NDN 的 Interest-Data 通信原语的前提下实现基于推送的通信方式。NDN 定义了基于消费者驱动的“拉”数据传输模型，生产者一旦产生数据，需要保持在线并等待数据请求，但是基于推送的通信方式具有更高的数据同步效率，更加适合分布式同步场景。(2)选择适合受限物联网设备的轻量级数据集摘要数据结构。需要考虑数据集摘要计算和查询开销，而且数据集摘要一般作为 Interest 包名字的一部分，因此数据集摘要的大小受限于链路层 MTU 的限制。现有的 NDN 分布式同步方案包括 CCNx 0.8 Sync，iSync，CCNx 1.0 Sync，ChronoSync，RoundSync 和 PSync[46]，采用的数据集摘要数据结构包括哈希树、可逆布隆过滤器。

5.4 基于 NDN 的边缘计算

现有的物联网系统严重依赖于云计算平台，这种设计存在两个问题：(1)云计算平台与物联网设备距离较远，无法满足物联网服务低时延的要求；(2)海量的原始物联网数据上传到云计算平台，占用了大量带宽资源[47]。基于此，边缘计算提出将云计算模式扩展到网络边缘，利用网络边缘侧设备(如基站、路由器等)的剩余计算和存储能力，为物联网提供数据预处理、低时延反馈控制、计算任务卸载等服务[48]。近年来，边缘计算普遍被学术界和工业界认为是物联网架构必不可少的一部分，因此基于 NDN 的边缘计算解决方案是 NDN 物联网未来的一个重要研究方向。

边缘计算的一个基础研究问题是如何实现高效的服务部署和服务发现，NDN 的网络层语义、网络层缓存、灵活的转发策略可以在网络层为边缘计算提供支持[49]。文献[50]针对边缘计算中的服务部署和服务发现问题，提出将服务程序作为 NDN 中的一类可寻址数据，支持服务程序的命名、存储、随用户需求动态迁移和实例化，采用了轻量级容器 Unikernel 和微服务架构。但是文献[50]给出的 NDN 边缘计算解决方案并不全面，没有解决 PIT 超时时间、参数传递、安全等问题。文献[51]利用 ICN 基于命名的路由、接收端驱动的流量控制、基于内容的安全等特性，实现了通用的远程服务调用方式，为应用层提供了便捷的编程接口。边缘计算对于物联网设备来说，也是一种远程服务调用，因此文献[51]对基于 NDN 的边缘计算研究值得借鉴，不过应该结合考虑边缘计算节点的异构性、计算和存储资源动态性等特点。

基于 NDN 实现边缘计算虽然在服务部署和服务发现上有优势，但是也引入了一些新的研究问题。(1)PIT 超时时间与边缘计算响应时间不匹配。相比于普通的内容获取，对边缘计算服务的请求响应时间更长，很有可能在 PIT 超时时间到期之后相应的 Data 包才被发送，因此传统的 Interest-Data 通信模式在边缘计算场景下不适用。如何在保证与标准 NDN 兼容的前提下解决 PIT 超时时间与边缘计算响应时间不匹配的问题，值得研究。(2)由于边缘计算节点的计算和存储资源有限，因此单个边缘计算节点可能无法提供一个完整的服务，需要多个边缘计算节点合作，这就需要在边缘计算节点之间传递计算的参数。但是，简单地将计算参数作为 Interest 包命名的一部分进行传递，违背了 Interest 包作为 NDN 接收端流量控制方式中的“令牌”作用，因此需要研究更加高效的参数传递方案。

5.5 集中式与分布式相结合的控制模型

NDN 采用了完全分布式的控制模型，网络中的路由和转发节点具有更强的决策能力和更灵活的决策机制。例如，NDN 中的节点可以根据转发策略动态地为每个 Interest 包决定下一跳转发接口，也可以多接口转发。与 SDN 中控制平面和数据平面分离的机制不同，NDN 中控制平面和数据平面是完全耦合的。不同的物联网应用具有差异化的网络服务质量需求，如车联网应用需要低延时、高可靠的网络服务，而传感网络应用需要低功耗、高能效的网络服务。在具有差异化服务质量需求的不同物联网应用共存的情况下，NDN 单纯依靠完全分布式的控制模型来保证较高的网络服务质量和网络利用率是极具挑战性的。可能的解决方案是结合 SDN 集中式控制的思想，研究集中式和分布式结合的控制模型[52-53]。融合 SDN 的 NDN 物联网研究的挑战包括控制平面与数据平面的低时延通信、控制器的分布式部署方案等。

