内容中心网络
Content-Centric Network

土星组
网络安全实验室
信息技术研究院
清华大学
2011.11.22

背景——IP体系

- 互联网所承担的内容分发的压力越来越重
  - 信息急剧增长YouTube、Youku、BitTorrent….
  - 据Cisco预测，IP流量将以年复合增长率34%的速度增长，2014年全球的IP流量将达到每个月64 EB，而互联网上内容相关的流量将超过97.5%的份额
- 基于IP的互联网体系结构
  - IP网络在设计之初具有用户少、设备昂贵、应用简单、流量小等特点，因此确立了简洁而清晰的网络结构
  - 其体系建立在IP地址的基础上
  - “细腰结构”的突出特点：网络层简洁精干，将绝大多数工作交给上层去做

背景——IP体系

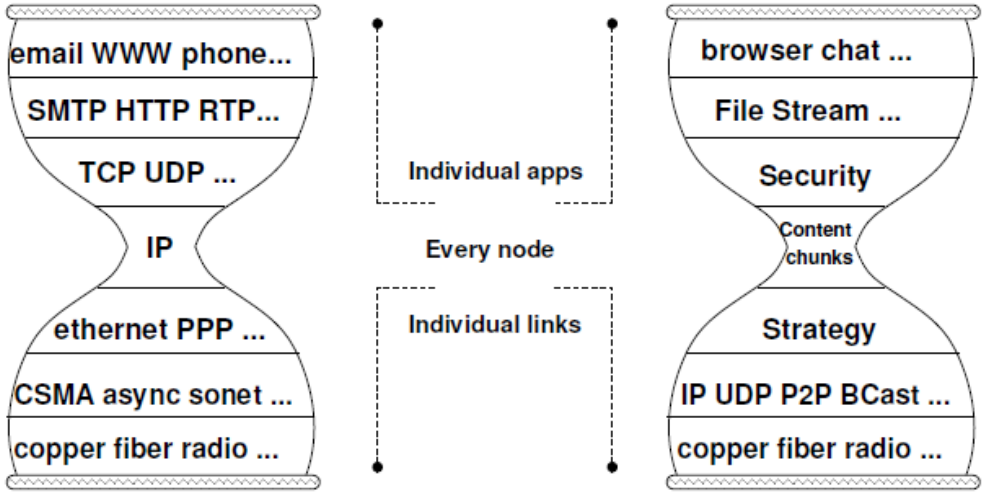
- IP体系结构已不再适应当前的网络状况
  - 网络终端移动性
    - 移动终端、智能手机、平板电脑
  - 网络多播
    - 网络流媒体
  - 网络安全
    - 目前只做到了数据容器（链路、服务器）的安全，而不是数据本身
- IP体系突出问题
  - 低效的数据分发
  - 数据的冗余传输
  - 路径安全性
- IP地址的双重属性(同时包含标识和位置信息)是导致目前互联网路由可扩展性、移动性差的根本原因

背景——改革

- 对目前互联网问题的解决方案
  - 增量式演进：应用层技术（CDN、P2P）
  - 革命式解决：ICN…
- ICN(Information Centric Network)
  - 目的：为了提出在网络上新的命名和路由模型
  - 以object ID为基础，object ID独立于网络位置
  - 目前有多个机构都在开展相关的方案研究
    - PSIRP： Publish-Subscribe Internet Routing Paradigm Europe
    - 4WARD-NetInf ： Network of Information Europe
    - DONA： Data-Oriented Networking Architecture USA
    - CCN/CCN： Content-Centric Network USA

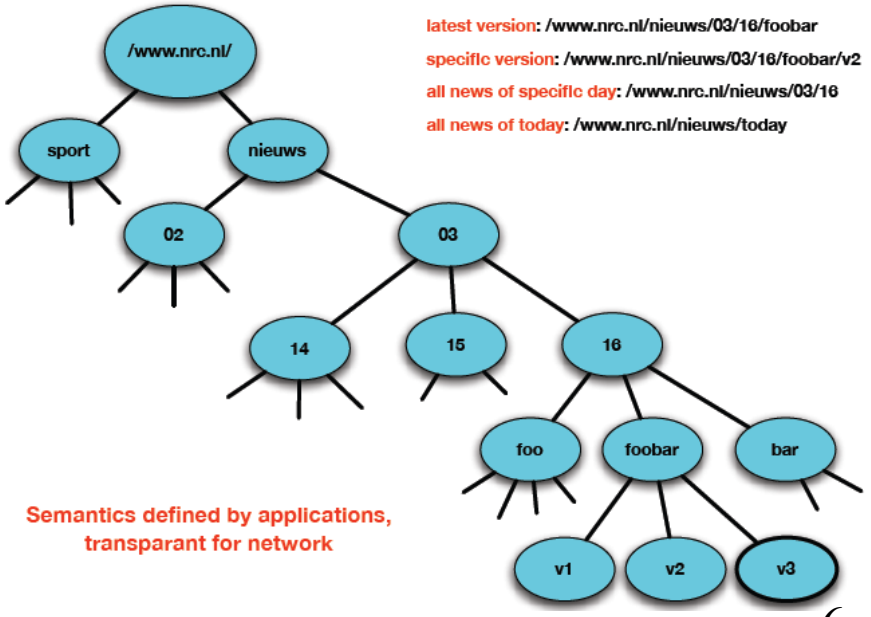
CCN的观点

- 存储网络化
  - 路由设备具备大容量存储能力，在路由器实现基于命名的数据缓存
- 网络的任务
  - CCN提出者认为网络设计的本来属性是为了数据分发而不是为了节点间的通信

