

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 8 月 23 日 (23.08.2018)



(10) 国际公布号
WO 2018/149101 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) **H04N 21/266** (2011.01)

(21) 国际申请号: PCT/CN2017/096996

(22) 国际申请日: 2017 年 8 月 11 日 (11.08.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 北京大学深圳研究生院(Peking University Shenzhen Graduate School) [CN/CN]; 中国广东省深圳市南山区西丽深圳大学城北大园区, Guangdong 518055 (CN)。

(72) 发明人: 雷凯(LEI, Kai); 中国广东省深圳市南山区西丽深圳大学城北大园区, Guangdong 518055 (CN)。 朱帅(ZHU, Shuai); 中国广东省深圳市

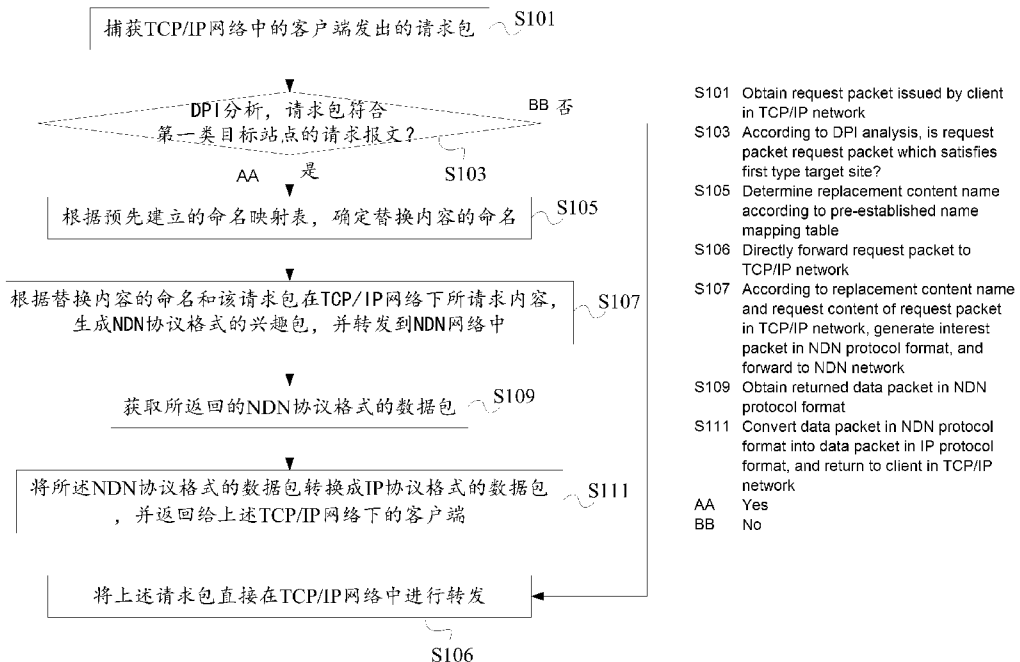
南山区西丽深圳大学城北大园区, Guangdong 518055 (CN)。 钟尚儒(ZHONG, Shangru); 中国广东省深圳市南山区西丽深圳大学城北大园区, Guangdong 518055 (CN)。 齐竹云(QI, Zhuyun); 中国广东省深圳市南山区西丽深圳大学城北大园区, Guangdong 518055 (CN)。 张翼(ZHANG, Yi); 中国广东省深圳市南山区西丽深圳大学城北大园区, Guangdong 518055 (CN)。

(74) 代理人: 深圳鼎合诚知识产权代理有限公司(DHC IP ATTORNEYS); 中国广东省深圳福田区金田路与福华路交汇处现代国际大厦2201, Guangdong 518048 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) Title: NDN AND IP FUSION NETWORK CONTENT CONTROL METHOD AND APPARATUS, AND STORAGE MEDIUM

(54) 发明名称: 一种NDN和IP融合网络的内容管控方法、装置及存储介质



(57) Abstract: An NDN and IP fusion network content control method and apparatus. The method comprises: obtaining a request packet issued by a client in a TCP/IP network; performing application layer protocol deep packet analysis on the request packet; upon determining that the request packet is a request packet which satisfies a first type target site, determining a replacement content name according to a pre-established name mapping table; according to the replacement content name and request content of the request packet in the TCP/IP network, generating an interest packet in an NDN protocol format, and forwarding to an NDN network; obtaining a data

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告 (条约第21条(3))。
- 在修改权利要求的期限届满之前进行, 在收到该修改后将重新公布 (细则48.2(h))。
- 根据申请人的请求, 在条约第21条(2)(a)所规定的期限届满之前进行。

packet in the NDN protocol format returned after the interest packet in the NDN protocol format was forwarded to the NDN network; converting the data packet in the NDN protocol format into a data packet in an IP protocol format, and returning to the client in the TCP/IP network. The present invention implements content granularity level content control, and modifies or replaces content for return to a user, something which cannot be achieved in traditional TCP/IP networks.

(57) 摘要: 一种NDN和IP融合网络的内容管控方法及装置。捕获TCP/IP网络中的客户端发出的请求包; 对该请求包进行应用层协议的深度报文分析, 当判断该请求包是符合第一类目标站点的请求报文, 则根据预先建立的命名映射表, 确定替换内容的命名; 根据替换内容的命名和该请求包在TCP/IP网络下所请求内容, 生成NDN协议格式的兴趣包, 并转发到NDN网络中; 获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包; 将所述NDN协议格式的数据包转换成IP协议格式的数据包, 并返回给所述TCP/IP网络下的客户端。本发明实现了内容粒度级别的内容管控, 可以对内容进行修改或替换, 再返回给用户, 这在传统TCP/IP网络是无法做到的。

