

信息中心网络 ICN 体系结构研究进展

李军, 陈震, 石希

清华大学 计算机系

信息技术研究院网络安全实验室

信息国家实验室

北京 100084

e-mail: ljun852@gmail.com

摘要: 当前的互联网体系结构是基于终端间包交换的点到点连接通信架构。随着实时视频、语音等通信业务量的日益激增, 由于TCP/IP体系固有结构的束缚, 互联网传输、处理这些实时多媒体数据的能力受到越来越大的挑战, 体现在效率低下、用户体验差。信息中心网络 (Information-Centric Networking, ICN) 应运而生, 它将内容与终端位置剥离, 通过对内容进行命名和基于内容名字的路由开展了对互联网体系结构变革的研究探索。

关键词: 网络体系结构; 未来网络体系结构; 信息中心网络

Advances in Research on Information-Centric Networking

LI Jun, CHEN Zhen, SHI Xi

Department of Computer Science and Technology

Research Institute of Information Technology (RIIT)

Tsinghua National Lab for Information Science and Technology (TNLIST)

Tsinghua University, Beijing, China, 100084

e-mail: ljun852@gmail.com

Abstract: The current Internet architecture is based on packet switching between the end to end communication architecture. With the growing surge of multimedia traffic and other communication services, especially video traffic, this architecture comes under increasing challenges in delivering contents over the Internet due to the obstacles of its inherent structure, which results in low content distribution efficiency, long retrieval latency and poor user experience etc. Information-Centric Networking (ICN) comes into being and tries to rescue this situation in this context. ICN separates content with the place where it stored, and brings out a new hot wave in research for the future Internet architecture.

Keywords: network architecture; the future network architecture; Information-Centric Networking

基金项目: 本文研究受国家 973 项目 (编号: No.2011CD302600, No.2011CB302805, No.2012CB315800) 和国家自然科学基金 A3 重点基金项目 (编号: No.61161140320) 资助。

作者简介: 李军 (1980-), 男, 山东, 硕士生, 主要研究领域为网络存储, 网络安全; 陈震 (1976-), 男, 浙江, 副研究员, 工学博士, 主要研究领域是网络安全, 云存储, 社交媒体; 石希 (1980-), 男, 山东, 硕士生, 主要研究领域网络安全。

本文通信联系人: 李军, 北京, 100084, 清华大学信息技术研究院网络安全实验室

1 研究背景

互联网上视频和话音通信业务量正在日益激增，高清视频点播服务无疑将进一步凸显TCP/IP体系结构所存在的数据传输瓶颈。P2P（Peer-to-Peer）系统诸如Bit Torrent被广泛应用于多媒体数据的传输，但是其传输效率也不理想，因为Peer只能从很小一部分Peer中获取数据块，总的来说就是在Peer下载同样的内容和网络拓扑时只拥有很有限的信息。信息中心网络（Information-Centric Networking，以下简称ICN）[1]（还有一种提法是Content Oriented Networking，CON）在这一背景下应运而生，它将改变当前互联网端到端的通信机制，把内容与终端位置剥离，通过发布/订阅范式（Publish/Subscribe Paradigm）来提供存储和多方通信等服务。ICN的提出，将用户的关注点由终端改为内容，即用户不用再关心从何处去获取自己想要的数据，而只需关心想要的内容是什么。

当前在 ICN 的研究方面涌现出了不少方法或者称为工程应用项目，可以划分为欧、美两大分支，在欧洲，主要有 PURSUIT（Publish-Subscribe Internet Technologies）、PSIRP（Publish-Subscribe Internet Routing Paradigm）、4WARD-NetInf（Network of Information，以下简称 NetInf）、SAIL（Scalable and Adaptive Internet Solutions）和 ANR-CONNECT（Content-Oriented Networking: a New Experience for Content Transfer），其中 PURSUIT/SAIL/PSIRP/4WARD-NetInf 受到 European Community's Seventh Framework Programme（FP7）的资助[3]，ANR-CONNECT 受到法国国家研究局资助。在美国，主要有 CCN/NDN（Content Centric Networking/Named Data Networking）和 DONA（Data Oriented Network Architecture）。