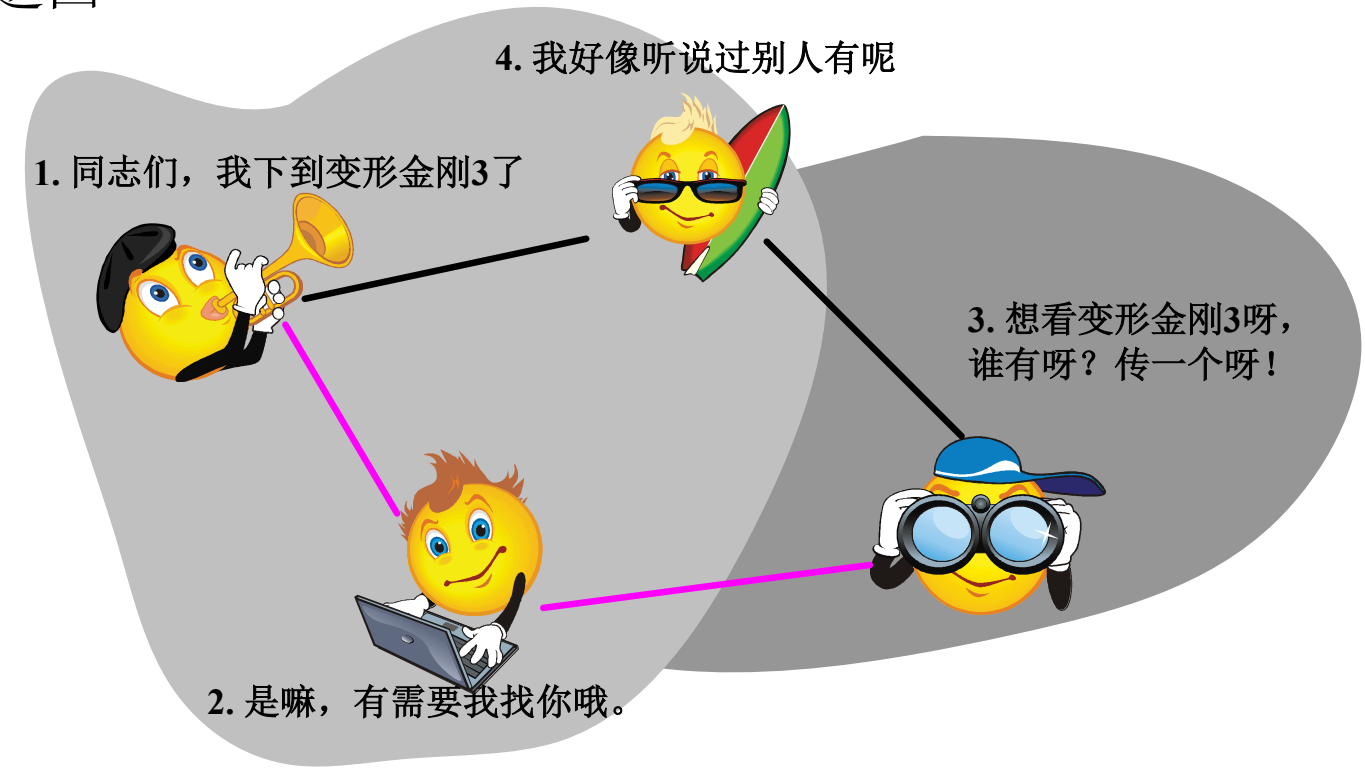


CCN命名

- CCN数据包都会拥有一个内容名称，同时该名称会被加密签名
- 层次化的结构命名，可以聚合
- 命名有时并不需要全局唯一，大多数为局部数据，那么通过局部广播/路由就可以获得（私有IP）