一种NDN和IP融合网络的内容管控方法、装置及存储介质

技术领域

[0001] 本发明涉及网络通信技术领域，具体涉及一种NDN和IP融合网络的内容管控方法及装置。

背景技术

[0002] Web 2.0时代下，互联网用户每天都在产生网络内容进行传播，有必要对网络内容进行合理的管控。在现有的TCP/IP网络架构下，一般通过DNS污染、IP屏蔽等方法，实现较粗粒度的内容过滤，换句话说，现在的技术中一般都是直接屏蔽需要管控的内容。

技术问题

[0003] 本申请提供一种NDN和IP融合网络的内容管控方法及装置，可以实现更细粒度的内容管控，即对需要管控的内容进行内容替换或修改后再返回对用户的客户端，而不是直接简单地进行屏蔽处理。

问题的解决方案

技术解决方案

[0004] 根据第一方面，一种实施例中提供一种NDN和IP融合网络的内容管控方法，包括：

[0005] 捕获TCP/IP网络中的客户端发出的请求包；

[0006] 对该请求包进行应用层协议的深度报文分析，以判断该请求包是否是符合第一类目标站点的请求报文；

[0007] 当判断该请求包是符合第一类目标站点的请求报文，则根据预先建立的命名映射表，确定替换内容的命名，其中所述替换内容用于替换该请求包在TCP/IP网络下所请求内容；

[0008] 根据替换内容的命名和该请求包在TCP/IP网络下所请求内容，生成NDN协议格

式的兴趣包，并转发到NDN网络中；

[0009] 获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；

[0010] 将所述NDN协议格式的数据包转换成IP协议格式的数据包，并返回给所述TCP/IP网络下的客户端。

[0011] 在一实施例中，所述方法还包括当判断该请求包不是符合第一类目标站点的请求报文，则将所述请求包直接在TCP/IP网络中进行转发。

[0012] 根据第二方面，一种实施例中提供一种NDN和IP融合网络的内容管控方法，包括：

[0013] 捕获TCP/IP网络中服务器返回的内容数据包；

[0014] 对所述内容数据包进行深度报文分析，以判断该内容数据包是否是第一类目标站点返回的响应报文；

[0015] 当判断所述内容数据包是第一类目标站点返回的响应报文，则判断该内容数据包是否含有禁止的内容；

[0016] 当判断所述内容数据包含有禁止的内容，则根据预先建立的命名映射表，确定替换内容的命名，其中所述替换内容用于替换所述内容数据包包含的内容；

[0017] 根据替换内容的命名和所述内容数据包，生成NDN协议格式的兴趣包，并转发到NDN网络中；

[0018] 获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；

[0019] 将所述NDN协议格式的数据包转换成IP协议格式的数据包，并按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[0020] 在一实施例中，所述方法还包括：当判断所述内容数据包不是第一类目标站点返回的响应报文，或判断所述内容数据包不包含禁止的内容，则将所述内容数据包直接在TCP/IP网络中按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[0021] 在一实施例中，所述服务器为流媒体服务器，所述内容数据包为视频流传输协议的数据包。

[0022] 在一实施例中，所述方法还包括：

[0023] 对捕获的请求包进行应用层协议的深度报文分析，以判断该请求包是否符合第二类目标站点的请求报文；其中所述请求包为TCP/IP网络中的客户端所发出；

[0024] 当判断所述请求包是符合第二类目标站点的请求报文，则将该请求包转换成NDN协议格式的兴趣包，并转发到NDN网络中；反之，则将所述请求包直接在TCP/IP网络中进行转发；

[0025] 当获取到所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包，则将所获取的NDN协议格式的数据包转换成IP协议格式的数据包，并返回给所述TCP/IP网络下的客户端；反之，则将所述请求包重新在TCP/IP网络中进行转发；

[0026] 当所述请求包是在TCP/IP网络中进行被转发，则捕获所述请求包在TCP/IP网络中进行转发服务器响应返回的数据包；将该返回的数据包返回给所述客户端，并且将该返回的数据包转换成NDN协议格式的数据包，缓存于最近的NDN节点本地。

[0027] 根据第三方面，一种实施例中提供一种NDN和IP融合网络的内容管控装置，包括：

[0028] NDN/IP网关，用于捕获TCP/IP网络中的客户端发出的请求包；对该请求包进行应用层协议的深度报文分析，以判断该请求包是否符合第一类目标站点的请求报文；当判断该请求包是符合第一类目标站点的请求报文，则根据预先建立的命名映射表，确定替换内容的命名，其中所述替换内容用于替换该请求包在TCP/IP网络下所请求内容；当判断该请求包不是符合第一类目标站点的请求报文，则将所述请求包直接在TCP/IP网络中进行转发；

[0029] NDN/IP转换单元，用于根据替换内容的命名和该请求包在TCP/IP网络下所请求内容，生成NDN协议格式的兴趣包，并转发到NDN网络中；获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；将所述NDN协议格式的数据包转换成IP协议格式的数据包，并通过NDN/IP网关返回给所述TCP/IP网络中的客户端。

[0030] 根据第四方面，一种实施例中提供一种NDN和IP融合网络的内容管控装置，包括：

[0031] NDN/IP网关，用于捕获TCP/IP网络中服务器返回的内容数据包；对所述内容数据包进行深度报文分析，以判断该内容数据包是否是第一类目标站点返回的响应报文；当判断所述内容数据包是第一类目标站点返回的响应报文，则判断该内容数据包是否含有禁止的内容；当判断所述内容数据包含有禁止的内容，则根据预先建立的命名映射表，确定替换内容的命名，其中所述替换内容用于替换该内容数据包包含的内容；当判断所述内容数据包不是第一类目标站点返回的响应报文，或判断所述内容数据包不包含禁止的内容，则将所述内容数据包直接在TCP/IP网络中按照服务器返回的目的地址，返回给TCP/IP网络下的客户端；

[0032] NDN/IP转换单元，用于根据替换内容的命名和所述内容数据包，生成NDN协议格式的兴趣包，并转发到NDN网络中；获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；将所述NDN协议格式的数据包转换成IP协议格式的数据包，并通过NDN/IP网关按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[0033] 在一实施例中，所述NDN/IP网关用于捕获TCP/IP网络中流媒体服务器返回的视频流。

