命名数据组网

张丽霞
Alexander Afanasyev
杰弗里·伯克
范·雅各布森
UCLA
Christos Papadopoulos
科罗拉多州立大学。

Kc claffy
CAIDA UC,
圣地亚哥
王澜
孟菲斯大学patri

ck Crowley
华盛顿大学圣路易斯分校

张北川
亚利桑那大学

abstract

命名数据网络(NDN)是由美国国家科学基金会在其未来互联网架构计划下资助的五个项目之一。NDN起源于早期的一个项目，内容中心网络(CCN)， Van雅各布森在2006年首次公开提出了这个项目。[1]NDN项目研究雅各布森提出的从今天以主机为中心的网络架构(IP)到以数据为中心的网络架构(NDN)的演变。这种概念上的简单转变对我们如何设计、开发、部署和使用网络和应用程序有着深远的影响。我们描述了这种新架构的动机和愿景，以及它的基本组件和操作。我们还提供了其当前设计、开发状态和研究挑战的快照。有关该项目的更多信息，包括原型实现，出版物和年度报告，可在nameddata.net上获得。

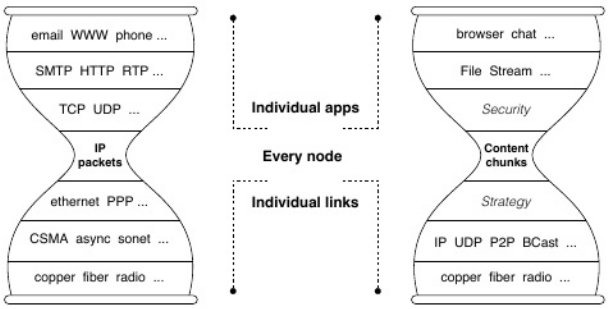

图1:NDN架构的主要构建块被命名为内容块，与IP架构的基本通信单元形成对比，后者是由IP地址标识的两个端点之间的端到端通道。

1. vision:全新的窄腰

今天的互联网沙漏架构以通用网络层(即IP)为中心，它实现了全球互联所必需的最小功能。这种细腰结构通过允许底层和上层技术独立创新，实现了互联网的爆炸式增长。然而，IP被设计为创建一个通信网络，其中数据包只命名通信端点。电子商务、数字媒体、社交网络和智能手机应用的持续增长导致了互联网作为分销网络的主导使用。分销网络比通信网络更为通用，通过点对点通信协议解决分销问题既复杂又容易出错。

命名数据网络(NDN)项目提出了IP架构的演进，该架构概括了这种细腰的作用，这样数据包就可以命名通信端点以外的对象(图1)。NDN改变了网络服务的语义，从将数据包发送到给定的目标地址到获取由给定名称标识的数据。NDN包中的名称可以命名任何东西——端点、电影或书籍中的数据块、打开某些灯的命令等等。这个概念上简单的改变允许NDN网络使用几乎所有经过良好测试的互联网工程属性来解决范围更广的问题，不仅包括端到端通信，还包括内容分发和控制问题。基于三十年来对当前互联网架构的优势和局限性的经验，该设计还构建了安全原语(通过对所有命名数据的签名)和网络流量的自我调节(通过兴趣和数据包之间的流量平衡)。该架构包括设计为有利于用户选择和网络发展竞争的功能，如多路径转发和网络内存储。

NDN是信息中心网络(information-centric networking, ICN)这一更为普遍的网络研究方向的一个实例，在这一方向下出现了不同的体系结构设计。互联网研究任务组(IRTF)于2012年建立了一个ICN研究工作组-[2]。在本文中，我们提供了NDN架构研究项目现状的一个简要(并且必然是不完整的)快照，该项目包括来自12个校区的16名nsf资助的主要研究人员，以及来自学术和工业研究社区的日益增长的兴趣。对最近活动的更完整描述见第三份年度项目报告[20]和NDN网站(nameddata.net)。

1 “A New Way to Look at Networking”，https://www.youtube.com/watch?v=oCZMoY3q2uM

2 http://trac.tools.ietf.org/group/irtf/trac/wiki/icnrg

2. NDN架构

NDN中的通信是由接收器驱动的，即数据消费者，通过交换两种类型的数据包:兴趣和数据。两种类型的数据包都带有一个名称，用于标识可以在一个数据包中传输的数据。消费者将所需数据的名称放入兴趣包中并将其发送到网络。路由器使用这个名称将兴趣包转发给数据生产者。一旦Interest到达具有所请求数据的节点，该节点将返回一个包含名称和内容的数据包，以及绑定两者的生产者密钥的签名(图2)。该数据包遵循Interest所采取的反向路径返回到请求消费者。