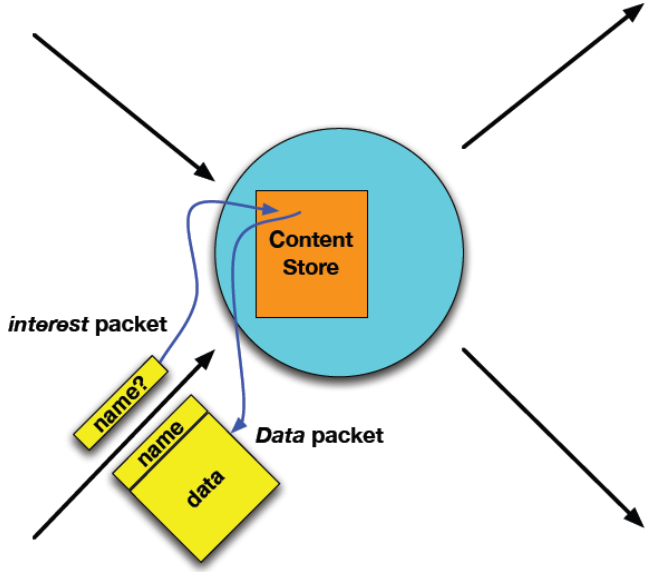


- 三向交换
  - 内容前缀广播
  - Interest数据路由
  - Data数据返回

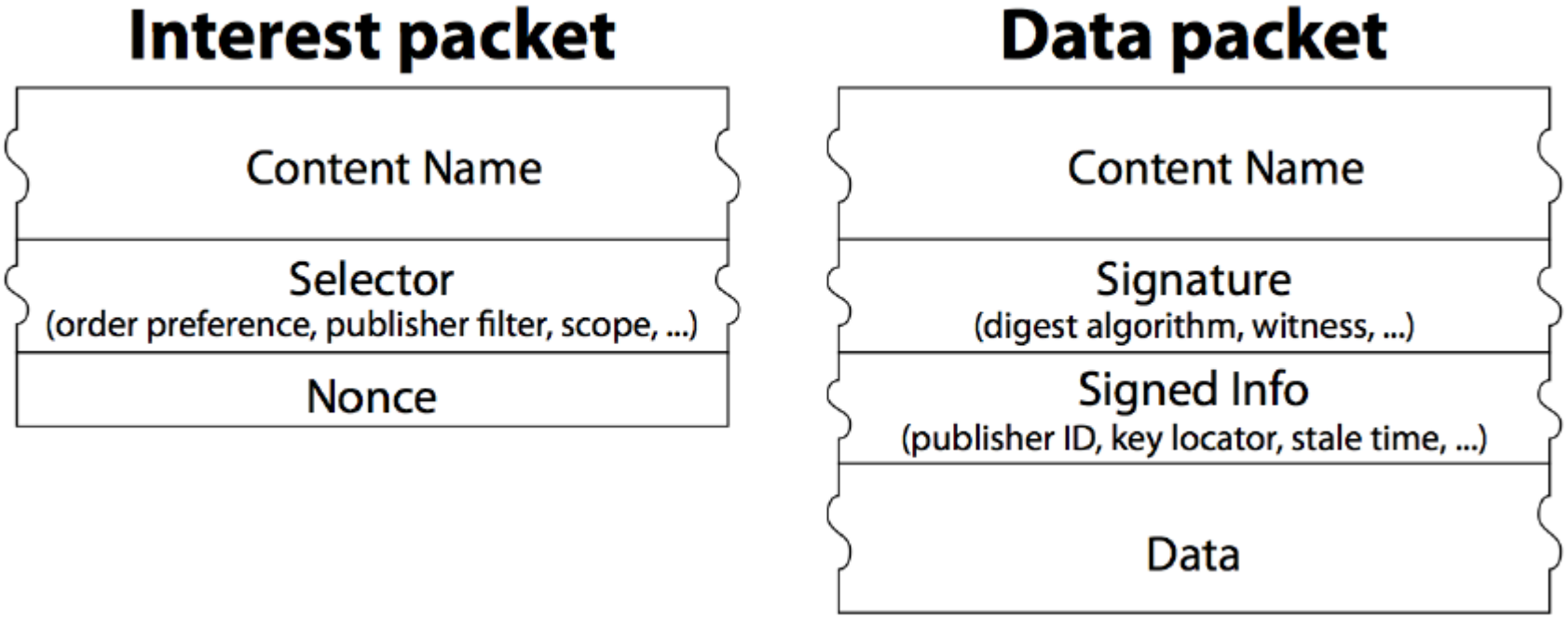


CCN

- CCN(Content Centric Network)
  - 对数据进行分片，每个数据片都有一个名字
    - /www.nrc.nl/nieuws/2011/03/14/foobar/v3
  - 请求数据时只需注明数据名称，而不需要声明去哪里取
    - 没有src，也没有dst
  - 两种包格式：Interest & Data



CCN包格式



- Interest Packet = 〈*name*〉
- Data Packet = 〈*name, data, signature*〉

CCN节点

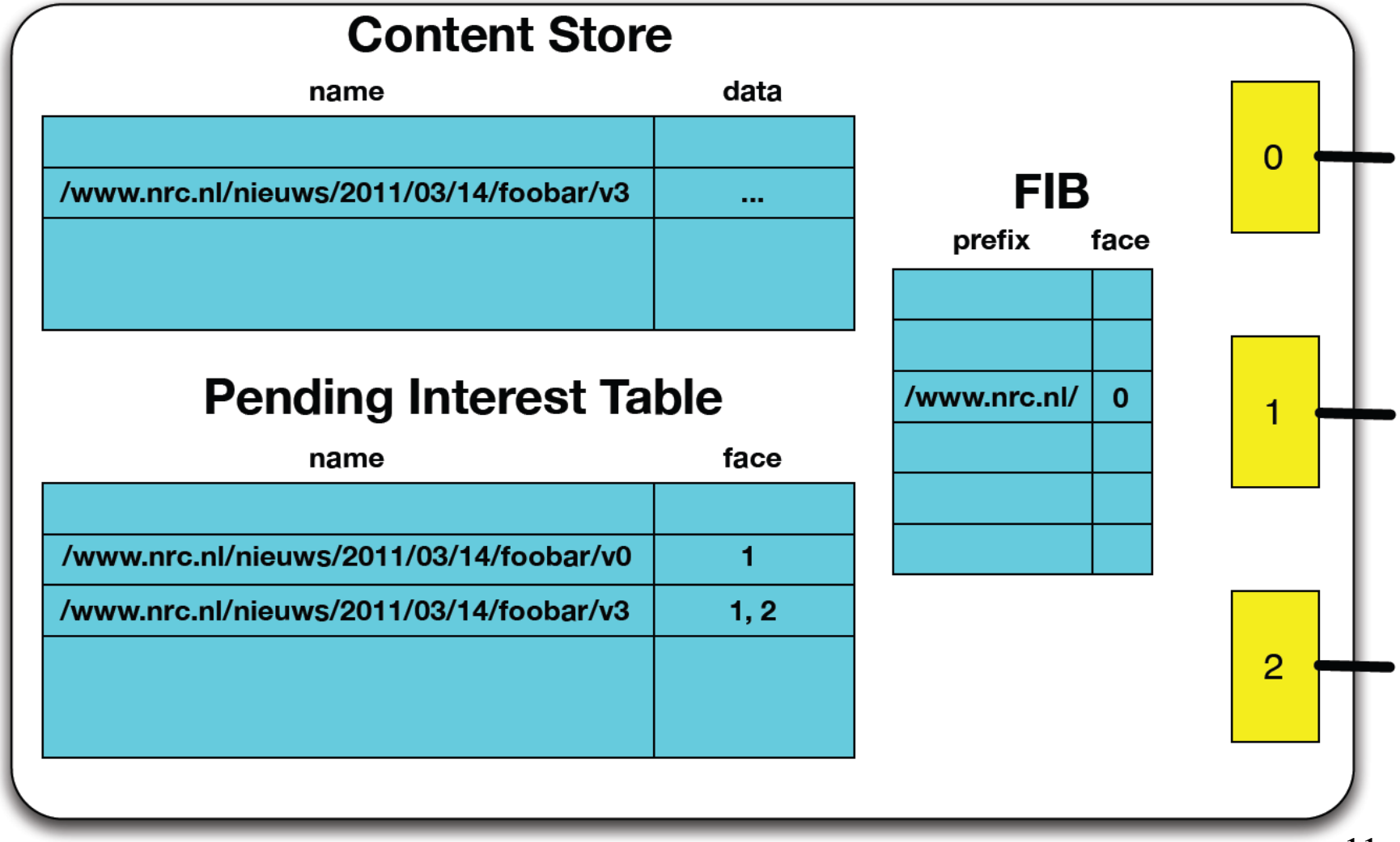
- 路由器要维护的表结构
  - Content Store

    数据缓存、缓存更新策略
  - Forwarding Information Base (FIB)

    由基于名称的路由协议生成
  - Pending Interest Table (PIT)

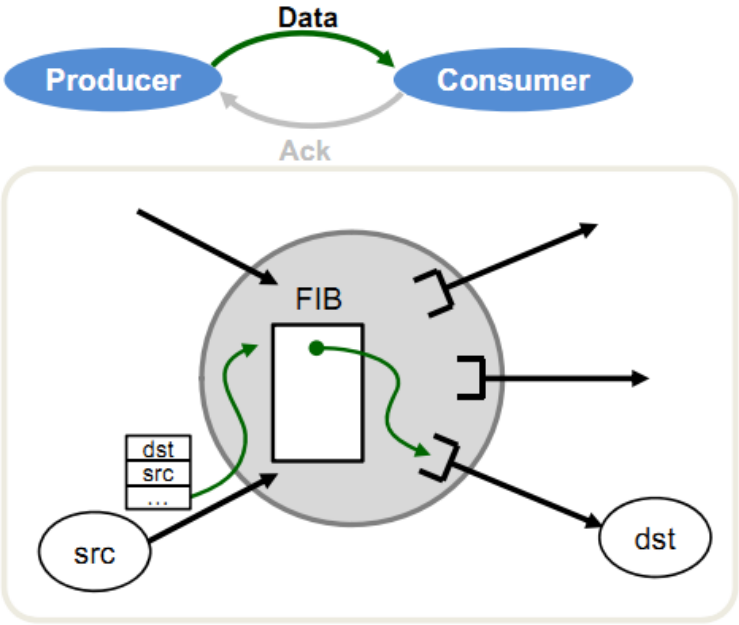
    Content Router会聚合下游网络对同一个内容的请求，用该表详细记录（广播和多播）