[0034] 根据第五方面，一种实施例中提供一种存储介质，包括程序，所述程序能够被处理器执行以实现上述任一实施例所述的内容管控方法。

发明的有益效果

有益效果

[0035] 依上述实施例的NDN和IP融合网络的内容管控方法、装置及存储介质，实现了内容粒度级别的内容管控，可以对内容进行修改或替换，再返回给用户，这在传统TCP/IP网络是无法做到的。

对附图的简要说明

附图说明

[0036] 图1为一种实施例的NDN和IP融合网络的内容管控方法的流程图；

- [0037] 图2为一种实施例的NDN和IP融合网络的内容管控装置的结构示意图；
- [0038] 图3为另一种实施例的NDN和IP融合网络的内容管控方法的流程图；
- [0039] 图4为另一种实施例的NDN和IP融合网络的内容管控装置的结构示意图；
- [0040] 图5为又一种实施例的NDN和IP融合网络的内容管控方法的流程图。

发明实施例

本发明的实施方式

- [0041] 具体实施方式

[0042] 下面通过具体实施方式结合附图对本发明作进一步详细说明。其中不同实施方式中类似元件采用了相关联的类似的元件标号。在以下的实施方式中，很多细节描述是为了使得本申请能被更好的理解。然而，本领域技术人员可以毫不费力的认识到，其中部分特征在不同情况下是可以省略的，或者可以由其他元件、材料、方法所替代。在某些情况下，本申请相关的一些操作并没有在说明书中显示或者描述，这是为了避免本申请的核心部分被过多的描述所淹没，而对于本领域技术人员而言，详细描述这些相关操作并不是必要的，他们根据说明书中的描述以及本领域的一般技术知识即可完整了解相关操作。

[0043] 另外，说明书中所描述的特点、操作或者特征可以以任意适当的方式结合形成各种实施方式。同时，方法描述中的各步骤或者动作也可以按照本领域技术人员所能显而易见的方式进行顺序调换或调整。因此，说明书和附图中的各种顺序只是为了清楚描述某一个实施例，并不意味着是必须的顺序，除非另有说明其中某个顺序是必须遵循的。

[0044] 本文中为部件所编序号本身，例如“第一”、“第二”等，仅用于区分所描述的对象，不具有任何顺序或技术含义。而本申请所说“连接”、“联接”，如无特别说明，均包括直接和间接连接（联接）。

[0045] 为了使本发明更为清楚，先对NDN网络作一个说明。以信息为中心的网络（ICN，Information-Center Network，简称信息中心网络）是近年来试图替代传统的基于TCP/IP协议的互联网架构，在ICN中用户只关心任何网络节点迅速地获取数据（或者副本），不关心内容的位置。这方面的代表是命名数据网络（NDN，Named Data Networking）。命名数据网络中所有的数据都是基于名字来标识

，网络中不再存在IP地址和通信连接的概念，其网络通信基于两类数据包，Interest包（兴趣包）和Data包（数据包），两者根据完整或相对的名字进行匹配。兴趣包用于数据请求方向网络中请求数据，而数据包是数据拥有者收到请求后返回的数据。NDN是一种基于拉（pull）的架构，其中消费者通过发送兴趣包来请求数据，相应的数据包沿相同路径返回，通过数据内置的缓存功能和灵活的转发策略层来获得良好的内容分发功能。NDN面向内容的网络传输特性使其能用于海量数据的内容分发。

[0046] NDN作为新型的未来网络架构，短时间内真实落地部署，并完全替换TCP/IP网络架构的想法并不现实，学术界开始研究TCP/IP往NDN过渡时期的解决办法，发明人考虑NDN和IP的融合网络是一种解决方案。基于IP覆盖网络（Overlay）之上构建NDN网络，把NDN包作为应用层数据封装在IP数据包内部，是一种垂直上下层的融合方案；基于协议解析的IP-NDN转译，通过提取IP包或者NDN包内容然后转换成另一种协议格式，是一种水平方向上的融合方案。

[0047] 本发明基于深度报文检测技术（Deep Packet Inspection, DPI）实现对网络特定内容（如流媒体）的数据包的捕获、侦测和分析，基于IP-NDN协议转换实现IP网络包和NDN网络包的协议转换，从而提供了NDN和IP的融合网络场景，并利用NDN内容感知的特性，提供了一种管控方法，可以实现内容级别（粒度更细）的替换修改管控方法。这种管控方法不仅可以实现较传统TCP/IP网络（基于URL实现过滤）更细粒度的内容替换或修改，在一些实施例中，还能支持传统对TCP/IP不能解决的流媒体内容的管控。其中，深度报文检测技术是一种在应用层对网络数据包的侦测和处理技术，可以通过对网络骨干路由器的流量和报文内容进行检测分析，根据定义的规则策略实现对报文内容的过滤，从而实现流量分析统计和抗应用层攻击等功能。

[0048] 下面通过若干实施例，并结合附图对本发明进行说明。

[0049]