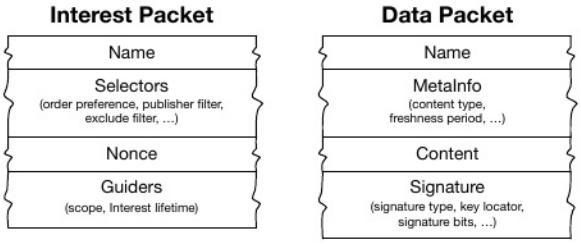

图2:NDN架构中的数据包。

为了实现Interest和Data报文转发功能，每台NDN路由器维护三种数据结构:未决兴趣表(PIT)、转发信息库(FIB)和内容库(CS)(图3)，以及一个转发策略模块(图中未显示)，该模块决定是否、何时以及在何处转发每个兴趣包。PIT存储路由器已转发但尚未满足的所有兴趣。每个PIT条目记录了Internet上携带的数据名称，以及它的传入和传出接口。当兴趣包到达时，NDN路由器首先检查内容库是否匹配数据;如果存在，则路由器返回兴趣源所在接口上的数据包。否则，路由器将在其PIT中查找该名称，如果存在匹配的表项，则将该感兴趣的入站接口记录在PIT表项中。在没有匹配的PIT表项的情况下，路由器将根据FIB中的信息以及路由器的自适应转发策略将兴趣转发给数据生产者。当路由器从多个下游节点接收到相同名称的兴趣时，它只将上游的第一个转发给数据生产者。FIB本身由基于名称前缀的路由协议填充，每个前缀可以有多个输出接口。

转发策略可能会在某些情况下决定放弃兴趣，例如，如果所有上游链路都拥塞或怀疑兴趣是DoS攻击的一部分。对于每个兴趣，转发策略从FIB中检索前缀最长的匹配条目，并决定何时何地转发兴趣。[3]内容库是路由器接收到的数据包的临时缓存。因为NDN数据包是有意义的独立于

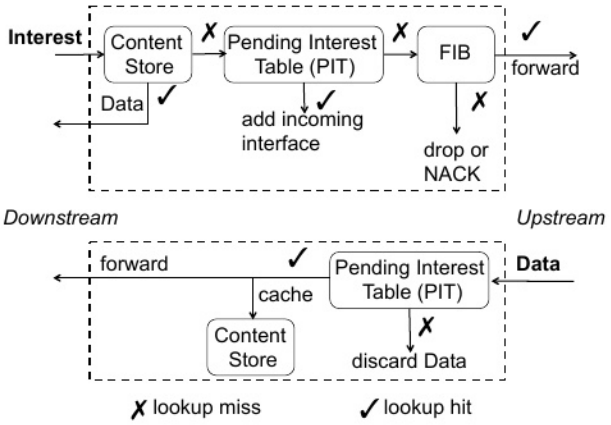

图3:NDN节点的转发过程

它来自哪里或被转发到哪里，它可以被缓存以满足未来的兴趣。

当数据包到达时，NDN路由器找到匹配的PIT表项，并将数据转发到该PIT表项中列出的所有下游接口。然后删除该PIT条目，并在内容库中缓存数据。数据包总是走兴趣的反向路径，在没有丢包的情况下，每个链路上的一个兴趣数据包会产生一个数据包，从而实现流量均衡。为了获取包含多个数据包的大型内容对象，兴趣在控制流量方面提供了类似于今天互联网中的TCP ack的作用:由数据消费者控制的细粒度反馈循环(参见2.1节)。Interest和Data包都不携带任何主机或接口地址;路由器根据数据包中携带的名称向数据生产者转发兴趣数据包，并根据每跳兴趣设置的PIT状态信息向消费者转发数据包。这种兴趣/数据包交换的对称性导致了一个逐跳控制循环(不要与对称路由混淆，或者根本不与路由混淆!)，并且在数据传递中不需要任何源节点或目标节点的概念，这与IP的端到端数据包传递模型不同。

2.1 名称

虽然路由器在名称中识别组件之间的边界，但它们不赋予名称任何意义，即NDN名称对网络是不透明的。这种设计决策允许每个应用程序选择适合其需求的命名方案，因此命名可以独立于网络而发展。NDN设计采用分层结构的名称，例如，UCLA制作的视频可能具有/ UCLA /videos/ demo的名称。mpg，其中“/”描绘了文本表示中的名称组件，类似于url。这种分层结构允许应用程序表示数据元素的上下文和关系。例如，UCLA演示视频版本1的第3段可能命名为/ UCLA /videos/demo.mpg/1/3。它还允许名称聚合，例如，/ucla可以对应于生成视频的自治系统。平面名称可以作为一种特殊情况，可能在本地环境中有用，但是分层名称空间在扩展路由系统和为数据提供必要的上下文方面都是必不可少的。(即使是扁平化路由的倡导者也承认扁平化名称通过引入一些层次结构[2]来扩展。)

[3]While an IP router may be able to reach a network prefix via multiple interfaces, it uses only one except in special cases where multiple best paths have identical cost.

为了检索动态生成的数据，使用者必须能够确定地为所需的数据片段构造名称，而不必事先看到该名称或数据。要么:(1)确定性算法允许生产者和消费者根据双方可用的信息得出相同的名称，要么(2)兴趣选择器与最长前缀匹配结合，通过一次或多次迭代检索所需的数据。到目前为止，我们的经验表明，一组简单的选择器可以支持重新检索部分已知名称的数据。例如，一个消费者想要第一个版本的演示。MPG视频可能会请求/ucla/videos/demo。mpg/1与兴趣选择器“最左边的子”，并接收一个数据包名为/ucla/videos/demo。Mpg /1/1对应第一段。消费者可以使用由第一个数据包揭示的信息和发布应用程序的命名约定的组合来请求后面的段。

可能被全局检索的数据必须具有全局唯一的名称，但是用于本地通信的名称可能只需要本地路由(或本地广播)就可以找到匹配的数据。单个数据名称在各种范围和上下文中都可能是有意义的，从“这个房间里的电灯开关”到“世界上所有国家的名称”。