CCN节点

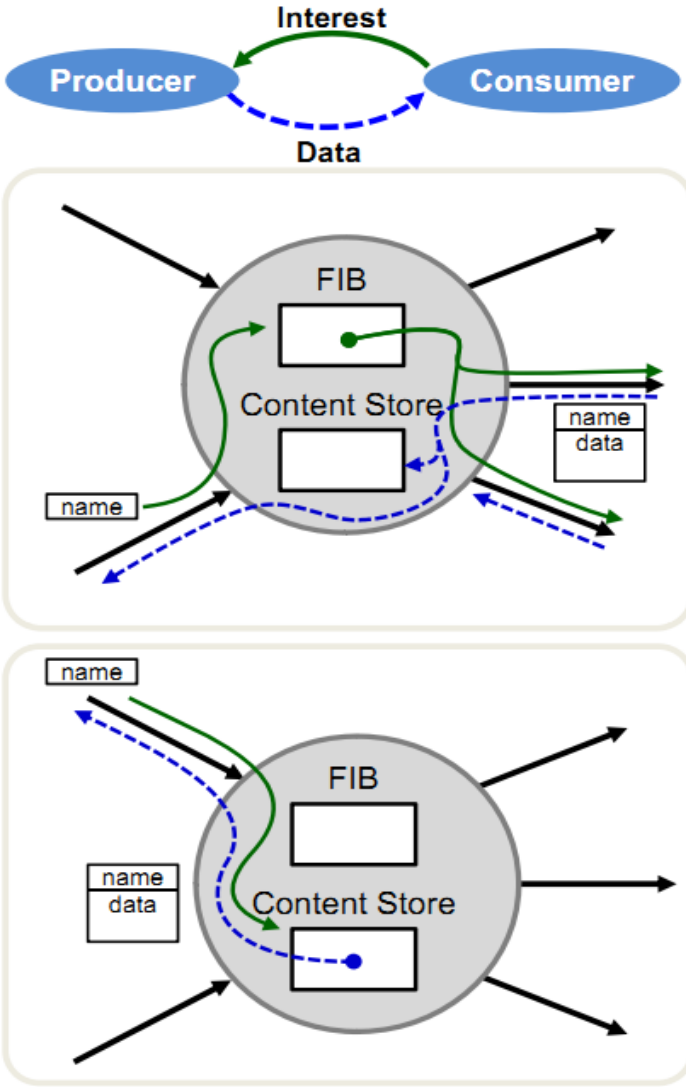

Content Store
name
data
/www.nrc.nl/nieuws/2011/03/14/foobar/v3
...
Pending Interest Table
name
face
/www.nrc.nl/nieuws/2011/03/14/foobar/v0
1
/www.nrc.nl/nieuws/2011/03/14/foobar/v3
1, 2
FIB
prefix
face
/www.nrc.nl/
0
0
1
2