2 发布/订阅范式

发布/订阅范式或系统（Publish/Subscribe Paradigm）[11]是消息队列范例的一种，是一个更大的消息中间件系统的一部分。发布者只负责发布信息，订阅者可以订阅多个发布者所发布的信息，两者之间不用理会是谁发布和谁订阅，而通过一个信息管理器（如图1中的“事件服务”）来处理两者之间的发布/订阅逻辑。

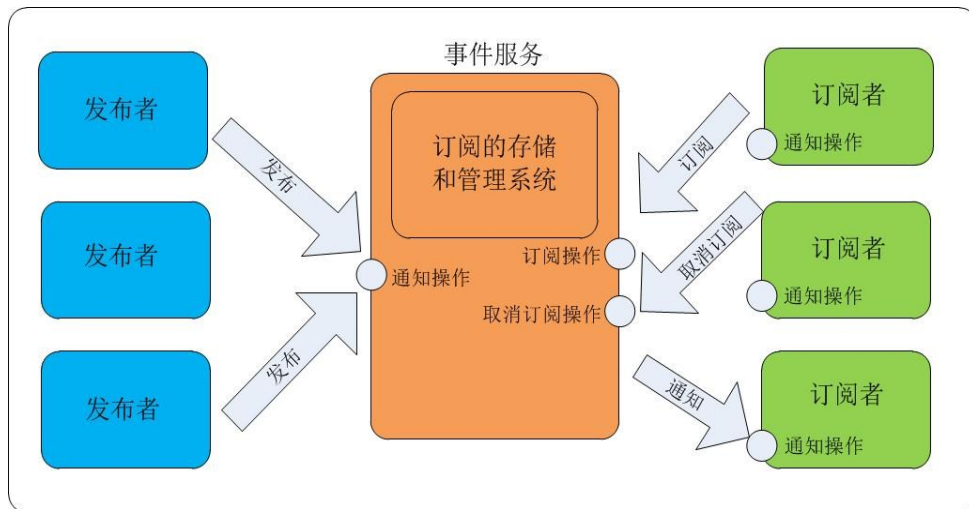


图1 一个简单的发布/订阅系统结构

如图1所示，发布/订阅系统模型依赖于“事件服务”来为事件的订阅和高效传输提供存储和管理。订阅者通过“订阅操作”来注册其感兴趣的事件，而无需了解这些事件的有效源。发布者通过“发布操作”来产生事件。“事件服务”将事件传送给所有相关订阅者，每个符合需求的事件都将通知到订阅者。“事件服务”将信息的产生和消费进行解耦，消除了参与者间的依赖，增强了可扩展性。这极大地减少了协调工作，使不同实体实现同步，并使所产生的通信基础设施能够很好地适应异步的分布式环境，如移动环境。

3 体系结构

文献[5-10]开展了以内容为中心的应用和高效服务的研究。ICN本质是在网络层将内容与终端进行了剥离。ICN的体系结构可以概括为四个方面：对内容进行命名；路由；传输和缓存内容。ICN相对于传统的TCP/IP

体系结构，主要有3个方面的显著区别[4]：

1.ICN节点以基于内容的名字进行路由，而不是基于终端位置。这将带来两个改变：

①以识别内容取代了识别终端。

②内容文件的位置与其名字剥离。在TCP/IP体系中，IP地址既是身份识别也是位置信息。

正是因为进行了这样的剥离，ICN在进行内容命名和路由时不存在位置依赖，从而摆脱了移动性问题束缚。

2.ICN采用发布/订阅范式或系统（Publish/Subscribe Paradigm）作为主要传输模型。内容发布者发布一个内容文件，用户可以内容名字来索取这份文件内容。在TCP/IP体系中，用户需要知道哪个数据源持有其感兴趣的文件，并且用户和数据源终端在整个数据传输过程中需要保持关联。ICN通过发布/订阅系统，将内容的产生、使用在时间和空间上进行了分离，从而使得内容传输效率更高、可扩展性更好。

3.数据的合法性可以方便地经公钥加密来进行认证。在TCP/IP体系中，用户所看见的终端地址与内容名字不相干，这将导致钓鱼攻击和网域交接攻击。ICN可以采用扁平的命名方法来进行内容命名（将在后面介绍）或给数据包进行签名，从而大大提高了安全性。