[0050] 实施例1

[0051] 请参照图1，本实施例公开了一种NDN和IP融合网络的内容管控方法，其包括步骤S101~S111，下面具体说明。

- [0052] 步骤S101: 捕获TCP/IP网络中的客户端发出的请求包。
- [0053] 步骤S103: 对该请求包进行应用层协议的深度报文分析, 以判断该请求包是否是符合第一类目标站点的请求报文。当判断该请求包是符合第一类目标站点的请求报文, 则进行步骤S105; 反之, 则进行步骤S106, 将上述请求包直接在TCP/IP网络中进行转发。
- [0054] 步骤S105: 当判断该请求包是符合第一类目标站点的请求报文, 则根据预先建立的命名映射表, 确定替换内容的命名, 其中替换内容用于替换该请求包在TCP/IP网络下所请求内容。在一实施例中, 预先建立的命名映射表可以是不合法站点URL映射到合法(视频)内容的命名, 也可以是不合法(视频)内容命名到合法(视频)内容的命名。
- [0055] 步骤S107: 根据替换内容的命名和该请求包在TCP/IP网络下所请求内容, 生成NDN协议格式的兴趣包, 并转发到NDN网络中。
- [0056] 步骤S109: 获取上述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包。
- [0057] 步骤S111: 将所述NDN协议格式的数据包转换成IP协议格式的数据包, 并返回给上述TCP/IP网络下的客户端。
- [0058] 请参照图2, 本实施例还提供一种NDN和IP融合网络的内容管控装置, 其包括NDN/IP网关110和NDN/IP转换单元130, 下面具体说明。
- [0059] NDN/IP网关110用于捕获TCP/IP网络中的客户端发出的请求包; 对该请求包进行应用层协议的深度报文分析, 以判断该请求包是否是符合第一类目标站点的请求报文; 当判断该请求包是符合第一类目标站点的请求报文, 则根据预先建立的命名映射表, 确定替换内容的命名, 其中替换内容用于替换该请求包在TCP/IP网络下所请求内容; 当判断该请求包不是符合第一类目标站点的请求报文, 则将所述请求包直接在TCP/IP网络中进行转发。
- [0060] NDN/IP转换单元130用于根据替换内容的命名和该请求包在TCP/IP网络下所请求内容, 生成NDN协议格式的兴趣包, 并转发到NDN网络中; 获取上述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包; 将上述NDN协议格式的数据包转换成IP协议格式的数据包, 并通过NDN/IP网关110返回

给上述TCP/IP网络中的客户端。

[0061] 下面再举一个例子来进一步说明本实施例的NDN和IP融合网络的内容管控方法及装置。

[0062] 例如，不妨以IP用户点播请求流媒体服务器“http://youtube.com”的视频内容为场景案例进行说明。TCP/IP网络中的客户端发出的请求包，其包含禁止信息的视频内容，比如“http://youtube.com/invalid_video/seg_1/chunk_1/”。需要说明的是，该处禁止信息可以通过预设进行定义，像一些比较敏感的信息或违反相关法律法规的信息。第一类目标站点包括“http://youtube.com”，因此当NDN/IP网关110捕捉到上述请求包时，则判断上述请求包是符合第一类目标站点的请求报文，那么就会根据预选建立的命名映射表，确定替换内容的命名，例如将上述的域名“http://youtube.com/invalid_video/seg_1/chunk_1/”映射为命名“/youtube.com/valid_video/seg_1/chunk1”。接着，NDN/IP转换单元130根据替换内容的命名和该请求包在TCP/IP网络下所请求内容，生成NDN协议格式的兴趣包，并转发到NDN网络中。NDN/IP转换单元130再获取上述兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包，并将该NDN协议格式的数据包换成IP协议格式的数据包，通过NDN/IP网关110返回给上述TCP/IP网络中的客户端。因此，通过本发明实现了内容粒度级别的内容管控，可以对内容进行修改或替换，再返回给用户，这在传统TCP/IP网络是无法做到的。

[0063]

[0064] 实施例2

[0065] 请参照图3，本实施例公开了一种NDN和IP融合网络的内容管控方法，其包括步骤S201~S213，下面具体说明。

[0066] 步骤S201：捕获TCP/IP网络中服务器返回的内容数据包。在一实施例中，服务器为流媒体服务器，内容数据包为视频流传输协议的数据，换句话说，步骤S201捕获TCP/IP网络中流媒体服务器返回的视频流。

[0067] 步骤S203：对上述内容数据包进行深度报文分析，以判断该内容数据包是否是第一类目标站点返回的响应报文。

[0068] 步骤S205：当判断所述内容数据包是第一类目标站点返回的响应报文，则判断

该内容数据包是否含有禁止的内容。在一实施例中，禁止的内容可以通过预设进行定义，像一些比较敏感的内容或违反相关法律法规的内容。

[0069] 步骤S207：当判断上述内容数据包含有禁止的内容，则根据预先建立的命名映射表，确定替换内容的命名，其中替换内容用于替换该内容数据包包含的内容。在一实施例中，预先建立的命名映射表可以是不合法站点URL映射到合法（视频）内容的命名，也可以是不合法（视频）内容命名到合法（视频）内容的命名。

[0070] 步骤S208：当判断上述内容数据包不是第一类目标站点返回的响应报文，或判断上述内容数据包不包含禁止的内容，则将上述内容数据包直接在TCP/IP网络中按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[0071] 步骤S209：根据替换内容的命名和上述内容数据包，生成NDN协议格式的兴趣包，并转发到NDN网络中。

[0072] 步骤S211：获取上述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包。

[0073] 步骤S213：将上述NDN协议格式的数据包转换成IP协议格式的数据包，并按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[0074] 请参照图4，本实施例还提供一种NDN和IP融合网络的内容管控装置，其包括NDN/IP网关210和NDN/IP转换单元230，下面具体说明

[0075] NDN/IP网关210用于捕获TCP/IP网络中服务器返回的内容数据包；对上述内容数据包进行深度报文分析，以判断该内容数据包是否是第一类目标站点返回的响应报文；当判断上述内容数据包是第一类目标站点返回的响应报文，则判断该内容数据包是否含有禁止的内容；当判断上述内容数据包含有禁止的内容，则根据预先建立的命名映射表，确定替换内容的命名，其中所述替换内容用于替换该内容数据包包含的内容；当判断上述内容数据包不是第一类目标站点返回的响应报文，或判断上述内容数据包不包含禁止的内容，则将上述内容数据包直接在TCP/IP网络中按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。在一实施例中，NDN/IP网关210用于捕获TCP/IP网络中服务器返回的内容数据包中，服务器为流媒体服务器，所述内容数据包为视频流传输协议的数