名称空间管理不是NDN体系结构的一部分，正如地址空间管理不是IP体系结构的一部分一样。然而，命名是NDN应用程序设计中最重要的部分。命名数据可以支持诸如内容分发、多播、移动性和容忍延迟的网络等功能。

允许应用程序开发人员(有时是用户)为数据交换设计自己的命名空间有几个好处:增加应用程序数据与其网络使用之间映射的紧密性;减少了对二次标记的需求(将应用程序配置映射到网络配置的记录保存);并扩大开发人员可用的抽象范围。[4]

我们正在通过实验学习应用程序应该如何选择既能促进应用程序开发又能促进网络交付的名称。当我们开发和完善我们的命名原则和指导方针时，我们将它们转换为命名约定并在系统库中实现它们以简化未来的应用程序开发(参见[19]的一个示例，用于当前代码库[22]的预期使用)。幸运的是，名称对网络的不透明性允许架构开发与应用程序开发上下文中对命名空间结构和导航的研究并行进行。

2.2 Data-Centric Security

TCP/IP将安全责任(或缺乏安全责任)留给端点，与之相反，NDN通过要求数据生产者对每个数据包进行加密签名来保护数据本身。发布者的签名确保了完整性，并能够确定数据的来源，从而允许消费者对数据的信任与数据的获取方式或地点脱钩。它还支持细粒度的信任，允许消费者推断公钥所有者是否是特定上下文中特定数据块的可接受的发布者。第二个主要的研究重点是设计和开发可用的机制来管理用户信任。我们已经试验了hi-层次信任模型，其中密钥命名空间授权使用密钥(携带公钥的数据包实际上是一个证书，因为它是由第三方签名的)来签署特定数据[5]，以及信任网络来实现安全通信，而不需要预先约定的信任锚[36]。

NDN以数据为中心的安全性在内容访问控制和基础设施安全方面具有自然的应用。应用程序可以通过加密控制对数据的访问，并将(数据加密)密钥作为加密的NDN数据分发，从而将数据安全边界限制在单个应用程序的上下文中。要求在网络路由和控制消息(像任何其他NDN数据一样)上签名，为保护路由协议免受欺骗和篡改提供了坚实的基础。NDN使用多路径转发，加上自适应转发策略模块，减轻了前缀劫持，因为路由器可以检测到由劫持引起的异常，并通过备用路径[31]检索数据。由于NDN数据包引用的是内容而不是设备，因此恶意攻击特定设备的难度更大，尽管需要针对其他NDN特定攻击的缓解机制，例如兴趣泛洪DoS[4]。

2.3 路由和转发

NDN基于名称路由和转发报文，解决了IP架构中由于地址导致的地址空间耗尽、NAT遍历和地址管理三个问题。没有地址耗尽的问题，因为命名空间是无界的。不存在NAT遍历问题，因为NDN不涉及公共或私有地址。最后，本地网络不再需要地址分配和管理。

NDN可以使用传统的路由算法，如链路状态和距离矢量。NDN路由器不是宣布IP前缀，而是宣布涵盖路由器愿意服务的数据的名称前缀。路由协议在网络中传播这些通告，通知每个路由器构造自己的FIB。传统的路由协议，如OSPF和BGP，可以通过将名称视为不透明组件序列并根据FIB表对兴趣数据包中的名称进行组件最长前缀匹配来适应名称前缀路由。

每个路由器上的PIT状态支持跨NDN数据平面转发，记录每个待处理的兴趣和入接口，并在收到匹配的数据或超时发生后删除兴趣。这种每跳、每包的状态不同于IP的无状态数据平面。根据FIB中的信息和性能测量，每个路由器中的自适应转发策略模块做出明智的决策:将哪些兴趣转发到哪些接口，在PIT中允许有多少未满足的兴趣，不同兴趣的相对优先级，在多个接口之间负载均衡兴趣转发，以及选择替代路径以避免检测到的故障[32,31]。如果路由器认为Interest不能满足，如上行链路断开、FIB中没有转发表项、发生极度拥塞等，路由器可以向发送Interest的下游邻居发送NACK报文。这样的NACK可能会触发接收路由器将Interest转发到其他接口以探索替代路径。PIT状态使路由器能够识别和丢弃循环数据包，允许它们自由地使用通往同一数据生产者的多条路径。

[4]These examples of increased usability are based on Green and Petre’s “cognitive dimensions” framework [12].

PIT状态还有其他有价值的用途。首先，由于它记录了同一数据名称的兴趣到达的接口集，因此它自然支持多播数据传递。其次，由于每个兴趣最多只能检索一个数据包，因此路由器可以通过控制待处理兴趣的数量来控制流量负载，从而实现流量均衡。第三，PIT表项的数量是路由器负载的一个指标;限制它的大小限制了DDoS攻击的效果。最后，PIT条目超时提供了相对便宜的攻击检测，并且每个PIT条目中的到达接口信息可以支持推回方案。

2.4 网内存储

因为每个NDN数据包都带有一个名称和一个签名性质，所以无论请求者是谁或从何处检索它，它都是有意义的。因此，路由器可以在其内容库中缓存接收到的数据包，并使用它们来满足未来的请求。内容库类似于IP路由器中的缓冲存储器，但是IP路由器在将数据包转发到目的地后不能重用它，而NDN路由器可以。在数据检索方面，NDN将存储通道和网络通道等同对待。对于静态文件，NDN实现了几乎最佳的数据传输。即使是动态内容也可以在多播(例如，实时电话会议)或丢包后重传的情况下受益于缓存。