3.1 命名方法

1.分层命名（Hierarchical, human-readable naming）

CCN[6]和TRIAD[8]采用了分层命名方法对内容进行命名。这种命名是自由形态的层级，是人可读的字符串序列[2]。便于理解、记忆，加密算法变化时名字可以保持不变。这种命名与web URL相似，并且是可聚合的，因此能够方便地与URL相匹配，这意味着在当前网络环境上进行部署时将较为容易。如图2所示，如果所有内容的名字都是以www.nrc.nl开始并存储在一个节点上，那么这些内容就只需要一个路由入口。不过也存在如果同一内容文件被复制存储到多个节点上，聚合程度降低的问题。

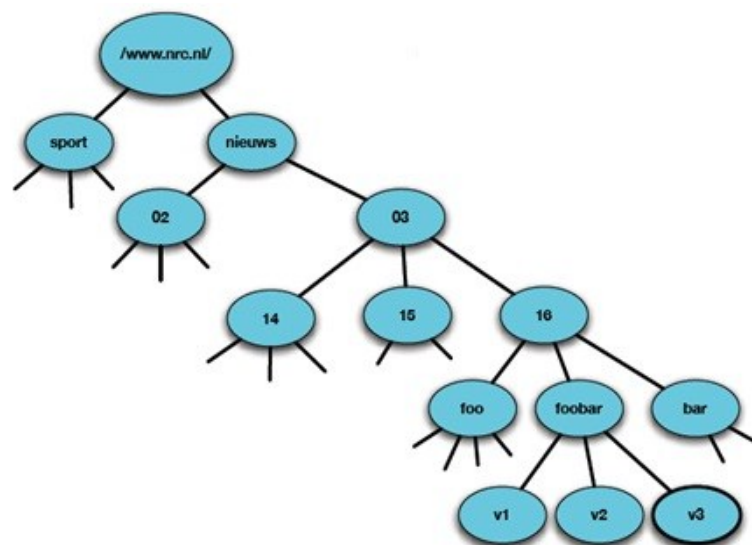


图2 分层命名示例

2.扁平命名（Flat, self-certifying naming）

DONA[5]、PSIRP[9]和NetInf[7]采用了扁平命名方法进行内容命名，其格式是P:L，P是内容发布者公钥的加密哈希，L是标签[2]。这样的命名是没有语义的哈希串，具有较好的稳定性和唯一性，但也带来了不便于理解、记忆，加密算法升级后名字将发生变化等问题。

3.基于属性的命名（Attribute-Based Naming）

与CCN、DONA不同，CBCB[10]采用属性值对（Attribute-Value Pairs, AVPs）来命名内容。用户通过AVPs的合取和析取来表示其索要的内容，因此ICN节点可以通过对比广播的AVPs与内容源来定位合适的内容，这样能提高网络内部的搜索和路由效率。不过也存在AVP不唯一、语义含糊、数量过大等问题。

4.分层命名和扁平命名方法的比较

鉴于分层命名和扁平命名两种方法的关联性，下面对它们做一对比。

1.基本绑定

这两种命名方法都要对下面三个实体建立两两绑定，目的是增强安全性。

●RWI（Real-World Identity），即“真实身份”，是真实世界中的人或组织名称。

●Name，即“名字”，是提交到网络中用于进行内容索取时的名字，由发布者负责。文献[2]用principal指代内容发布者这一角色，其不仅创建、提供内容，更要证实、担保内容。可以看出在ICN体系中，更重视内容源头的合法性。

●Public Key，即“公钥”，每个内容发布者都关联一对公钥和私钥，订阅者使用公钥核实RWI确实签署了内容。

将RWI-public key和public key-name这两对绑定称为可信机制。

2.安全性比较

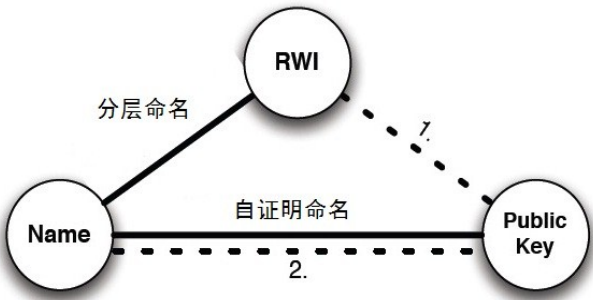


图3 基本绑定

如图3所示，分层命名的内在绑定是RWI-name，扁平命名的内在绑定是public key-name。两种方法都需要一种外部认证来提供另一种绑定，分层命名需要的是public key-name绑定，扁平命名需要的是RWI-public key绑定。表1和表2分别对两种方法的安全性和绑定特性进行了比较。