据包，换句话说，NDN/IP网关210用于捕获TCP/IP网络中流媒体服务器返回的视频流。

[0076] NDN/IP转换单元230用于根据替换内容的命名和上述内容数据包，生成NDN协议格式的兴趣包，并转发到NDN网络中；获取上述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；将上述NDN协议格式的数据包转换成IP协议格式的数据包，并通过NDN/IP网关按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[0077] 下面再举一个例子来进一步说明本实施例的NDN和IP融合网络的内容管控方法及装置。

[0078] 例如，不妨以IP用户点播请求流媒体服务器“http://youtube.com”的视频内容为场景案例进行说明。NDN/IP网关210捕获流媒体服务器返回的视频流并进行深度报文分析，当判断上述视频流是第一类目标站点返回的响应报文，且该视频流含有禁止的内容，因此根据预选建立的命名映射表，确定替换内容的命名，例如将“http://youtube.com/movie/seg_2/invalid_chunk_1”映射为“youtube.com/movie/seg_2/valid_chunk_1”。接着，NDN/IP转换单元230根据替换内容的命名和上述内容数据包，生成NDN协议格式的兴趣包，并转发到NDN网络中。NDN/IP转换单元230可以获取到上述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包，并将该NDN协议格式的数据包换成IP协议格式的数据包，通过NDN/IP网关按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。因此，通过本发明实现了内容粒度级别的内容管控，可以对内容进行修改或替换，再返回给用户；例如，可以实现视频流替换部分不合法内容，具体表现为替换电影中的一段不合法画面，这在传统TCP/IP网络是无法做到的。

[0079]

[0080] 实施例3

[0081] 在实施例1或实施例2的基础上，请参照图5，本实施例3公开的NDN和IP融合网络的内容管控方法，还可以包括以下步骤S301~S309。

[0082] 步骤S301：对捕获的请求包进行应用层协议的深度报文分析，以判断该请求包是否是符合第二类目标站点的请求报文；其中该请求包为TCP/IP网络中的客户

端所发出。当判断上述请求包是符合第二类目标站点的请求报文，则进行步骤S303；反之，则进行步骤S304，将上述请求包直接在TCP/IP网络中进行转发。

[0083] 步骤S303：当判断上述请求包是符合第二类目标站点的请求报文，则将该请求包转换成NDN协议格式的兴趣包，并转发到NDN网络中。

[0084] 步骤S305：当上述NDN协议格式的兴趣包在NDN网络中存在对应的数据包，则可以获取到上述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包，之后将所获取的NDN协议格式的数据包转换成IP协议格式的数据包，并返回给上述TCP/IP网络下的客户端。

[0085] 步骤S307：当上述NDN协议格式的兴趣包在NDN网络中不存在对应的数据包，则将上述请求包重新在TCP/IP网络中进行转发。

[0086] 步骤S309：当在步骤S304或步骤S307中将请求包在TCP/IP网络中进行转发，则捕获该请求包在TCP/IP网络中进行转发服务器响应返回的数据包，将该返回的数据包返回给所述客户端，并且将该返回的数据包转换成NDN协议格式的数据包，缓存于最近的NDN节点本地。

[0087] 在实施例1或2的基础上，本实施例3公开的NDN和IP融合网络的内容管控装置，包括NDN/IP网关和NDN/IP转换单元，该NDN/IP网关和NDN/IP转换单元还可以包括以下结构和作用。

[0088] NDN/IP网关用于对捕获的请求包进行应用层协议的深度报文分析，以判断该请求包是否是符合第二类目标站点的请求报文；其中所述请求包为TCP/IP网络中的客户端所发出；当判断所述请求包是符合第二类目标站点的请求报文，则将该请求包转换成NDN协议格式的兴趣包，并转发到NDN网络中；反之，则将所述请求包直接在TCP/IP网络中进行转发；

[0089] NDN/IP转换单元用于当获取到所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包，则将所获取的NDN协议格式的数据包转换成IP协议格式的数据包，并返回给所述TCP/IP网络下的客户端；反之，则将所述请求包重新通过NDN/IP网关在TCP/IP网络中进行转发。

[0090] 当所述请求包是在TCP/IP网络中进行被转发，NDN/IP网关捕获所述请求包在TCP/IP网络中进行转发服务器响应返回的数据包；将该返回的数据包返回给所述

客户端，NDN/IP转换单元将该返回的数据包转换成NDN协议格式的数据包，缓存于最近的NDN节点本地。

[0091] 通过本实施例实现了内容加速和缓存。

[0092]

[0093] 以上就是本发明的若干实施例，本发明可以将IP网络中用户请求的敏感内容数据包，转入NDN网络并替换部分内容，实现内容级别的替换和管控。本发明利用NDN的内容感知特性，基于NDN/IP网关实现对特定站点流量的劫持和内容的缓存，从而实现对HTTP等TCP/IP网络下内容缓存和替换管控。

[0094] 例如，IP用户请求敏感或不合法内容的数据包经过NDN/IP网关，DPI可以识别劫持不合法请求包，根据命名映射表确定要替换的合法视频块的命名，经过NDN/IP转换单元转译为用于替换的合法内容兴趣（Interest）包到NDN网络，返回合法的视频内容。例如，对于流媒体服务器返回的网络视频包中，经过网络骨干处的NDN/IP网关截获，通过深度学习等方法识别出视频包中的不合法视频块（段或者帧），根据命名映射表确定要替换的合法视频块的命名，经过NDN/IP转换单元转译成兴趣（Interest）包进入NDN网络，在NDN路由节点中的网内缓存命中后，返回合法的视频块，在NDN/IP网关重组替换后的含合法视频块的网络视频包，返回给用户。

