北京郵電大學

论文题目：

Named Data Networking：下一代互联网架构的演进与研究综述

学院：计算机学院（国家示范性软件学院）

专业：计算机科学与技术

班级：2022211305

学号：2022211683

姓名：张晨阳

2025 年 6 月 6 号

目录

摘要

Named Data Networking（NDN）作为一种基于内容命名的数据通信范式，被广泛认为是未来互联网的重要发展方向之一。相较于传统基于地址的 IP 架构，NDN 通过“以内容为中心”的模型，在提升网络可扩展性、安全性与内容分发效率方面展现出独特优势。近年来，NDN 架构不断演进，涌现出多种面向特定应用场景的增强方案，如 f-NDN、ENDN、IoT-NDN 等，同时其在物联网、车联网、软件定义网络等领域也得到深入探索与应用。本综述论文系统梳理了 NDN 的基本架构与核心机制，分析其在命名、转发、缓存、安全性等方面的研究进展，并对代表性扩展架构及其应用进行了比较和评述。在总结现有研究成果的基础上，本文指出 NDN 面临的关键挑战，并对其未来发展趋势进行展望，以期为后续研究提供参考。

关键词：Named Data Networking，未来互联网，缓存机制，转发策略，NDN-IoT，架构演进。

1 引言

传统互联网自 20 世纪 70 年代诞生以来，主要采用 TCP/IP 协议栈作为通信基础，其通信范式基于 IP 地址与端口号的“端到端”模型。在这种模型中，网络的基本任务是实现数据从源主机传输至目的主机。然而，随着互联网规模的不断扩大以及应用场景的日趋复杂，这一通信范式在处理内容分发、终端异构、网络移动性、安全性和可扩展性等方面暴露出诸多问题。

特别是在移动互联网、社交平台、视频点播、内容分发网络（CDN）和物联网快速发展的背景下，用户更关注“获取什么内容”，而非“从哪台主机获取”。传统 IP 网络依赖中心化服务器和中继节点进行数据传输，存在路径不透明、缓存难部署、安全性弱等问题。

此外，当前的 IP 网络缺乏对内容命名、本地缓存、安全认证等原生支持，导致网络效率低下、攻击面扩大、运维复杂。

为解决上述问题，学术界提出了多种“后 IP 时代”的互联网架构模型，其中最具代表性的是信息中心网络（Information-Centric Networking，ICN）。Named Data Networking（NDN）作为 ICN 的主流实现之一，提出“以数据为中心”的全新网络架构。NDN 将通信核心从地址切换为“命名内容”，通过 Interest/Data 包交互机制、命名路由结构（FIB）、待处理表（PIT）和内容缓存（CS）等关键组件，打造出一个具备高效率、高安全、强适应性的网络传输框架。

Named Data Networking（NDN）作为信息中心网络（Information-Centric Networking, ICN）架构的代表，通过将通信核心从地址转向“命名数据”，提出了完全不同于传统 IP 网络的架构体系。NDN 的通信以数据名称为标识，采用 Interest/Data 包交互机制，结合网络层的内容路由（FIB）、内容请求追踪（PIT）与内容缓存（CS）策略，实现更高效、安全、灵活的内容传递方式。

本文旨在综述 NDN 体系结构的核心机制、关键组件、典型实现与模拟工具、扩展架构、当前研究热点与挑战，并从应用落地和未来发展角度提出个人思考。

2 NDN 基本概念与核心结构

Named Data Networking（NDN）作为信息中心网络（ICN）的一种关键实现，其核心思想在于通过内容名称替代主机地址来完成数据通信。这种模型强调“获取什么”而不是“向谁获取”，从而显著提升网络在内容分发、缓存利用、安全认证等方面的灵活性和效率。

2.1 通信模型与命名机制

NDN 采用“请求-响应”式拉模型。通信过程以 Interest 包和 Data 包为基本单位。消费者通过发送一个包含内容名称的 Interest 包表达数据请求，网络中节点依据名称前缀将其转发到数据提供者或缓存节点，若命中缓存或到达源节点，则以 Data 包回应。

NDN 的命名方式具备如下特性：

- **层级结构**：例如 /edu/ucla/cs/class1/slide1.pdf，支持命名空间分区与聚合；
- **可读性强**：适合人类理解与逻辑组织；
- **可扩展性**：支持任意深度和粒度，适用于多种场景需求；
- **独立于位置**：消除了对固定 IP 地址的依赖，便于移动性和弹性网络部署。