表1 分层命名与扁平命名方法的安全性比较

命名方法	绑定的可靠性和健壮性	数据确认的时机	
		数据一经产生就确认	取得数据才确认
分层命名	内在绑定RWI-name是脆弱的，依赖于name是便于理解的且明确的	需要外部机制来绑定name和public key。网络需要了解与特殊当事人相关的外部可信机制，这将限制外部可信机制的使用	
扁平命名	内在绑定public key-name是健壮的，是强加密的	绑定public key-name本身就是内在的。网络可以直接要求内容发布者提供与内容相关的签名	在这种模式下，ICN必须在public key-name基础上运行，自然选取扁平命名方法更为合适

分层命名需要PKI（Public-key Infra Structure）提供绑定public key-name，而PKI需要根可信认证（Root Trust Authority）和策略的通用授权。

表2 绑定的比较

命名方法	绑定的可靠性和健壮性
------	------------

分层命名	其内在绑定RWI-name存在不足, 因此需要外部机制来提供两种绑定。需要PKI来对绑定public key-name进行翻译, 以使网络能够理解
扁平命名	提供了清晰的、算法化的内在绑定public key-name, 其该绑定能被网络所理解

分层命名和扁平命名方法均具有各自的优缺点。在形式上, 分层命名比扁平命名更便于人的理解、记忆, 并且其可聚合的特点也有利于控制路由规模, 但后者在安全性、灵活性方面则比前者更具优势。

3.2 路由方法

1. 无结构路由

这种结构类似于 IP 路由, 采用无结构来维护路由表, 因此其路由公告主要通过洪泛进行。CCN 采用了这种路由机构, 与 IP 路由存在继承关系, 因此与 IP 网络的兼容性较高, 也就意味着 CCN 将易于在当前 IP 网络基础上进行部署。CCN 用内容标识取代了网络前缀, 因此对于 IP 路由协议和系统的修改将不会太大。CCN 在路由是采用了可聚合的分层内容标识。需要注意的是, 随着内容复制和移动的激增将导致聚合程度降低, 控制通信的开支将增大。

2. 结构路由

有两种形式: 树状结构和分布式哈希表 (Distributed Hash Table, DHT)。DONA 采用了树状路由机制, 其路由器组成了一棵分层树, 每个路由器都维护其子路由器所发布的所有内容的路由信息。当一份内容文件发布、复制或删除时, 变更公告将通过树进行传播, 直到遇到相匹配的路由入口。根路由器将维护整个网络所有内容的路由信息, DONA 的内容命名是非聚合的, 其可扩展问题将会比较突出。PSIRP 采用了分布式哈希表路由机制。哈希表由随机的、统一的路由器布局构成, 通常比树状结构维持了更长的路径, 这将便于提取网络拓扑结构信息。需要注意的是, 结构化路由的扁平性给路由器带来了对等的、规模的路由负担。这两种无结构路由形式相比较而言, 树形路由结构在传输性能方面具有优势, 而分布式哈希表路由结构在可扩展性和弹性方面具有优势[12]。

3.3 多源传输

ICN 的发布/订阅系统非常适应一对多的连接传输[5,9], 这一点可以说是 ICN 与生俱来的。对于多对多的连接传输, 这里有两种情况: 一是 M 个不同实体传输给 N 个接收者, 二是 M 个源将一个内容的不同部分传输给 N 个接收者。对于后者, 其典型应用就是 P2P 系统。