[0095] 因此，本发明可以实现内容粒度级别的内容感知，过滤并返回合法的内容块实现部分视频内容的替换。

[0096] 本领域技术人员可以理解，上述实施方式中各种方法的全部或部分功能可以通过硬件的方式实现，也可以通过计算机程序的方式实现。当上述实施方式中全部或部分功能通过计算机程序的方式实现时，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器、随机存储器、磁盘、光盘、硬盘等，通过计算机执行该程序以实现上述功能。例如，将程序存储在设备的存储器中，当通过处理器执行存储器中程序，即可实现上述全部或部分功能。另外，当上述实施方式中全部或部分功能通过计算机程序的方式实现时，该程序也可以存储在服务器、另一计算机、磁盘、光盘、闪存盘或移动硬盘等存储介质中，通过下载或复制保存到本地设备的存储器中，或对本地设备的系统进行

版本更新，当通过处理器执行存储器中的程序时，即可实现上述实施方式中全部或部分功能。

[0097] 以上应用了具体个例对本发明进行阐述，只是用于帮助理解本发明，并不用以限制本发明。对于本发明所属技术领域的技术人员，依据本发明的思想，还可以做出若干简单推演、变形或替换。

权利要求书

- [权利要求 1] 一种NDN和IP融合网络的内容管控方法,其特征在于, 包括:
- 捕获TCP/IP网络中的客户端发出的请求包;
- 对该请求包进行应用层协议的深度报文分析, 以判断该请求包是否是符合第一类目标站点的请求报文;
- 当判断该请求包是符合第一类目标站点的请求报文, 则根据预先建立的命名映射表, 确定替换内容的命名, 其中所述替换内容用于替换该请求包在TCP/IP网络下所请求内容;
- 根据替换内容的命名和该请求包在TCP/IP网络下所请求内容, 生成NDN协议格式的兴趣包, 并转发到NDN网络中;
- 获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包;
- 将所述NDN协议格式的数据包转换成IP协议格式的数据包, 并返回给所述TCP/IP网络下的客户端。
- [权利要求 2] 如权利要求1所述的内容管控方法, 其特征在于, 还包括: 当判断该请求包不是符合第一类目标站点的请求报文, 则将所述请求包直接在TCP/IP网络中进行转发。
- [权利要求 3] 一种NDN和IP融合网络的内容管控方法, 其特征在于, 包括:
- 捕获TCP/IP网络中服务器返回的内容数据包;
- 对所述内容数据包进行深度报文分析, 以判断该内容数据包是否是第一类目标站点返回的响应报文;
- 当判断所述内容数据包是第一类目标站点返回的响应报文, 则判断该内容数据包是否含有禁止的内容;
- 当判断所述内容数据包含有禁止的内容, 则根据预先建立的命名映射表, 确定替换内容的命名, 其中所述替换内容用于替换所述内容数据包包含的内容;
- 根据替换内容的命名和所述内容数据包, 生成NDN协议格式的兴趣包, 并转发到NDN网络中;

获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；

将所述NDN协议格式的数据包转换成IP协议格式的数据包，并按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[权利要求 4] 如权利要求3所述的内容管控方法，其特征在于，还包括：当判断所述内容数据包不是第一类目标站点返回的响应报文，或判断所述内容数据包不包含禁止的内容，则将所述内容数据包直接在TCP/IP网络中按照服务器返回的目的地址，返回给TCP/IP网络下的客户端。

[权利要求 5] 如权利要求3所述的的内容管控方法，其特征在于，所述服务器为流媒体服务器，所述内容数据包为视频流传输协议的数据包。

[权利要求 6] 如权利要求1至5中任一项所述的内容管控方法，其特征在于，还包括：

对捕获的请求包进行应用层协议的深度报文分析，以判断该请求包是否是符合第二类目标站点的请求报文；其中所述请求包为TCP/IP网络中的客户端所发出；

当判断所述请求包是符合第二类目标站点的请求报文，则将该请求包转换成NDN协议格式的兴趣包，并转发到NDN网络中；反之，则将所述请求包直接在TCP/IP网络中进行转发；

当获取到所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包，则将所获取的NDN协议格式的数据包转换成IP协议格式的数据包，并返回给所述TCP/IP网络下的客户端；反之，则将所述请求包重新在TCP/IP网络中进行转发；

当所述请求包是在TCP/IP网络中进行被转发，则捕获所述请求包在TCP/IP网络中进行转发服务器响应返回的数据包；将该返回的数据包返回给所述客户端，并且将该返回的数据包转换成NDN协议格式的数据包，缓存于最近的NDN节点本地。

[权利要求 7] 一种NDN和IP融合网络的内容管控装置，其特征在于，包括：NDN/IP网关，用于捕获TCP/IP网络中的客户端发出的请求包；对该

请求包进行应用层协议的深度报文分析，以判断该请求包是否是符合第一类目标站点的请求报文；当判断该请求包是符合第一类目标站点的请求报文，则根据预先建立的命名映射表，确定替换内容的命名，其中所述替换内容用于替换该请求包在TCP/IP网络下所请求内容；当判断该请求包不是符合第一类目标站点的请求报文，则将所述请求包直接在TCP/IP网络中进行转发；

NDN/IP转换单元，用于根据替换内容的命名和该请求包在TCP/IP网络下所请求内容，生成NDN协议格式的兴趣包，并转发到NDN网络中；获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；将所述NDN协议格式的数据包转换成IP协议格式的数据包，并通过NDN/IP网关返回给所述TCP/IP网络中的客户端。

[权利要求 8]

一种NDN和IP融合网络的内容管控装置，其特征在于，包括：

NDN/IP网关，用于捕获TCP/IP网络中服务器返回的内容数据包；
对所述内容数据包进行深度报文分析，以判断该内容数据包是否是第一类目标站点返回的响应报文；当判断该内容数据包是第一类目标站点返回的响应报文，则判断该内容数据包是否含有禁止的内容；当判断该内容数据包含有禁止的内容，则根据预先建立的命名映射表，确定替换内容的命名，其中所述替换内容用于替换该内容数据包包含的内容；当判断该内容数据包不是第一类目标站点返回的响应报文，或判断该内容数据包不包含禁止的内容，则将该内容数据包直接在TCP/IP网络中按照服务器返回的目的地址，返回给TCP/IP网络下的客户端；