5.6 基于区块链的跨域分布式安全

物联网作为物理世界与信息世界的连接接口，其安全直接关系到用户的人身、财产、隐私安全。在基于 NDN 的物联网中，典型的安全攻击包括 Interest 泛洪、缓存污染、伪造数据源、拒绝服务、非法篡改、非法访问等，这些安全攻击的目标可大致分为影响内容可达性和用户隐私两大类。区块链作为一种去中心化的分布式总帐技术，由系统中的所有节点共同维护一个记录了系统中所有交易的数据库，具有去中心化、防篡改、可追溯、可编程等特点。将区块链用于物联网安全的优势体现在分布式架构和跨域信任两大方面。相比集中式安全架构，基于区块链的分布式物联网安全解决方案[54-55]具有更强的可扩展性和鲁棒性，不依赖于单一节点的可信性。目前，不同垂直物联网领域之间存在设备孤岛和数据孤岛问题，由于缺乏跨域信任，不同信任域的 IoT 设备和数据之间无法便捷地互相访问。区块链建立和维护跨域信任体系的有效性已经被实际应用所验证，如基于区块链的跨银行结算，因此基于区块链的分布式安全机制有利于打破物联网设备和数据孤岛。

基于区块链的跨域分布式安全研究包括基于区块链设计分布式跨域访问控制机制、跨域统一身份标识生成算法等。将区块链应用于基于 NDN 的物联网也存在诸多挑战：(1)物联网节点计算、存储、网络资源受限，而区块链中区块的生成和存储需要消耗大量算力和存储空间，因此需要合理选择存

储在区块链上的物联网信息;(2)需要保障在区块链存储的信息中进行物联网安全攻击识别和防御的实时性;(3)物联网节点上线和下线频繁,如何在高动态性环境下维护区块链系统的稳定运行是另一大挑战。

结束语 5G 三大应用场景中的 uRRLC 和 mMTC 都属于大规模物联网业务,随着 5G 标准的制定及实际部署,大规模物联网业务将具备实现实际部署的通信层基础。大规模物联网业务下将出现百亿级物联网终端设备接入、ZB 量级物联网数据传输的连接和通信需求,对上层网络架构提出了异构性、可扩展性、移动性、安全性四大挑战。TCP/IP 网络架构采用标识与位置绑定、基于端到端连接通信的设计原则,难以应对以上四大挑战,研究适合 5G 大规模物联网业务的新型网络架构具有必要性和可行性。NDN 网络架构以内容为中心,将发送端与接收端解绑,天然支持多对多通信和多播,具有网络层缓存和基于内容的安全机制,可以更加高效地应对以上四大挑战。

参 考 文 献

[1] AL-FUQAHA A, GUIZANI M, MOHAMMADI M, et al. Internet of Things: a survey on enabling technologies, protocols, and applications[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2347-2376.

[2] ZHU H B, YANG L X, YU Q. Investigation of technical thought and application strategy for the internet of things[J]. Journal on Communications, 2010, 31(11): 2-9.

[3] TURNER V, GANTZ J F, REINSEL D, et al. The digital universe of opportunities: Rich data and the increasing value of the internet of things[J]. Journal of Telecommunications and the Digital Economy, 2014, 2(3): 47. 1-47. 9.

[4] XU L W, LIN W. Research on Outage Probability Performance of Mobile Multi-user Communication System[J]. Journal of Liaocheng University (Natural Science Edition), 2020, 33(2): 43-48.

[5] ZHANG L, AFANASYEV A, BURKE J, et al. Named data networking[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73.

[6] JACOBSON V, SMETTERS D K, THORNTON J D, et al. Networking named content[J]. Proc Acm Conext, 2009, 55(1): 1-12.

[7] SHI W S, ZHANG X Z, WANG Y F, et al. Edge computing: State-of-the-Art and Future Directions[J]. Journal of Computer Research and Development, 2019, 56(1): 69-89.

[8] MCKEOWN N. Software-defined networking [J]. INFOCOM Keynote Talk, 2009, 17(2): 30-32.

[9] PANARELLO A, TAPAS N, MERLINO G, et al. Blockchain and iot integration: A systematic survey[J]. Sensors, 2018, 18(8): 2575.