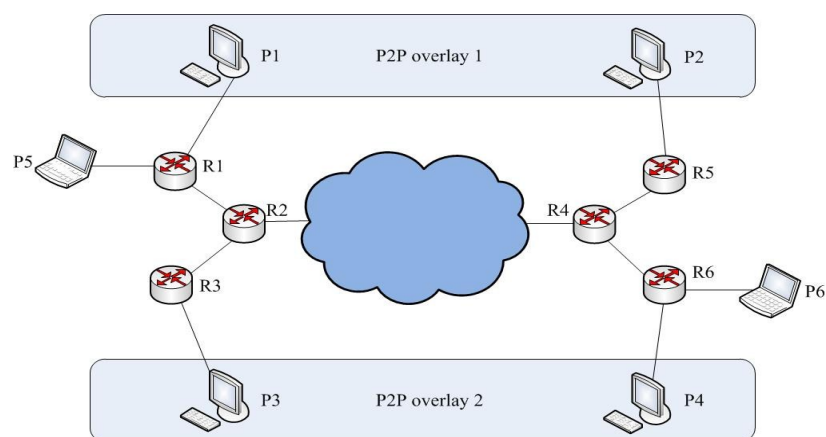


图 4 CON 与 P2P 覆盖网传输对比

如图 4 所示, P2P overlay 1 和 P2P overlay 2 是两个覆盖网, 它们将下载同一份文件。因为 P2P 系统是在应用层的通信解决方案, 其提取网络拓扑信息的能力较弱。而 ICN 将向接收者 (P1-P6) 高效地传输内容文件, 因为 R2 和 R4 节点将帮助接收者从其他覆盖网中下载文件。实际上, R2 和 R4 将内容进行了缓存, 接收者不用再到数据源头去索取数据, 所以其传输效率更高。

3.4 扩展性

首先给出一个定义, 信息对象 (Information Objects, 以下简称 IO): 独立于存储位置和物理表象的信

息本身。

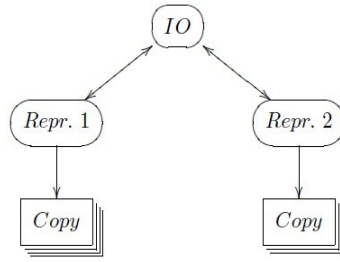


图 5 IO[3]

如图 5 所示，一个 IO 可以拥有多个不同的表现形式，如统一的二进制代码格式可以代表同一信息，而每个表现形式可以拥有多个副本。

当前 IP 网络的主要扩展性指标是骨干路由器中路由表 IP 地址前缀的数量。而在 ICN 中，主要扩展性指标是 IO 数量。截至 2010 年底，在 DNS 注册的二级域名数量达到了 1.18 亿，那么 IO 的数量将是多大呢？

NetInf 的 IO 采用扁平命名，其名字解析系统要为每个 IO 提供一个入口，因此需要巨大的名字空间。如果路由能在 NetInf 的名字认证标签进行聚合，其名字空间规模将达到前面所提到的二级域名的规模水平。

CCN 的 IO 采用分层命名，其全局路由系统至少需要在内容提供商层面处理 IO 名字前缀，此外，每个包的转发状态将沿着传输路径把数据包引导给用户。CCN 的名字前缀数量也将到达二级域名的规模水平；

PSIRP 的 IO 采用扁平命名，扁平集合在分布的作用域上进行处理。作用域的地位相当于 DNS 入口，作用域的数量将至少为当前 DNS 服务器的数量。

DONA 的解析层基于分层的名字解析服务（Name Resolution Service, NRS），其全局规模将达到 DNS 的规模。

3.5 移动性

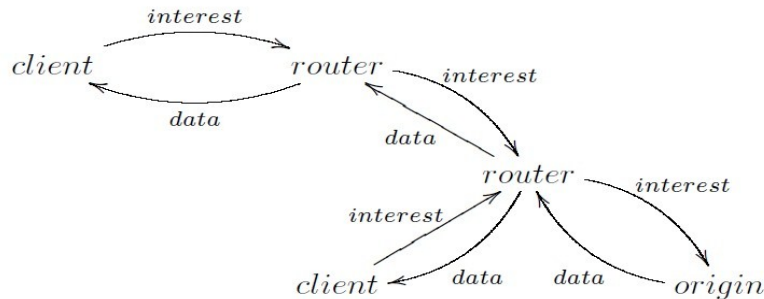


图 6 CCN 运行原理[3]