这种命名机制不仅服务于路由，还在安全机制中起到关键作用，每个数据包的签名均绑定于其名称，确保内容完整性和可追溯性。

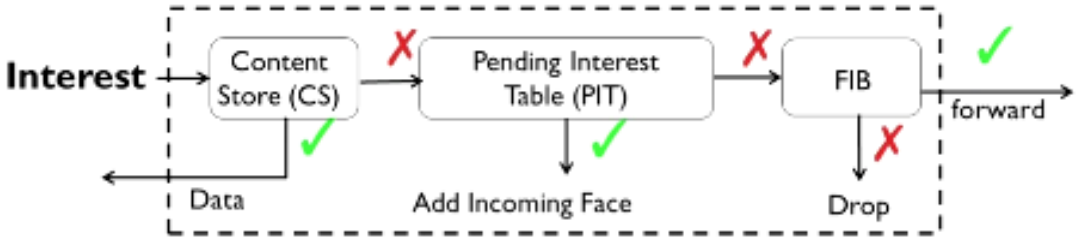
2.2 路由器核心组件

NDN 的路由器与传统 IP 路由器在结构和功能上有显著不同，其主要由以下三个核心组件构成：

- **PIT（Pending Interest Table）**：用于追踪每个转发的 Interest 包，记录其到达接口。若匹配的 Data 包返回，PIT 决定数据从哪些接口返回。每个 PIT 项目会在一定时间内超时失效，防止表项无限增长。
- **FIB（Forwarding Information Base）**：负责将未命中的 Interest 转发至下一跳节点。FIB 基于前缀匹配（最长匹配）进行查找，条目由名称前缀与下一

跳接口对应构成。

- **CS（Content Store）**：即缓存模块，用于存储曾经经过的 Data 包。CS 可被动返回数据以满足后续的 Interest 包，提高命中率、降低时延和带宽负载。



图表 1 兴趣包的路由机制

NDN 的这一结构使其具备天然的缓存与多播能力。例如，多个用户请求相同内容时，路由器可通过 CS 直接回应而无需多次回源，节省资源并提升效率。

此外，PIT 的状态特性也带来新型控制能力：例如支持基于内容的反向追踪机制、链路故障恢复和组播分发路径重用，但同时也对资源管理与安全性提出挑战。

3 NDN 的实现和模拟平台

NDN 作为一种颠覆式的新型网络架构，其发展依赖于强有力的原型实现与模拟平台支持。在理论设计之外，实际系统的搭建、协议栈开发与功能验证是推动其工程化落地的重要手段。

3.1 CCNx 原型实现

CCNx（Content-Centric Networking）是由帕洛阿尔托研究中心（PARC）早期提出的 NDN 原型系统，代表了第一个可运行的命名数据网络实现平台。该平台实现了 Interest/Data 包封装、名称匹配与缓存机制等核心功能，具有如下特点：

- **跨平台支持**：可运行于 Linux、macOS、Windows 和 Android；
- **守护进程架构**：核心服务通过 ccnd 守护进程运行，统一协调转发与缓存逻辑；
- **协议模块完备**：包括 FIB、PIT、CS、签名与安全验证、内容发现机制；
- **开放源代码**：便于研究人员分析底层实现结构并基于其构建增强功能。

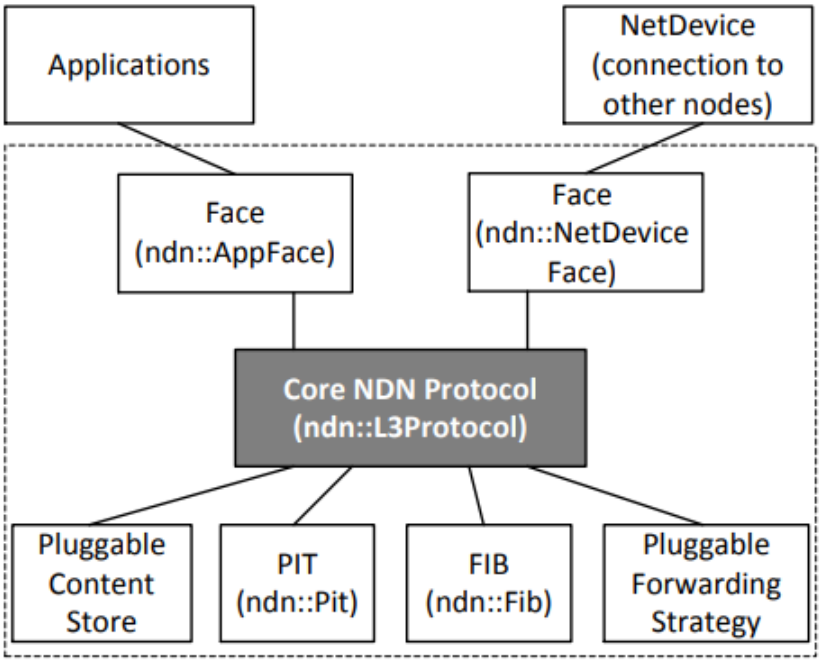
然而，CCNx 的性能瓶颈也逐步显现。研究表明，在无硬件加速支持的场景下，CCNx 难以实现 1Gbps 以上的吞吐量，主要限制因素包括名称解析效率低、内存访问冲突、缓存查找开销大等 [6]。