CCN节点

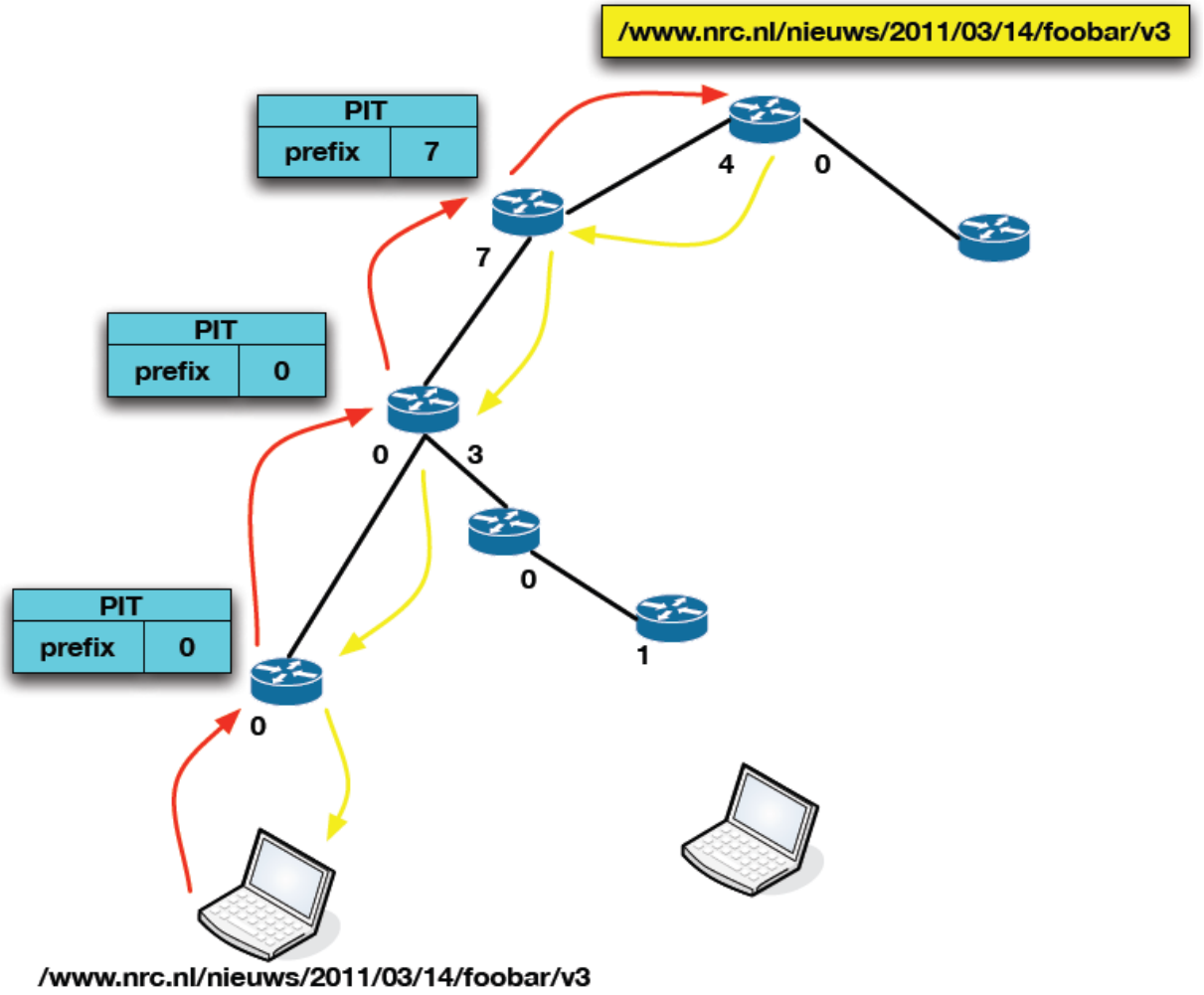
IP Packet Forwarding



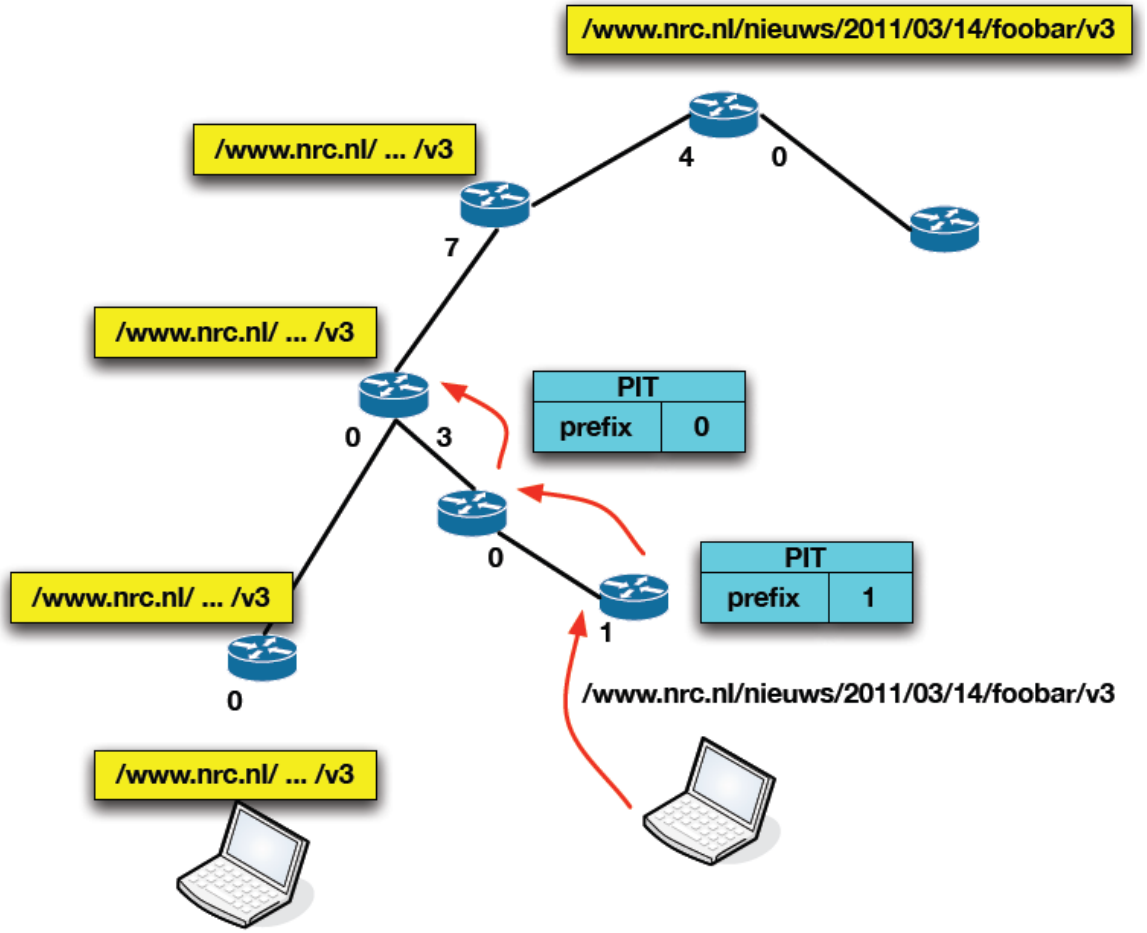
CCN Interest Forwarding



CCN路由


/www.nrc.nl/nieuws/2011/03/14/foobar/v3
PIT
prefix
7
PIT
prefix
0
PIT
prefix
0
4
0
7
0
3
0
1
0
/www.nrc.nl/nieuws/2011/03/14/foobar/v3

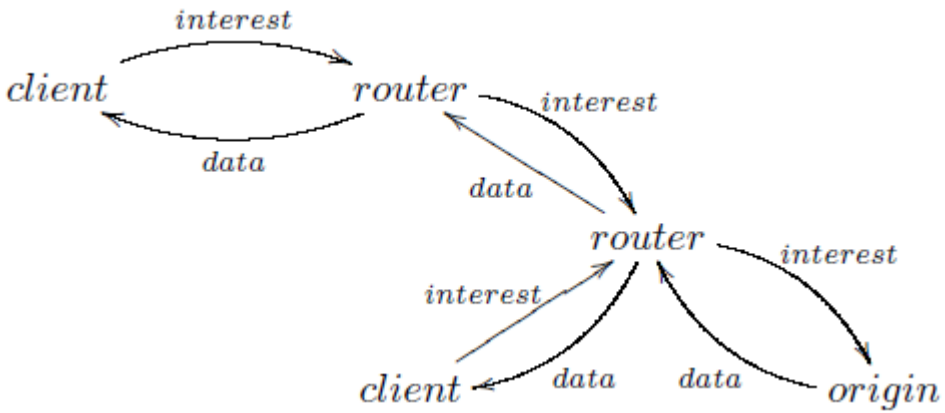
CCN路由


/www.nrc.nl/nieuws/2011/03/14/foobar/v3
/www.nrc.nl/ ... /v3
4
0
7
/www.nrc.nl/ ... /v3
PIT
prefix
0
0
3
0
/www.nrc.nl/ ... /v3
PIT
prefix
1
1
0
/www.nrc.nl/nieuws/2011/03/14/foobar/v3
/www.nrc.nl/ ... /v3