除了内容库之外，该体系结构现在还支持更持久、容量更大的网络内存储，称为Repository(简称Repo)。这种类型的存储可以支持类似于今天的内容交付网络(cdn)的服务，而无需使用创造性的协议技巧(例如，DNS操作)将其设计为应用层覆盖以使其工作。

缓存命名数据引起了与IP不同的隐私问题。在IP中，可以检查数据包头和负载，以了解谁在使用什么数据。在NDN网络中对数据进行命名和缓存可以方便地观察所请求的数据，但是如果没有目标地址，就很难确定是谁在请求它(除非一个主机与请求主机直接连接到同一子网)。因此，NDN提供了一种与当前IP网络根本不同的隐私保护方式。

一些研究人员特别强调网络内缓存是ICN架构的基本增益，例如[10]。尽管NDN可以支持比TCP/IP更强大的CDN架构，但NDN还提供了许多其他功能(保护数据，流量平衡，有状态数据平面，它本身会带来许多收益)，这些功能甚至呈现出更显著和重要的优势。

2.5 传输功能

NDN架构没有单独的传输层。它将当今传输协议的功能(解复用、可靠交付和拥塞控制)转移到应用程序、支持库和转发平面的策略模块中。传输层信息(如端口和序列号)是不必要的;传输所需的所有信息都在数据名称中。例如，名称/ucla/videos/demo。mpg/1/3指定在哪里转发该名称的兴趣(/ucla/)，哪个应用程序应该接收它们(/video/)，以及任何特定于应用程序的信息(版本1，段3)。

当应用程序需要可靠的传递时，应用程序本身或其支持库将监视未完成的兴趣状态，并在需要时(例如，超时后)重新传输它们。NDN的流量平衡要求，加上节点通过限制每一跳的未决兴趣数来控制自身流量负载的能力，可以在整个网络中提供有效的拥塞控制。如果发生拥塞损失，缓存可以减轻影响，因为在数据包丢失点之前缓存的数据包可以满足重传的兴趣。因此，NDN可以避免在今天的互联网中可能发生的那种拥塞崩溃，当数据包在目的地附近丢失时，原始源主机的重复重传会消耗大部分带宽。

3. NDN架构开发

NDN协议规范要求对两种基本报文类型(兴趣和数据)采用标准格式，并对网络层支持的功能进行描述，即新的窄腰。构建可运营的NDN网络还需要软件库来支持命名、高性能转发和路由、转发策略和信任管理。与IP的支持组件(地址分配、路由协议、DNS)类似，这些库不是核心架构的一部分，但本质上支持它，并且都涉及令人望而生畏的研究挑战。本节描述了该项目应用驱动的、实验性的设计和开发架构的方法，包括说明其功能的示例，以及开放的研究挑战。

3.1 应用研究

该项目的方法是在NDN上设计和构建各种应用程序，以推动体系结构及其支持模块的开发和部署，测试原型实现，并鼓励社区使用，实验和反馈到设计中。应用程序驱动的开发还允许对NDN的性能和功能优势进行验证和确认，例如名称路由如何通过降低复杂性、出错机会以及设计和部署的时间和费用来提高复杂分布式应用程序的高效编写。几年来在NDN上设计和开发原型应用程序的经验揭示了应用程序研究的五个关键领域，它们映射到该体系结构的重要特征:(1)命名空间;(2)信任模型;(3)网内存储;(4)数据同步;(5)交会、发现和引导。这些挑战出现在应用程序内部和应用程序之间。命名空间设计还必须认识到特定于应用程序的数据分发需求和与信任相关的信息组织之间的相互作用，以及那些为有效路由/转发而强加的需求。在名称发现、引导和移动性支持方面也存在类似的挑战。这种对应用程序开发的承诺在项目早期就得到了回报:它揭示了用于持久存储的每个节点存储库和作为应用程序通用构建块的同步的意想不到的重要性。一些早期应用的例子说明了NDN的好处和挑战。

视频流。最早的NDN应用程序之一是一个功能性视频流应用程序，它展示了基于NDN的媒体传输的实际好处，它本质上支持缓存和多播。NDNVideo[17]通过NDN流直播和预先录制的高清视频，并有

已经在UDP和以太网传输上进行了测试和演示。在最近的现场演示中，亚马逊网络服务和NDN测试平台上的1000个客户端使用来自单个NDN video发布者的视频，中间节点[9]上只有“普通的”NDN转发器。NDN video应用程序不需要在发布者和消费者之间进行直接通信，通过NDN使用网络内存储实现与发布者无关的可伸缩性。执行动态内容组装或视频部分选择的应用程序，即帧级随机访问需求，直接通过命名空间设计得到支持。

实时会议。ChronoChat[36]多用户文本聊天应用程序提供了一个平台来探索可以支持点对点(即，没有中央服务器)聊天服务的数据同步技术。ChronoChat还推动了非分层信任模型的实验(第3.3节)，并开发了支持基于加密的访问控制的库。结合ChronoChat、NDN video和NDN音频会议工具[37]的早期工作经验，nd-nrtc是一个包含We-bRTC代码库的视频会议应用程序。该工具将能够研究ndn特定的方法来实现拥塞控制、速率适应和实时通信的播放同步。