3.2 ndnSIM 模拟器

为了支持对大规模 NDN 网络的可控实验与机制评估，UCLA 提出了基于 NS-3 网络仿真的 ndnSIM 平台 [1]。

该模拟器具有如下优势：

- **模块化组件**：Interest/Data 包、FIB、PIT、CS、策略选择器均可替换；
- **支持脚本化拓扑构建**：使用 NS-3 的拓扑脚本定义网络结构与流量模型；
- **高度还原真实协议行为**：可模拟缓存替换策略（如 LRU、FIFO）、转发机制（如 Best Route、Multicast）、延迟和丢包模型；
- **结果可视化与日志导出**：便于收集实验指标如时延、带宽、命中率等。



图表 2 ndn **组件结构**

ndnSIM 在以下研究领域得到广泛应用：

- NDN 路由策略与路径优化对网络延迟的影响研究；
- 多播转发策略与拓扑变化适应性实验；
- 缓存机制与命中率之间的平衡分析；
- 安全攻击（如 Interest flooding）下的网络恢复性能评估。

4 扩展架构组合：功能优化与实际需求

随着 NDN 理论架构逐步成熟，越来越多的研究者尝试将其与不同的网络场景融合，或针对特定问题设计增强型架构。这些扩展架构不仅提升了 NDN 在实际部署中的适应性，也丰富了其功能体系。以下将介绍三类代表性扩展方案：f-NDN、ENDN 和 IoT-NDN，它们分别面向流量感知优化、可编程网络控制以及物联网环境下的资源受限挑战。

4.1 f-NDN：面向流的网络优化

传统 NDN 通信以数据块为最小单位，难以识别多个 Interest 是否属于同一应用会话，导致对 QoS 管理支持不足。

f-NDN（Flow-aware NDN） [7] 通过引入“数据流”标识机制，对连续的 Interest 包建立流会话关系，实现如下增强：

- **流状态感知**：支持基于内容名称的流量聚合，便于进行优先级调度与速率控制；
- **PIT 简化与压缩**：合并同一数据流的多个 Interest 表项，减少资源开销；
- **多路径传输支持**：通过流级别的负载均衡，提高端到端吞吐与鲁棒性。

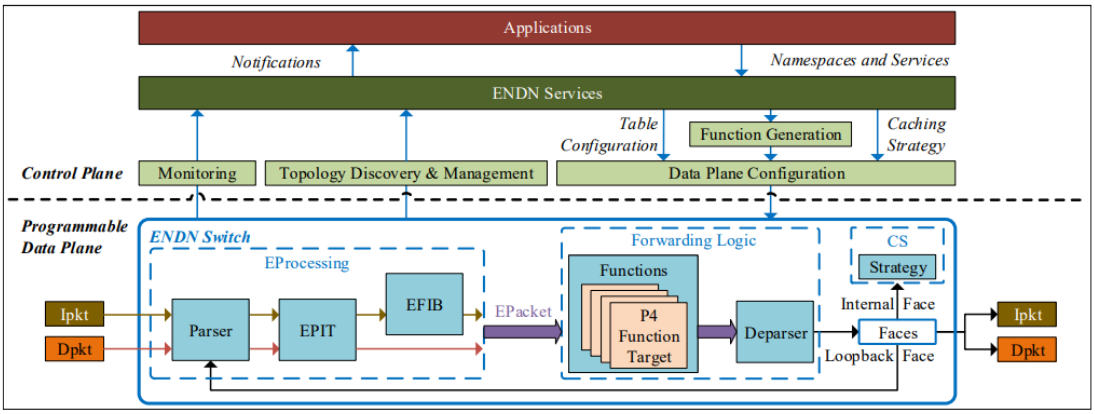
该方案尤其适合高清视频、远程教学等实时多媒体场景，在不改变核心协议栈的前提下，增强了对时延敏感业务的适配能力。