CCN路由

- 路由器节点对数据内容进行缓存
- 将interest包逐跳路由到数据源或者有该内容的CR处

  先在Content store找，有的话就返回；没有的话就查询PIB，没有该转发记录则加入PIB，根据FIB表选择多个face转发interest
- 数据从源再根据request 的reverse path 路由回来
- 沿途的CR对数据进行缓存



CCN路由（2）

- 数据的分发是由请求引起的
- 路由器之间通过路由协议，如IS-IS、BGP等发送命名前缀通告
- 请求者发送Interest包，包含了请求数据的标识
- 路由器接受到Interest包后，记录Interest包进入路由器的接口，然后通过基于命名的路由转发协议将其转发
- Interest包一旦发现节点上有相应的数据，则返回应答Data包：包括请求数据名称和相应数据
- Data包通过逆向路径返回给请求者

CCN设计思想—路由（3）

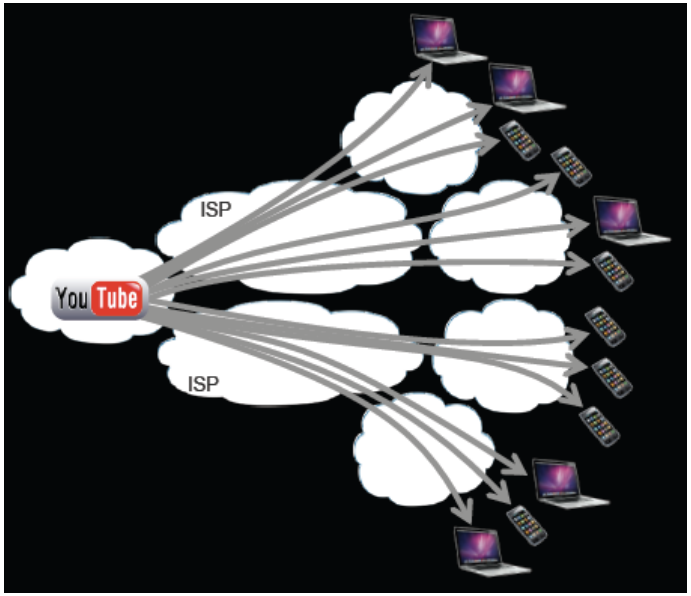
- 任何数据包都不包含主机/接口地址
- Interest包的路由是根据其承载的内容名称路由到data produces***(FIB)***
- Data包的路由路径是依赖于Interest包路由时在每跳路由器上留下的状态标记

CCN特性—多路径路由

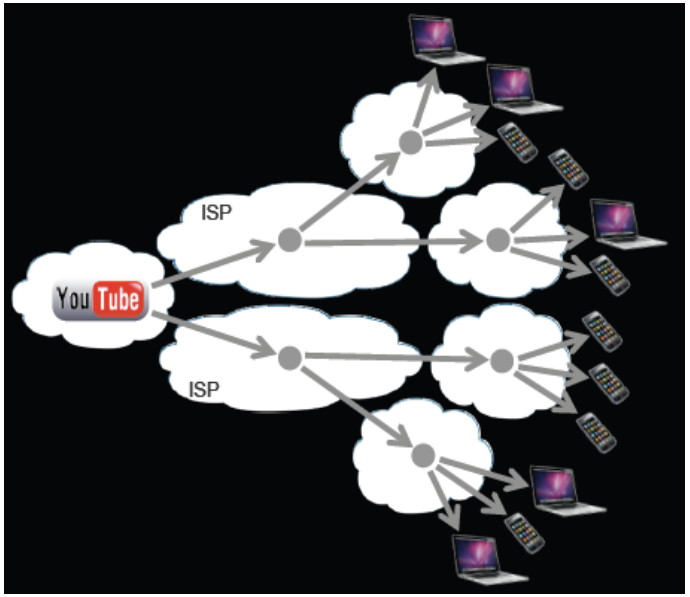
- Interest阶段会选择多个Interface进行转发，同时在接收到其它接口的Interface会根据PIB进行过滤
- Data阶段会根据PIB记录，将数据包复制多份，转发到多个Interface，但每个接口只会转发一份

vs IP：IP无法实现多路径路由，会造成环路，只能选择一条最优的路径进行包转发

CCN特性—广播、多播



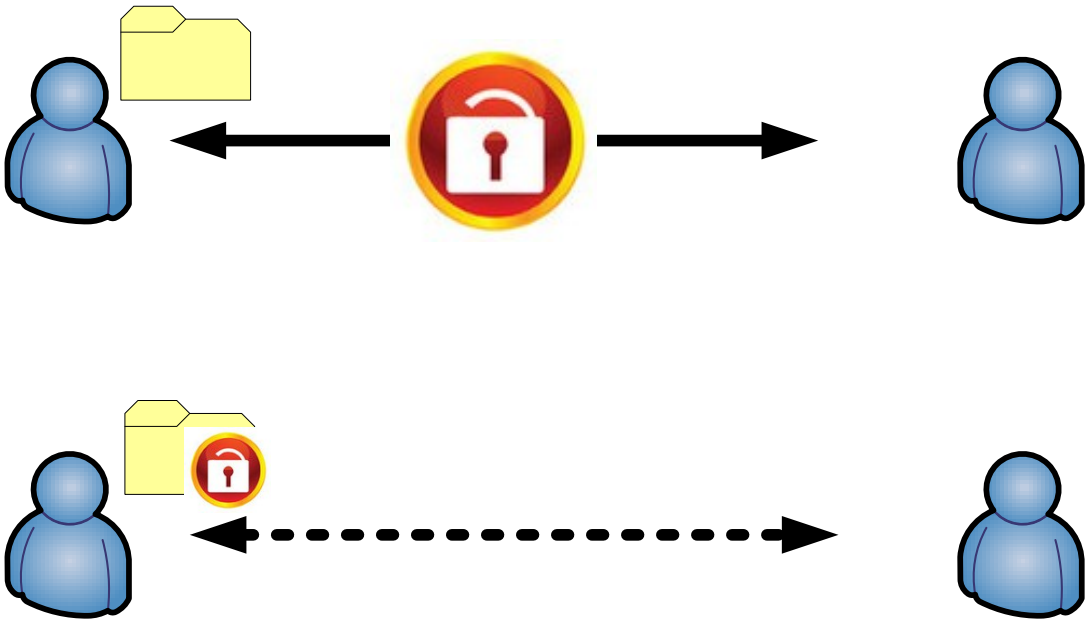
VS



IP不支持多路径路由，无法天然支持广播，需要依赖应用层参与

CCN的特性—安全性

- 保护通信安全→保证数据安全



CCN特性—安全性

- CCN的网络体系结构天然抵抗DoS 攻击
  - 路径上对内容缓存消除以针对某个目标主机的DoS
  - 针对同一数据的多个Interest请求会被忽略，并不会转发
  - 在Data阶段，每个Interface只转发一份数据拷贝