如图 6 所示，在 CCN 中，对 IO 的需求是朝着已发布了的 IO 所存在的位置进行路由。如果对一个 IO 的需求很多，则路径上所有节点将缓存该 IO 的副本。用户的移动是内在的，策略层将会关注转换并重新发布所有的待请求，而不需要等到 time-out。内容提供商的移动相对复杂一点，其必须更新所有邻居节点的路由表，这会比较慢。而且，内容提供商移动时，特殊前缀将会造成路由表污染，这将削弱前缀聚合的优势。

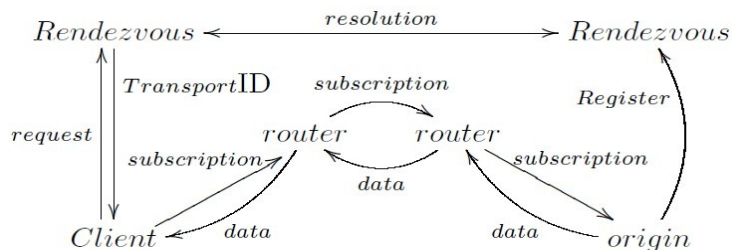


图 7 PSIRP 运行原理[3]

在 PSIRP 中, 发布和订阅通过 *Rendezvous System* 进行匹配。*Rendezvous* 的功能是在网络中定位发布内容和范围。*Rendezvous System* 由独立的 *Rendezvous Network* 组成, *Rendezvous Network* 提供存储发布内容广告的服务, 如图 7 所示。用户可以停止订阅, 转换网络并重新订阅, 新的路径将在路由层进行计算。缓冲和序列号允许无缝转移。内容提供商的移动要复杂一些, 并将牵涉到集合节点 (*Rendezvous Node*) 的路由状态更新, 其过程将是慢收敛的。

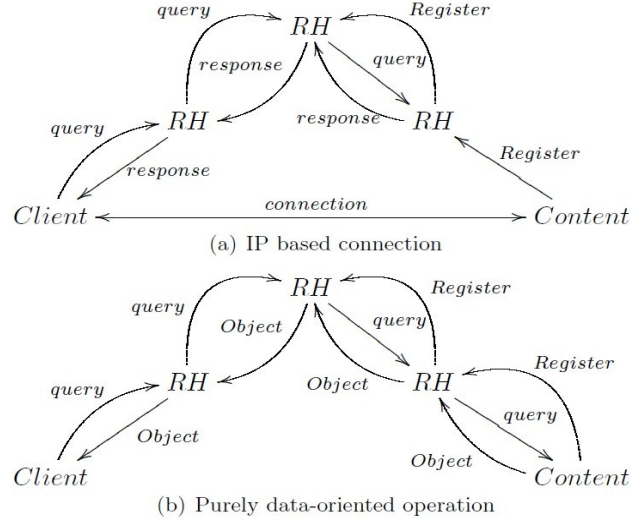


图 8 DONA 运行原理[3]

在 DONA 中, 节点将由数据注册器进行认证。内容一经注册, 对该内容的请求将路由到它。图 8 (b) 所展示模式中 IO 将沿着用户发出的请求的路径进行路由。DONA 的移动性与 PSIRP 相似, 用户注销原来的位置, 再重新注册新的位置。注销并不是强制的, 因为解析记号 (*Resolution Handler, RH*) 将会清除无法找到的内容记录。

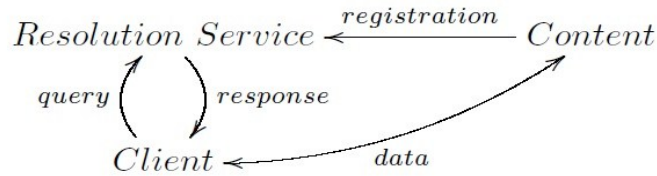


图 9 NetInf 运行原理[3]

如图 9 所示, 在 NetInf 中, 名字解析服务 (*Name Resolution Service, NRS*) 负责对 IO 和网络定位器进行注册。当订阅者想接收所需要的 IO 时, 该 IO 将由 *NSR* 解析到定位器集中, 这些定位器将从最佳的源那里接收 IO 副本。有一个中央集合点对着每个用户设备, 用户的无缝转移是可行的, 内容提供商的移动也是可行的, 但不是无缝的。