4.2 ENDN：可编程数据平面增强

ENDN（Enhanced NDN） [5] 是将可编程网络理念引入 NDN 的代表性工作。其核心思想是使用 P4 编程语言构建支持命名数据处理的数据平面，实现如下功能：

- **名称级转发控制**：在转发器中对内容名称进行解析与匹配，实现快速路径选择；
- **自定义缓存逻辑**：允许开发者定义内容存储与替换策略，提升缓存命中率；
- **状态监控与策略调整**：可动态捕获网络状态，实现基于网络拥塞与流量热点

的策略更新。



图表 3 ENDN **架构**

ENDN 提升了 NDN 在多租户网络、边缘路由器和 5G 网络环境下的灵活性，使其具备更强的服务定制能力与自动化调控能力。

4.3 IoT-NDN：轻量化物联网适配

在物联网（IoT）场景下，节点常常资源受限（如低功耗、低计算能力、间歇性连通）。IoT-NDN [2] 是专门为此类应用设计的轻量级 NDN 扩展架构，其改进点包括：

- **命名压缩机制**：通过编码与缩写简化数据包长度，减轻传输负担；
- **广播与邻居发现机制**：适配无路由状态的轻节点，支持邻居感知与缓存共享；
- **异步数据交换**：支持 DTN（延迟容忍网络）模型，实现断续连接下的数据转发。

IoT-NDN 广泛适用于智能家居、农业监测、环境感知等边缘部署场景，在低能耗基础上实现较高的数据可达率。

5 NDN 安全性与网络防护机制

网络安全是下一代互联网架构设计中不可忽视的重要课题。相比传统 IP 网络主要依赖“通信端点”安全模型，NDN 采用“数据本身可信”的理念，通过在协议层对内容进行加密签名来确保其来源与完整性。这种机制不仅提升了数据级别的可验证性，也为抵御数据篡改和传输劫持提供了新的思路。

5.1 内容级安全机制

NDN 在设计之初便将安全机制集成至数据层：每个 Data 包都必须附带由内容提供者生成的加密签名，消费者收到数据后通过公钥进行验证。这种“绑定命名内容与发布者身份”的机制具有如下优点：

- **天然抗劫持与重放**：因为每份内容都有签名，攻击者难以伪造有效数据包；
- **安全与通信解耦**：无需建立加密通道即可验证数据内容，有利于组播、多播等场景；
- **粒度可控的信任模型**：用户可选择信任某类命名前缀、特定公钥发布者，支持灵活访问控制。

此外，NDN 社区提出了多种基于名称的访问控制机制，如密钥命名体系（Key Name Hierarchy）与基于属性的加密（ABE），以应对内容保护和隐私共享的现实需求。

5.2 潜在攻击与防御机制

尽管 NDN 提供了内容级的安全保障，但其特有机制也引入了新的攻击面，主要包括：

- **Interest Flooding 攻击**：攻击者连续发送伪造或难以满足的 Interest，导致路由器 PIT 被占满，正常请求被延迟或丢弃；
- **缓存污染攻击**：通过频繁请求冷门或伪造内容，使高价值数据被逐出缓存，影响命中率与性能；
- **名称仿冒与转发表欺骗**：利用名称相似性诱导 Interest 被错误路由到攻击节

点，造成内容篡改或拦截。

针对上述问题，研究者提出了多种防御策略：

- **速率限制与接口控制**：为每个接口配置 Interest 速率上限，避免单一来源请求过载 [1]；
- **PIT 项过滤机制**：对频繁失败或无响应的名称模式执行 PIT 清除与黑名单过滤；
- **内容认证与缓存验证**：引入内容溯源机制，对 CS 中数据按策略周期性验证签名，有效提升缓存可信度 [2]；
- **命名白名单与访问控制策略**：限制特定前缀或命名域仅允许授权用户访问，结合密钥加密体系增强安全边界 [9]。