vs IP：需要其它的附属手段来解决DoS攻击

CCN特性—传输隐私性

- Interest
  - 不知道Interest最后的目的地是哪里
  - 不知道Interest是谁发出来的
  - 靠近数据请求者(consumer)的位置会泄露请求数据的名字
- Content
  - 不知道当时的Content从哪里传出来的
  - 传统的签名方法会泄露源 (producer)

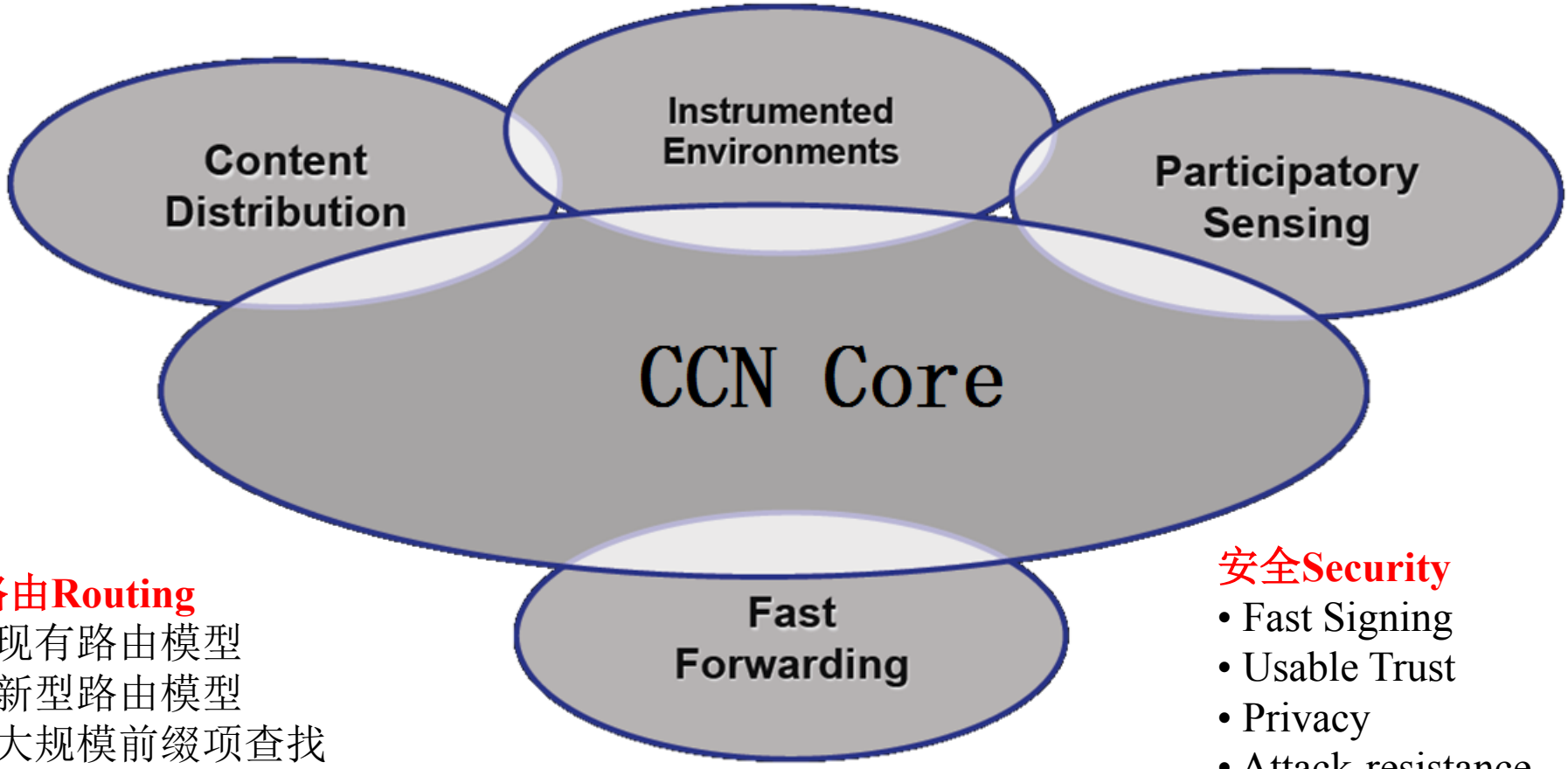
vs IP：IP源、目的地址直接泄露所有隐私

CCN研究领域

清華大學 Tsinghua University

- 命名
  - 命名分成两种： provider-assigned names 和user-selected names
    由ISP进行命名便于聚合/att/atlanta/alice/blog；再建立后者/aliceblog到前者的映射关系进行翻译
- 路由
  - 内容前缀宣告：拓展现有的OSPF、BGP协议，以支持CCN的内容前缀分发和Interest的多路径路由
- 存储
  - ContentStore算法
  - Cache性能优化
- 安全方面
  - 内容验证，快速签名，用户隐私
  - 中间CR攻击抵制

CCN研究领域



路由Routing
- 现有路由模型
- 新型路由模型
- 大规模前缀项查找

基本理论(Fundamental Theory)
- Any-to-Any 通信模型
- 带宽、内存和传输路径设计折中

安全Security
- Fast Signing
- Usable Trust
- Privacy
- Attack-resistance
- App. Security

CCN研究问题

清華大學 Tsinghua University

- 命名
  - 如何保障全局唯一
  - 如何加快名字处理
- 路由
  - 内容前缀宣告：拓展现有的域间域内协议
  - 多路径路由
- 存储
  - ContentStore算法
  - Cache性能优化
- 安全方面
  - 内容验证，快速签名，用户隐私
  - 中间CR攻击抵制
- 软硬件的高速处理架构