总的来看, ICN 中用户和内容提供商的移动都是可行的, 但用户的移动更容易实现, 所造成的影响也较小; 而内容提供商 (源) 的移动相对就要复杂一些, 并且代价较大, 将会影响路由系统的聚合性和扩展性。

3.6 安全性

ICN 的安全性由所采用的命名方法有着密切关系。由 2.1 中对命名方法的比较可以看出, 扁平、自证明的命名方法在安全性方面要优于分层命名方法。其中, DONA、PSIRP 和 NetInf 采用的扁平命名机制自身整合了名字认证, 但其可读性较差, 人机交互不是太理想; CCN 采用的分层命名机制可读性好, 但其名字认证需要第三方支撑。

3.7 隐私问题

ICN 被认为将会威胁到言论自由，因为经营管理者将会过滤不受欢迎的观点、内容或服务。而实际上，IO 的身份证明不会被加上更多的过滤功能，因为对象标识符被创立时用的是参与者的密钥，而不是拥有者的密钥。这里我们可以看看在 CCN 中，控制谁能够下载到特殊内容的唯一方法是控制所有处于最后一跳位置的路由器，也就是网络中的所有路由器，而这样做的代价是很大的。

4 ICN 工程应用实例对比

通过前面的描述，对 ICN 的命名和路由方法都有了一个基本了解，现对当前 ICN 的几种主要工程应用实例做一比较。

表 3 ICN 工程应用实例对比

项目	命名方法	命名方法优势	路由结构	路由规模	控制通信开销
CCN	分层命名	与 IP 兼容	无结构路由	N (最好情况) C (最差情况)	High
DONA	扁平命名	稳固	结构路由(树状结构)	C	Low
PSIRP	扁平命名	稳固	结构路由(分布式哈希表)	$\log C$	Low
NetInf	扁平命名	稳固	结构路由(多层分布式哈希表)	$\log C$	Low
TRIAD	分层命名	与 IP 兼容	无结构路由	N	High
CBCB	基于属性的命名	便于网内搜索	基于源的多播树	2^A	High

注： N 是发布（提供商）节点数量， C 是内容的数量， A 是属性的数量

如表 3 所示，CCN 和 TRIAD 采用了分层命名方法，因此它们与 IP 体系具有较好的兼容性，但其无结构路由的洪泛特性将会增大控制通信开销。在 TRIAD 中，如果同一内容发布者所提供的内容存储在一个节点上，那么这些内容的路由入口将聚合到一个节点上，因此路由规模与内容发布节点的数量成正比。而在 CCN 中，通过内容的复制将聚合的路由入口进行了分割，在最坏的情况下，其路由规模将取决于内容的数量。

DONA、PSIRP 和 NetInf 采用了扁平命名方法，在安全性等方面优势明显，同时其结构化的路由降低了控制通信开销。在 DONA 中，根路由节点要维护网内所有内容的路由信息，因此其路由规模也取决于内容数量。而 PSIRP 的分布式哈希表路由结构，将路由规模降低到所有内容数量的对数级别。

CBCB 独树一帜采用了基于属性的内容命名方法，这种命名方法便于进行网内搜索，并通过基于源的多播树进行内容传输。因为每个属性存在被选中或者不在搜索查询中的情况，因此一个路由器的路由入口数量将达到 2^A 。每个新的查询必须在整个网络进行洪泛，因此其控制通信开销较高。

5 总结与思考

ICN 作为一种具有革命性的网络体系结构，其提出的基于内容的路由通信方式带来了由“Where”到“What”的根本性转变，它致力于使互联网支持不考虑内容存储所在物理位置，而直接提供面向内容的功能。ICN 作为一个崭新的概念，其带给网络的革命性改变引人关注，已成为当前的热点研究领域。