此外，还存在一些主动防御方向，如基于机器学习的 Interest 异常检测、命名图谱异常行为识别等，虽尚处于探索阶段，但已展现良好前景。

6 结论与思考

Named Data Networking 构建了一种以内容为中心的新型网络范式，从根本上改变了传统 IP 网络以地址为核心的通信逻辑。其设计强调数据本体安全、内置缓存支持和多路径分发能力，不仅提升了网络传输效率，也为未来网络服务提供了全新思路。通过本文所述的标准架构、模拟平台及多项扩展方案，可以看出 NDN 在科研与工程两个维度都已取得积极进展。

然而，值得深入思考的是：

NDN 并非传统互联网的“替代品”，而更可能是其未来结构中的“有机补充”。在具体部署中，NDN 是否应当作为底层通信协议替代 IP？或是作为边缘内容分发机制与现有网络共存？这是产业界与学界尚未达成共识的关键议题。

此外，我们也应关注 NDN 的系统性挑战：

命名空间的规模扩展如何控制在可管理范围？

缓存策略如何在公平性与命中率之间寻求平衡？

数据安全签名如何在低算力设备中高效实现？

面对主动攻击，NDN 能否在不引入过多控制面的基础上构建“自防御”能力？

在我看来，NDN 的最大潜力不止于技术层面，而在于它激发我们重新思考“互联网的本质目标”——信息流通是否可以摆脱对位置信息的依赖，是否可以以信任为核心而非边界构筑安全？

NDN 所引导的方向，促使网络系统不再围绕地址和通道构建信任，而是围绕数据本身构建信任，这是互联网体系观的一次深刻重构。

因此，未来的研究不仅要继续完善 NDN 协议族与实现效率，更应聚焦以下几个交叉方向：

- **体系融合性设计**：研究 NDN 与现有 TCP/IP、HTTP、QUIC 等协议的融合机制，实现渐进式部署；
- **跨域标准协调**：推动国际标准组织对 NDN 命名结构、安全机制、缓存策略的标准化讨论；
- **应用场景适配**：在视频分发、边缘协同、工业互联网等典型场景中构建实测原型，验证其可行性与性能优势；

- **社会信任机制重构**：结合区块链与分布式认证模型，在 NDN 基础上构建更为透明可控的数据信任体系。

综上所述，NDN 不仅是下一代网络架构的技术候选，更代表着我们对未来网络“内容、信任与效率”三者关系的全新理解。它不仅是一项工程实践，也是一种理念探索，其价值将在未来互联网不断演化的过程中持续显现。

REFERENCES

[1] A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM: NDN simulator for NS-3," NDN, Technical Report NDN-0005, Revision 2, Oct. 5, 2012. [Online]. Available: http://named-data.net/techreports.html

[2] M. A. Hail, "IoT-NDN: An IoT Architecture via Named Data Networking (NDN)," in *Proc. 2019 IEEE Int. Conf. Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, 2019.

[3] Z. Yan, S. Zeadally, and Y.-J. Park, "A Novel Vehicular Information Network Architecture Based on Named Data Networking (NDN)," *IEEE Internet Things J.*, vol. 1, no. 6, pp. 317–326, Dec. 2014.

[4] S. Rowshanrad, M. R. Parsaei, and M. Keshtgari, "Implementing NDN Using SDN: A Review of Methods and Applications," *IIUM Eng. J.*, vol. 17, no. 2, pp. 11–24, 2016.

[5] O. Karrakchou, N. Samaan, and A. Karmouch, "ENDN: An Enhanced NDN Architecture with a P4-programmable Data Plane," Univ. of Ottawa, Canada, 2020.

[6] H. Yuan, T. Song, and P. Crowley, "Scalable NDN Forwarding: Concepts, Issues and Principles," Washington Univ., St. Louis, MO, and Beijing Inst. of Technology, Beijing, China.

[7] X. Tan, W. Feng, J. Lv, Y. Jin, Z. Zhao, and J. Yang, "f-NDN: An Extended Architecture of NDN Supporting Flow Transmission Mode," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6053–6066, Oct. 2020.

[8] S. Li, Y. Zhang, D. Raychaudhuri, and R. Ravindran, "A Comparative Study of MobilityFirst and NDN-based ICN-IoT Architectures," in *Proc. 2014 Int. Conf. Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE)*, 2014.

[9] A. Tariq, R. A. Rehman, and B.-S. Kim, "Forwarding Strategies in NDN-Based Wireless Networks: A Survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 640–670, First Quart. 2020.