威胁模型 threat model

- 被动攻击
  - 流量观察和fingerprinting
  - 定时和大小相关性
- 主动攻击
  - 攻击路由器和内容发布者
  - 主动和动态的恶意行为

CCN网络安全与防御

清華大學 Tsinghua University

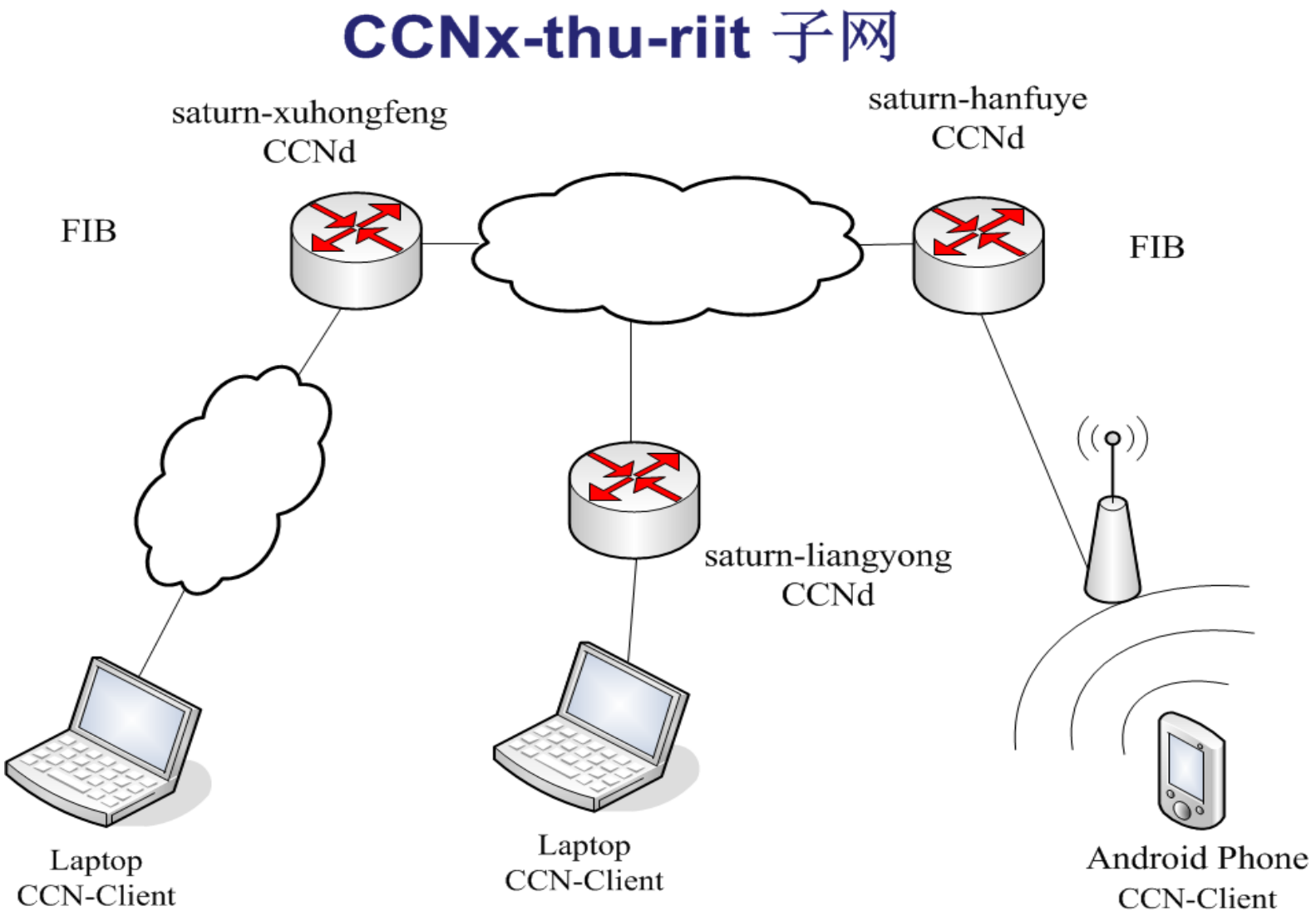
- 两类主要的ccn攻击
  - Interest Flooding Attacks
  - Interest泛洪攻击
  - Content Pollution Attacks
  - 内容污染攻击
  - 创建恶意内容

CCN内容保护和隐私

- 内容的完整性，可认证性和可信性
  - 内容发布者希望细粒度的访问限制 对于有价值内容或敏感内容
  - 内容消费者希望获取内容同时保护自己的信息不被泄露
  - 内容防火墙: content firewall

- 隐私
  - Cache隐私性
  - 名字隐私性
  - 签名隐私性
  - 隐私虚拟专用网: privacy VPN

CCNx-thu-riit 子网 Demo



讨论

清華大學 Tsinghua University

- 网络在物理世界的合理任务是什么，到底在底层应该提供什么基本功能（比如找对象功能，这个对象可以是主机、用户、服务、地理位置、内容。命名注意语意区分），才能满足各种信息技术的网络要求，才是正确的网络，而不再被“革命”？
- 分层设计时如何考虑好性能和代价的均衡的（端到端原则），这也是要看网络的主要使用。起初，为了信息的传递，设计出通信网络，该网络尽力而为的找到的对象是目的主机（问题是给对象命名时存在ID/Locator语意重载）；现在，人们大多使用网络获取信息，设计出了命名数据的网络（NDN）以及其基本实现CCN网络，该网络要找的对象是内容，为了性能和代价，网络节点增加了信息缓存的功能。

讨论

- 以后随着物联网的不断发展，很可能网络的基本功能又要改变，网络节点要增加更常用的信息处理功能，使用最近的计算资源来更有效的满足逐渐增多的终端的计算要求。所以网络的核心本质还有待于研究，合理的目标和原则还有待研究，主体对象命名承载的实体语意及其如何区分处理还有待于研究。

小结

- CCN即是一项技术，也是一个架构、一个基础；包含很多未实现的具体的技术，相当于取代IP协议之后重新建筑上层协议
- CCN实现了通信方式由“Where”到“What”的根本转变，致力于使互联网支持不考虑内容存储所在的物理位置，直接提供面向内容的功能
- CCN面临着路由可扩展性以及对端到端通信类应用有效支持等挑战
- 目前CCN框架里还存在很多问题供大家去解决

谢谢！