楼宇自动化系统。企业楼宇自动化和管理系统(BAS/BMS)是NDN研究的理想驱动程序，因为精心设计的命名空间和信任模型可以支持对传感器[7]的认证控制。到目前为止，最大的NDN应用研究工作之一是与加州大学洛杉矶分校设施管理公司的合作，该公司运营着一个拥有超过15万个传感和控制点的网络，并促进了专用、工业标准的电力需求监测系统，并从现有系统获取数据，用于NDN研究[23]。BAS/BMS应用对数据命名和信任的要求与多媒体应用不同。例如，当前基于NDN的BMS设计在三个名称空间中发布数据:一个用于遵循物理构建系统配置的应用程序数据访问，另一个用于设备发现和引导，以及一个用于包含机构角色和主体关系的密钥的信任管理名称空间。另一个挑战是探索命名空间和存储设计如何支持来自许多异构传感器和其他设备的数据聚合和挖掘。

车联网。车载网络是NDN架构提供优势的另一个领域，它支持基于位置的内容检索和新的信任模型，以支持自组织的机会性通信[11]。车载应用的实验也导致了NDN协议栈本身的更新，包括对其他媒体的支持(例如，3G/LTE, DSRC/WAVE, WiFi, WiMAX)和网络层对数据复用的支持。其中车载NDN节点缓存通过广播通道听到的数据包，这些数据包在其PIT中没有匹配的未决兴趣，以便稍后将它们提供给其他车辆或传递给基础设施。

其他应用。现有的NDN软件平台[22]使学生和其他人能够探索基于NDN的分布式文件系统、多用户游戏和网络管理工具。在接下来的几年里，上述应用的工作将继续进行，气候建模和移动健康环境的新探索将作为NDN架构研究和开发的驱动因素。

新的架构组件:Sync。作为尝试构建健壮、高效和真正分布式(即无服务器)点对点NDN应用程序的直接结果，该架构现在支持一个名为Sync[35]的新构建块。Sync使用NDN的基本兴趣-数据交换通信模型，使用命名约定使多方能够同步他们的数据集。通过交换单独计算的数据摘要，双方可以快速可靠地了解新的或丢失的数据，然后通过NDN内置的多播传输有效地检索数据。

3.2 NDN路由转发

NDN转发平面面临着两大挑战:转发策略和可扩展性转发。与此同时，项目团队开发了基于NDN的路由协议原型，以支持近期和中期在测试平台上的使用，同时还研究了NDN自适应转发平面能够实现的更激进的新路由方向。在几个案例中，路由协议设计揭示了当前软件库中缺失的功能。

转发策略设计。每个节点的转发策略模块是NDN弹性和效率的关键。通过有效利用NDN的多路径功能，自适应转发策略可以沿着性能最佳的路径发送消费者兴趣，避免拥塞和故障，平衡路径上的负载，并检测和响应前缀劫持和DDoS[31]等攻击。但回馈策略设计是一个全新的研究领域，关于如何针对不同的环境和设备设计简单有效的策略，存在许多悬而未决的问题。

转发引擎设计。转发引擎必须支持线速操作，包括可变长度名称的快速表查找、存储数百万到数十亿个名称的高效数据结构以及快速数据包处理。项目团队成员提出了一种高度可扩展的转发结构和引擎[34,33]。模拟原型支持在小于10MB的存储空间中存储数百万个条目的FIB, FIB查找速度在微秒量级。此外，来自Cisco[26]和Alcatel-Lucent[27]的工业团队已经开发出可行的原型路由器。

路由协议设计。第一个NDN路由协议是一个OSPF扩展(OSPFN[28])，它定义了一种新型的不透明链路状态通告，用于携带名称前缀和计算基于名称的FIB，目的是在试验台上快速建立基于名称的转发原型，同时更多冒险的路由研究也在并行进行。但是这种对基于IP的路由协议的简单改编，恰恰带来了NDN设计要避免的负担，包括管理GRE隧道、管理底层IP地址，以及支持多跳转发的黑客攻击，因为OSPF只支持单路径和等成本的多路径转发。当前NDN路由协议为NDN-

基于NLSR (link-state routing)的[14]，它使用名称来标识网络、路由器、进程、数据和密钥。NLSR可以使用任何底层通信通道(如eth - ethernet、IP隧道、TCP/UDP隧道)交换路由消息。具体来说，路由器使用兴趣包来重新检索数据包中携带的路由更新，这些更新由原始路由器签名，以允许验证真实性。最重要的是，NLSR在每个路由器中创建基于名称的多路径FIB，以支持NDN的转发平面。

设计NLSR协议需要考虑与任何其他NDN应用相同的维度:(a)如何命名路由器、链路、路由更新等;(b)如何分发加密密钥以及如何在这些密钥中获得信任;(c)路由更新传播，这需要拉更新而不是(OSPF的)推送更新;(d)如何为每个名称前缀生成多个下一跳并对其进行排序，以促进NDN的多径转发。