[10] AKPAKWU G A, SILVA B J, HANCKE G P, et al. A survey on 5G networks for the Internet of Things: Communication technologies and challenges[J]. IEEE Access, 2017, 6: 3619-3647.

[11] PALATTELLA M R, DOHLER M, GRIECO A, et al. Internet of things in the 5G era: Enablers, architecture, and business models[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(3): 510-527.

[12] LI S, DA XU L, ZHAO S. 5G Internet of Things: A survey[J]. Journal of Industrial Information Integration, 2018, 10: 1-9.

[13] SHANG W, ZHANG L, BANNIS A, et al. Named Data Networking of Things (Invited Paper)[C]// IEEE First International Conference on Internet-Of-Things Design and Implementation. 2016: 117-128.

[14] AMADEO M, CAMPOLO C, QUEVEDO J, et al. Information-centric networking for the internet of things: challenges and opportunities[J]. IEEE Network, 2016, 30(2): 92-100.

[15] LINDGREN A, ABDESSLEM F B, AHLGREN B, et al. Design choices for the IoT in Information-Centric Networks[C]// 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). 2016.

[16] AKPAKWU G, SILVA B, HANCKE G P, et al. A survey on 5G networks for the Internet of Things: communication technologies and challenges[J]. IEEE Access, 2018, 6(99): 3619-3647.

[17] 3GPP. Release freeze and end dates[EB/OL]. [2019-06-09]. https://www.3gpp.org/specifications/releases.

[18] RATASUK R, MANGALVEDHE N, ZHANG Y, et al. Overview of narrowband IoT in LTE Rel-13[C]// IEEE Conference on Standards for Communicatons and Networking. IEEE, 2016: 1-7.

[19] 3GPP TS 36.300. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description[S/OL]. https://www.etsi.org/deliver/etsi_ts/136300_136399/136300/13.02.00_60/ts_136300v130200p.pdf.

[20] RAZA U, KULKARNI P, SOORIYABANDARA M. Low power wide area networks: An overview[J]. IEEE Communications Surveys & Tutorials, 2017, 19(2): 855-873.

[21] ZHANG L, ESTRIN D, BURKE J, et al. Named data networking (ndn) project[R]. Xerox Palo Alto Research Center-PARC, 2010.

[22] KUSHALNAGAR N, MONTENEGRO G, SCHUMACHER C. IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals[R]. IETF, 2007.

[23] SHELBY Z, HARTKE K, BORMANN C. The constrained application protocol (CoAP)[R]. IETF, 2014.

[24] TARIQUE M, TEPE K E, ADIBI S, et al. Survey of multipath routing protocols for mobile ad hoc networks[J]. Journal of network and computer applications, 2009, 32(6): 1125-1143.

[25] HAN H, SHAKKOTTAI S, HOLLOT C V, et al. Multi-path TCP: a joint congestion control and routing scheme to exploit path diversity in the Internet[J]. IEEE/ACM Transactions on Networking, 2006, 14(6): 1260-1271.

[26] SHANG W, YU Y, DROMS R, et al. Challenges in IoT networking via TCP/IP architecture: Technical Report NDN-0038[R]. 2016.

[27] ESTRIN D, FARINACCI D, HELMY A, et al. Protocol independent multicast-sparse mode (PIM-SM): Protocol specification[R]. 1998.