这里，我们再从实际应用角度对文中所提到的 ICN 的工程应用实例做一回顾。目前，CCN 和 PSIRP 均提供了开放源代码服务（NetInf 需进行认证后提供代码）[13-15]，开发人员可以方便地利用其代码进行工程开发。特别需要提及的是 CCN，因为其继承了 IP 特性，与 IP 体系具有较好的兼容性，是在当前网络架构环境下将 ICN 理念转化为实际应用的较为便捷的技术途径。当然，这并不是说其他工程应用实例不利于部署实现，诸如 DONA 等在综合性能方面更为均衡，对其未来发展同样充满期待。

我们可以总结一下 ICN 所能带来的好处，数据的安全性更好（由命名机制所决定）、与生俱来支持多

路径路由、天然抵抗 DoS 攻击等等。但我们应该意识到, 这些好处也可以通过其他的办法或机制来实现, 并不一定要完全通过 ICN 来实现。也就是说, 互联网架构的变革将不仅仅是 ICN 这一条路。这条路到底好不好, 除了 ICN 自身的不断演进, 使其更加完善, 更需要检验衡量。

由此, 我们提出如下几个思考问题: 1.关于命名的问题, ICN 的安全模型基于名字的性能, 而不是内容的传输机制, 可以说“命名”是 ICN 的一个关键环节。目前的研究已给出了对内容进行命名的方法, 还需针对具体命名方法的制定命名规范, 否则可能造成命名的混乱, 并直接影响到 ICN 的可用性; 2.关于缓存的问题, 需要多大的缓存来维持 ICN 的正常运转? 太小了影响正常运转, 太大则浪费资源, 不符合绿色节能的要求; 有的内容不需要或者是不允许缓存, 如何判断和操作(其实这个问题涉及到了内容隐私问题)? 3.关于路由问题, 如何设计针对域内和域外的多源路由协议? 由于要缓存内容, 路由器的负担将加大, 对路由器的可靠性将提出更高要求; 4.关于安全问题, 由于存在洪泛, 如何抵御洪泛攻击? 如何抵御内容污染、恶意内容攻击? 这些问题都关系到 ICN 的可行逻辑, 值得深入研究。

References:

- [1] Ali Ghodsi et al., Information-Centric Networking Seeing the Forest for the Trees[C]. Hotnets'11, Cambridge, MA, USA. 6-18.
- [2] Ali Ghodsi et al., Naming in Content-Oriented Architectures[C]. SIGCOMM ICN'11, Toronto, Ontario, Canada, 2011. 1-6.
- [3] Bengt Ahlgren et al., A Survey of Information-Centric Networking[C]. <http://drops.dagstuhl.de/opus/volltexte/2011/2941>. 1-18.
- [4] Jaeyoung Choi et al., A Survey on Content-Oriented Networking for Efficient Content[C]. IEEE Communications Magazine, March 2011. 121-126.
- [5] T. Koponen et al., A Data-Oriented (and Beyond) Network Architecture[C]. SIGCOMM '07, 2007. 81-92.
- [6] V. Jacobson et al., Networking Named Content[C]. CoNEXT '09, New York, NY, 2009. 1-12.
- [7] Christian Dannewitz, NetInf: An Information-Centric Design for the Future Internet[C]. European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216041. 1-3.
- [8] M. Gritter and D. R. Cheriton. TRIAD: A New Next-Generation Internet Architecture[C]. <http://www-dsg.stanford.edu/triad/>, July 2000. 2-11.
- [9] Lagutin, D., Visala, K., and Tarkoma, S. Publish/Subscribe for Internet: PSIRP Perspective[C]. Towards the Future Internet - Emerging Trends from European Research, 2010. (Valencia FIA book 2010). 77-82.
- [10] A. Carzaniga et al., A Routing Scheme for Content-Based Networking[C]. IEEE INFOCOM '04, Hong Kong, China, Mar. 2004. 1-2.
- [11] Patrick Th. Eugster et al., The Many Faces of Publish/Subscribe[C]. ACM Computing Surveys, Vol. 35, No. 2, June 2003. 114-131.
- [12] Jaeyoung Choi et al., Performance Comparison of Content-oriented Networking Alternatives[C]. LCN, Switzerland, Oct. 2009. 1-4.
- [13] CCN: <http://www.ccnx.org/>
- [14] PSIRP: <http://www.psirp.org/>
- [15] NetInf: <http://www.netinf.org/home/home/>