探索新的路由范式。今天的IP路由体系结构需要传播拓扑和策略信息、路由计算，有时还需要延长收敛时间，因为路由器会检测和路由故障。在NDN中，转发平面本身可以进行快速的故障检测和恢复，减少了路由对自启动转发的作用，并传播长期的拓扑或策略信息[30]。这种解耦允许研究更激进的、可扩展的路由方法，这在IP网络中是不可能的。例如，NLSR现在通过在链路状态广告中传播双曲坐标来支持一种双曲路由[16,6]。AS层的互联网拓扑是一个无标度的、强聚类的小世界[18]，它与有效地隐藏在拓扑[16]下面的潜在空间的双曲几何结构有着深刻的联系。假设路由器拓扑和名称空间具有双曲结构，我们可以使用每个名称前缀的双曲坐标以及邻居的坐标来使用贪婪转发(greedy forwarding - forward)来计算下一跳——每个路由器将Interest数据包转发给离目的地名称最近的邻居路由器。目前正在对NDN上的双曲路由与链路状态路由协议的性能进行比较。[5]其他可能的路由方法，如小世界、伪势梯度和流行病渗透，可能值得探索NDN。

3.3 信任管理

为了验证数据包的签名，应用程序可以获取适当的密钥，在数据包的密钥位置域中识别，就像任何其他内容一样。但是信任管理，即如何确定给定应用程序中特定数据包的给定密钥的真实性，是一个主要的研究挑战。与实验方法一致，NDN信任管理研究是由应用程序开发和使用驱动的:首先解决特定问题，然后确定通用模式。

例如，NLSR的安全需求需要开发一个简单的分层信任模型，其中密钥以反映其信任关系的名称发布。根密钥由网络域的管理员拥有，根下面是站点密钥，每个站点密钥由单个站点的管理员拥有，由根密钥签名，并在层次结构的下一层发布。然后，每个站点密钥对站点的密钥进行签名操作员密钥，它们依次为路由器密钥签名，路由器密钥依次为该路由器上的NLSR进程的密钥签名。最后，NLSR密钥对由NLSR生成的路由数据进行签名。在这个信任模型中，命名空间匹配信任委托的层次结构，即(概念上)/root/site/operator/ router/process。在层次结构中发布具有特定名称的密钥，授权他们对特定的数据包进行签名，并限制其范围。现实世界的信任倾向于遵循分层模式的其他应用程序，例如在我们的建筑管理系统(BMS)[23]中，可以为建筑运营商和应用程序数据使用两个单独的层次结构，以方便对谁有权访问哪些数据进行精细控制。更灵活、更有表现力的信任关系，比如我们的聊天应用[36]，激发了对信任网络模型的实验。当前的聊天室参与者可以通过签署新人的密钥将新人介绍给其他人。未来的应用将实现交叉认证模型(SDSI)[13,3]，该模型提供了更多的验证冗余，允许数据和密钥名称独立，从而更容易适应各种现实世界的信任关系。

4. NDN社区和部署

新架构的成功需要广泛的社区参与和吸收。在学术界和工业界的参与下，NDN已经获得了动力。但是，激励增量部署需要证明NDN可以解决基于TCP/ ip的解决方案存在问题或不存在的现实问题。NDN团队还维护NDN协议栈的开源实现、模拟器和测试台，以促进测试和更广泛的社区参与。

像IP一样，NDN是一个通用的覆盖层:NDN可以运行在任何可以转发数据报的设备上(以太网、WiFi、蓝牙、蜂窝、IP、TCP等)，任何设备都可以运行在NDN上，包括IP。NDN无需尝试替换或更改已部署的IP基础设施，而是可以简单地在其上运行。NDN还可以利用经过数十年发展的Internet经过良好测试的工程解决方案，例如用于命名和路由的约定、策略和管理实践。因此，NDN在内容分发、应用友好的通信和命名、健壮的安全性、支持移动性和广播性等方面的优势可以逐步实现，而且相对轻松。

对于企业应用程序(例如，自动建筑控制)，基于NDN的解决方案可以通过本地部署带来即时价值。诸如无服务器聊天室之类的广域应用程序可以在IP隧道上运行。随着基于NDN的应用程序的部署，我们设想出现NDN节点岛，使用集合解决方案通过在非NDN云上隧道进行互连。一旦NDN应用获得广泛接受，ISP部署NDN路由器将为他们自己和他们的客户提高性能和效率，为基础设施的发展提供自然的激励。IP架构在其自身的部署历史中提供了类似的覆盖功能和增量效益激励

开源软件支持。免费提供的软件库和工具对于NDN架构的可扩展部署至关重要。NDN项目最初使用PARC的开源包CCNx[8]作为其代码库。为研究提供更敏捷的开发平台，2013年

[5]http://netwisdom.cs.memphis.edu/hrhome.html.

NDN团队派生了一个版本的CCNx，并在2014年初从零开始实现了一个新的NDN转发器NFD[21]。NFD支持新开发的NDN数据包格式，并具有模块化和可扩展性，以方便各种实验。NDN平台软件发布[22]包括用于构建和测试NDN网络和应用程序的关键组件的支持包。以流行且易于使用的语言(如Python和Javascript)提供NDN支持，进一步促进了社区[24]的开发活动。该团队计划继续开发和支持NDN代码库，包括在浏览器中支持通过NDN发布web风格的内容，以帮助NDN项目以及更广泛的社区编写创新的、实验性的NDN应用程序。[6]

该项目团队还维护了一个基于NS-3的开源模拟器ndnSIM [1]，它提供了一个通用平台，帮助研究人员评估大型网络中NDN系统性能的各个方面。ndnSIM邮件列表在来自十几个国家的100多个成员中积极讨论ndnSIM的使用和发展[7]。