[28] HUI J，KELSEY R. Multicast protocol for low-power and lossy networks (MPL)[R]. 2016.
[29] DIERKS T，RESCORLA E. The transport layer security (TLS) protocol version 1. 2[R]. IETF，2008.
[30] RESCORLA E，MODADUGU N. Datagram transport layer security version 1. 2[R]. IETF，2012.
[31] SELANDER G，MATTSSON J，PALOMBINI F，et al. Object security of coap (oscoap)：Internet-Draft draft-ieff-core-object-security-04[S]. Internet Engineering Task Force，2017.
[32] BACCELLI E，MEHLIS C，HAHM O，et al. Information centric networking in the IoT：Experiments with NDN in the wild[C]// Proceedings of the 1st ACM Conference on Information-Centric Networking. 2014：77-86.
[33] AMADEO M，CAMPOLO C，IERA A，et al. Information Centric Networking in IoT scenarios：The case of a smart home[C]// IEEE International Conference on Communications. 2015：648-653.
[34] GÜNDOČAN C，KIETZMANN P，LENDERS M，et al. NDN，CoAP，and MQTT：A Comparative Measurement Study in the IoT[C]// 5th ACM Conference on Information-Centric Networking(ICN'18). 2018.
[35] ZHANG T K，SHAN S Y，XU X G，et al. Survey on Caching Techniques of Information Centric Networking[J]. Journal of Beijing University of Posts and Telecommunications，2016，39(3)：1-15.
[36] PSARAS I，ASCIGIL O，RENE S，et al. Mobile data repositories at the edge[C]//{USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18). 2018.
[37] PFENDER J，VALERA A，SEAH W K. Performance comparison of caching strategies for information-centric IoT[C]// Proceedings of the 5th ACM Conference on Information-Centric Networking. 2018：43-53.
[38] HAHM O，BACCELLI E，SCHMIDT T C，et al. Low-power internet of things with NDN & cooperative caching[C]// Proceedings of the 4th ACM Conference on Information-Centric Networking. 2017：98-108.
[39] LEE J，KIM D. Proxy-assisted content sharing using content centric networking (CCN) for resource-limited mobile consumer devices[J]. IEEE Transactions on Consumer Electronics，2011，57(2)：477-483.
[40] VASILAKOS X，SIRIS V A，POLYZOS G C，et al. Proactive selective neighbor caching for enhancing mobility support in information-centric networks[C]// Edition of the Icn Workshop on Information-Centric Networking. 2012：61-66.
[41] JACOBSON V，BRAYNARD R L，DIEBERT T，et al. Custodian-based information sharing[J]. Communications Magazine IEEE，2012，50(7)：38-43.
[42] PIAO X，Z Y，LEI K. Survey of mobility management technologies based on Named Data Networking[J]. Application Research of Computers，2017，34(4)：961-964.
[43] GHASEMI C，YOUSEFI H，SHIN K G，et al. On the Granularity of Trie-Based Data Structures for Name Lookups and Updates[J]. IEEE/ACM Transactions on Networking，2019，27(2)：777-789.
[44] ASCIGIL O，REÑÉ S，XYLOMENOS G，et al. A keyword-based ICN-IoT platform[C]// ACM Conference on Information-Centric Networking. 2017：22-28.
[45] PAPALINI M. Tagnet：A scalable tag-based information-centric network[D]. Università della Svizzera italiana，2015.
[46] SHANG W，YU Y，WANG L，et al. A survey of distributed dataset synchronization in Named Data Networking：Technical Report NDN-0053[R]. 2017.
[47] SHANG W，WANG Z，AFANASYEV A，et al. Breaking Out of the Cloud：Local Trust Management and Rendezvous in Named Data Networking of Things[C]// International Conference on Internet-Of-Things Design and Implementation. 2017：3-13.
[48] TIAN H，FAN S S，LV X C，et al. Mobile Edge Computing for 5G Requirements[J]. Journal of Beijing University of Posts and Telecommunications，2017，40(2)：1-10.
[49] MTIBAA A，TOURANI R，MISRA S，et al. Towards Edge Computing over Named Data Networking[C]. 2018 IEEE International Conference on Edge Computing (EDGE). 2018：117-120.
[50] KRÓL M，PSARAS I. NFaaS：named function as a service[C]. Proceedings of the 4th ACM Conference on Information-Centric Networking，2017：134-144.
[51] KRÓL M，HABAK K，ORAN D，et al. Rice：Remote method invocation in icn[C]// Proceedings of the 5th ACM Conference on Information-Centric Networking. 2018：1-11.
[52] AHMED S H，BOUK S H，KIM D，et al. Named data networking for software defined vehicular networks[J]. IEEE Communications Magazine，2017，55(8)：60-66.
[53] SALSANO S，BLEFARI-MELAZZI N，DETTI A，et al. Information centric networking over SDN and OpenFlow：Architectural aspects and experiments on the OFELIA testbed[J]. Computer Networks，2013，57(16)：3207-3221.
[54] JIN T，ZHANG X，LIU Y，et al. BlockNDN：A bitcoin blockchain decentralized system over named data networking[C]// 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN). 2017：75-80.
[55] LOU J，ZHANG Q，QI Z，et al. A blockchain-based key management scheme for named data networking[C]// 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). 2018：141-146.

XIE Ying-ying，born in 1994，postgraduate. Her main research interests include Internet of Things and Named Data Networking.

LEI Kai，born in 1976，Ph.D，associate professor，is a member of China Computer Federation. His main research interests include Named Data Networking，knowledge graph，Blockchain and big data.