运行NDN试验台。对我们网络研发的实验方法至关重要的是一个大规模的测试平台，以评估应用程序和核心架构组件。在项目的第一年，NDN团队在华盛顿大学建立了一个本地测试平台，并配备了可编程路由器和一个广域覆盖测试平台，连接所有参与nsf资助的NDN项目的机构。本地测试平台支持NDN原型实现的基线评估，广域测试平台支持NDN组件的测试，包括视频流、会议工具和路由协议。监控脚本和可视化工具促进了测试平台管理[8]。虽然NDN团队鼓励研究人员创建自己的测试平台，但它也接受外部站点连接到NDN项目测试平台[9]的请求。

5. 开放问题

Ververidis等人。[29]提供了许多现有ICN项目的调查，并确定了社区中几个重要的争论，最值得注意的是与可扩展信任管理和命名本身的策略有关。

与其他ICN设计一样，NDN通过使用密码学来实现数据的真实性、保密性和完整性。密钥用于通过签名将名称绑定到数据，并通过加密来保护数据(或名称)。因为这些密钥本身被命名为数据，所以可以利用NDN架构的所有特性来解决密钥管理的常见挑战，例如分发和撤销;这是一个活跃的研究领域。高性能加密算法的开发和集成也是必不可少的。然而，最重要的挑战是稳健和可用的信任管理，它允许内容消费者在给定的上下文中确定可接受的签名密钥。

此外，大多数提出的ICN体系结构依赖于自认证名称，这使得任何节点都能够验证数据包中的名称与其内容是否匹配。然而，自认证名称要求每个应用程序必须确定内容是否是所需的内容，如果使用与应用程序名称的二次绑定，则会产生额外的安全风险。NDN提供了一种不同的方法，直接从应用程序中获取每个数据包的数据名称，然后将这些名称安全地绑定到内容。因此，命名空间设计是一个关键的研究领域，因为它将应用程序的数据、通信和存储模型与NDN中名称的路由和安全含义结合在一起。除了基于这些名称的可扩展转发之外，NDN研究的一个重要挑战是为当前和预期的应用程序架构开发和评估命名空间和相关协议设计，并找到可应用于常见用例的可重用方法。

最后，在与社会科学家的合作下，我们正在探索NDN的社会影响，特别是与今天的TCP/IP架构形成鲜明对比的四个方面:对语义分类、来源、发布和分散通信的支持。我们相信，这些特性将增加言论自由、安全、隐私和匿名的机会，同时提出有关数据保留和内容监管[25]的新挑战。

6. 展望

应用驱动的实验性NDN研究方法取得了进展，并为NDN [15]的原始愿景提供了新的深度。但该团队在命名空间结构和导航、信任模型和管理机制、可扩展转发和路由、转发策略设计、分布式数据同步以及会合、发现和引导等方面的研究只触及了表面。我们已经为一组试验性NDN应用程序展示了合理的命名方法，并对剩余的挑战有了更清晰的了解。我们实现了一个支持传统链路状态和双曲线路由的NDN路由协议。我们勾画了Sync的初步设计方法，这是一种支持跨集合数据同步的新型传输。同步填补了NDN网络层简单的兴趣-数据交换和分布式应用程序同步其数据集的需求之间的空白。

幸运的是，其他与NDN密切相关的研究工作正在世界各地进行，正如学术研讨会和会议活动的增长所表明的那样。NDN团队已经采取了一些措施，希望能将更广泛的社区参与到项目的下一阶段。特别是，NDN网站定期发布软件更新、测试平台文档、技术和年度报告、常见问题解答和博客条目，并为对技术讨论感兴趣的用户存档NDN兴趣公共邮件列表。

注:除了作者之外，原始NDN FIA项目的其他pi有:Tarek Abdelzaher (UIUC)， Daniel Massey (CSU)， Gene Tsudik (UCI)， Ersin Uzun和Jim Thornton (PARC)，以及Edmund Yeh (东北大学)。国家科学基金资助项目包括:CNS-1040868 (UCLA)， CNS-1039646 (UCSD)， CNS-1039585(CSU)，CNS-1039615(亚利桑那州立大学)，CNS-1205562(东北)，CNS-1040380 (UIUC)， CNS-1040643(华盛顿)。美国)，CNS-1040802(加州大学欧文分校)，CNS-1040036(孟菲斯)和CNS-1040822 (PARC)。

[6]The NDN team is currently working on establishing an in-tellectual property consortium to navigate the complex is-sues related to patents on NDN-related technologies.

[7] http://www.lists.cs.ucla.edu/mailman/listinfo/ndnsim

[8] http://ndnmap.arl.wustl.edu/

[9] http://named-data.net/ndn-testbed/

7. 参考文献

[1] NS-3-based NDN simulator. http://ndnsim.net.

[2] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker. Naming in content-oriented architectures. In ACM SIGCOMM Workshop on Information-Centric Networking (ICN), 2011.

[3] M. Abadi. On SDSI's linked local name spaces. Journal of Computer Security, 6(1-2):3–21, Oct. 1998.

[4] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang. Interest flooding attack and countermeasures in Named Data Networking. In Proc. of IFIP Networking, May 2013.

[5] C. Bian, Z. Zhu, A. Afanasyev, E. Uzun, and L. Zhang. Deploying key management on NDN testbed. Technical Report NDN-0009, Rev.2, Feb 2013.

[6] M. Bogu☒ na´, F. Papadopoulos, and D. Krioukov. Sustaining the Internet with Hyperbolic Mapping. Nature Comms, 1:62, 2010.

[7] J. Burke, P. Gasti, N. Nathan, and G. Tsudik. Securing instrumented environments over Content-Centric Networking: the case of lighting control. In IEEE INFOCOM 2013 NOMEN Workshop, Apr. 2013.

[8] CCNx. Ccnx software. http://www.ccnx.org.

[9] P. Crowley. Named Data Networking (Demo). In China-America Frontiers of Engineering Symposium, Frontiers of Engineering, 2013.

[10] S. K. Fayazbakhsh, Y. Lin, A. Tootoonchian, A. Ghodsi, T. Koponen, B. Maggs, K. Ng, V. Sekar, and S. Shenker. Less pain, most of the gain: Incrementally deployable ICN. SIGCOMM Comput. Commun. Rev., 43(4), Aug. 2013.

[11] G. Grassi, D. Pesavento, G. Pau, R. Vuyyuru, R. Wakikawa, and L. Zhang. VANET via Named Data Networking. In IEEE INFOCOM NOMEN Workshop, Apr. 2014.

[12] T. R. G. Green and M. Petre. Usability analysis of visual programming environments: a "Cognitive dimensions" framework. Journal of Visual Languages and Computing, 7 (2), 1996.

[13] J. Y. Halpern and R. van der Meyden. A logic for SDSI's linked local name spaces. In IEEE Computer Security Foundations Workshop, 1999.

[14] A. Hoque, S. O. Amin, A. Alyyan, B. Zhang, L. Zhang, and L. Wang. Named-data link state routing protocol. In ACM SIGCOMM ICN Workshop, 2013.

[15] V. Jacobson, , D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard. Networking named content. In CoNEXT, 2009.

[16] D. Krioukov, F. Papadopoulos, M. Kitsak, A. Vahdat, and M. Bogu☒ na´. Hyperbolic geometry of complex networks. Physical Review E, 82:036106, 2010.

[17] D. Kulinski and J. Burke. NDN Video: Live and Prerecorded Streaming over NDN. Technical Report NDN-0007, Sept 2012.

[18] P. Mahadevan, D. Krioukov, M. Fomenkov, B. Huffaker, X. Dimitropoulos, kc claffy, and A. Vahdat. The Internet AS-level topology: Three data sources and one definitive metric. Comput Commun Rev, 36(1), 2006.

[19] I. Moiseenko and L. Zhang. Consumer-Producer API for NDN. Technical Report NDN-0017, Feb 2014.

[20] NDN Team. Named Data Networking (NDN) Project 2012 - 2013 Annual Report, Sept 2013.

[21] NDN team. NDN Forwarding Daemon, 2014. http://named-data.net/doc/NFD/current/.

[22] NDN team. NDN Platform, 2014. http://named-data.net/codebase/platform/.

[23] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang. Securing building management systems using named data networking. IEEE Network Special Issue on Information-Centric Networking, Apr 2014.

[24] W. Shang, J. Thompson, M. Cherkaoui, J. Burke, and L. Zhang. NDN.JS: A JavaScript Client Library for Named Data Networking. In IEEE INFOCOM 2013 NOMEN Workshop, Apr 2013.

[25] K. Shilton, J. Burke, kc claffy, C. Duan, and L. Zhang. A World on NDN: Affordances and Implications of NDN. Technical Report NDN-0018, April 2014.

[26] W. So, A. Narayanan, and D. Oran. Named data networking on a router: Fast and DoS-resistant forwarding with hash tables. In ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), Oct 2013.

[27] M. Varvello, D. Perino, and J. Esteban. Caesar: A content router for high speed forwarding. In ACM SIGCOMM Workshop on ICN, 2012.

[28] L. Wang, A. K. M. M. Hoque, C. Yi, A. Alyyan, and B. Zhang. OSPFN: An OSPF-based routing protocol for NDN. Technical Report NDN-0003, July 2012.

[29] G. Xylomenos, C. Ververidis, V. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. Katsaros, and G. Polyzos. A survey of information-centric networking research. IEEE Communications Surveys Tutorials, 2013.

[30] C. Yi, J. Abraham, A. Afanasyev, L. Wang, B. Zhang, and L. Zhang. On the role of routing in Named Data Networking. Technical Report NDN-0016, Dec 2013.

[31] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang. A case for stateful forwarding plane. Computer Communications: ICN Special Issue, 36(7):779−791, April 2013.

[32] C. Yi, A. Afanasyev, L. Wang, B. Zhang, and L. Zhang. Adaptive Forwarding in Named Data Networking. ACM SIGCOMM CCR, 42(3), 2012.

[33] H. Yuan and P. Crowley. Scalable pending interest table design: From principles to practice. IEEE INFOCOM, 2014.

[34] H. Yuan, T. Song, and P. Crowley. Scalable NDN forwarding: Concepts, issues and principles. In ICCCN, 2012.

[35] Z. Zhu and A. Afanasyev. Let's ChronoSync: Decentralized dataset state synchronization in NDN. In ICNP, 2013.

[36] Z. Zhu, C. Bian, A. Afanasyev, V. Jacobson, and L. Zhang. Chronos: Serverless multi-user chat over NDN. Technical Report NDN-0008, October 2012.

[37] Z. Zhu, J. Burke, L. Zhang, P. Gasti, Y. Lu, and V. Jacobson. A new approach to securing audio conference tools. In Asian Internet Engineering Conference, AINTEC, 2011.