NDN/IP转换单元，用于根据替换内容的命名和所述内容数据包，生成NDN协议格式的兴趣包，并转发到NDN网络中；获取所述NDN协议格式的兴趣包被转发到NDN网络后所返回的NDN协议格式的数据包；将所述NDN协议格式的数据包转换成IP协议格式的数据包，并通过NDN/IP网关按照服务器返回的目的地址，返回给TCP/IP网络下的

客户端。

[权利要求 9] 如权利要求8所述的内容管控装置，其特征在于，所述NDN/IP网关用于捕获TCP/IP网络中流媒体服务器返回的视频流。

[权利要求 10] 一种存储介质，其特征在于，包括程序，所述程序能够被处理器执行以实现如权利要求1-6中任一项所述的内容管控方法。

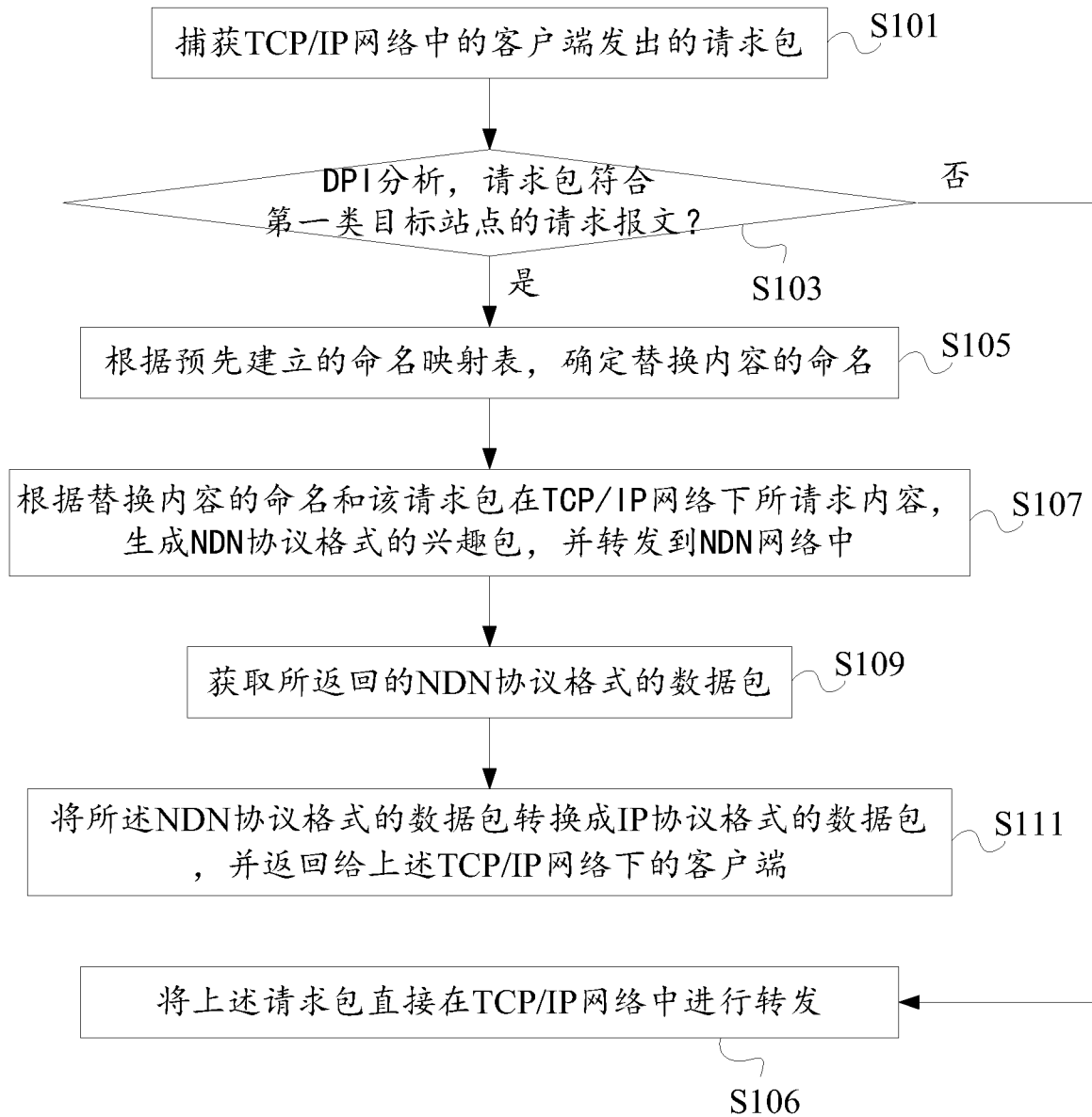


图 1

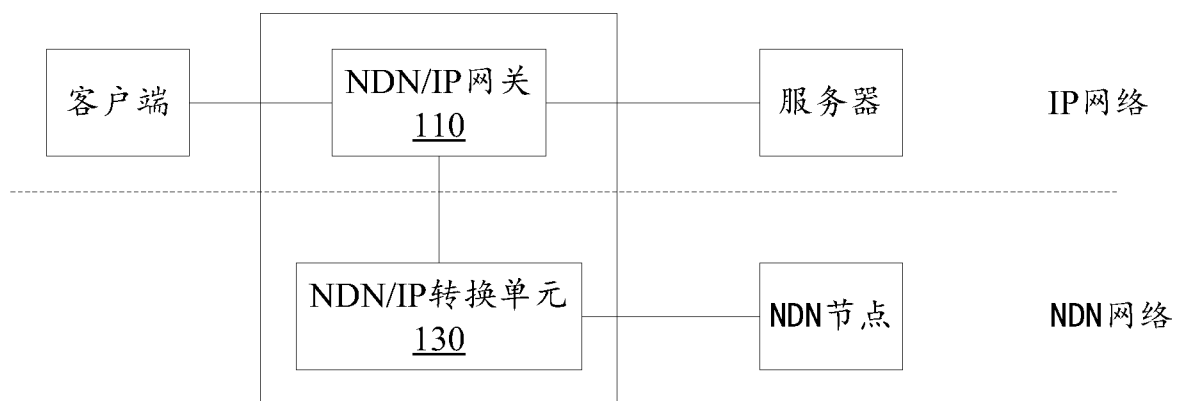


图 2

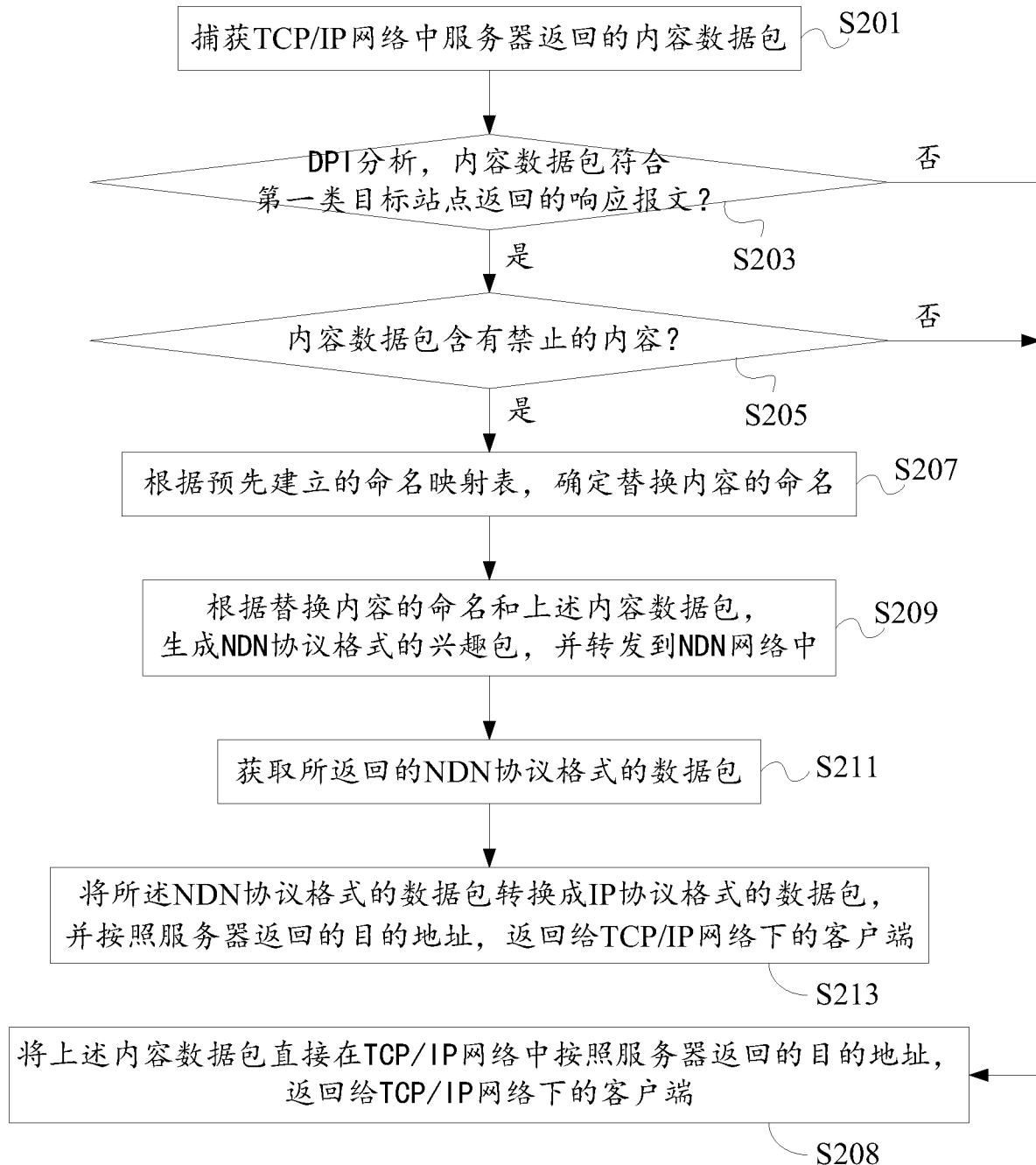


图 3

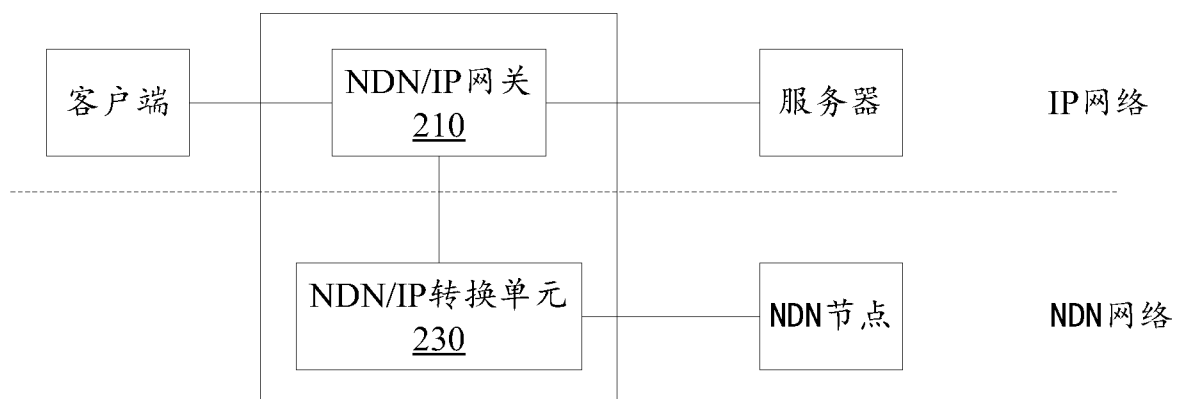


图 4

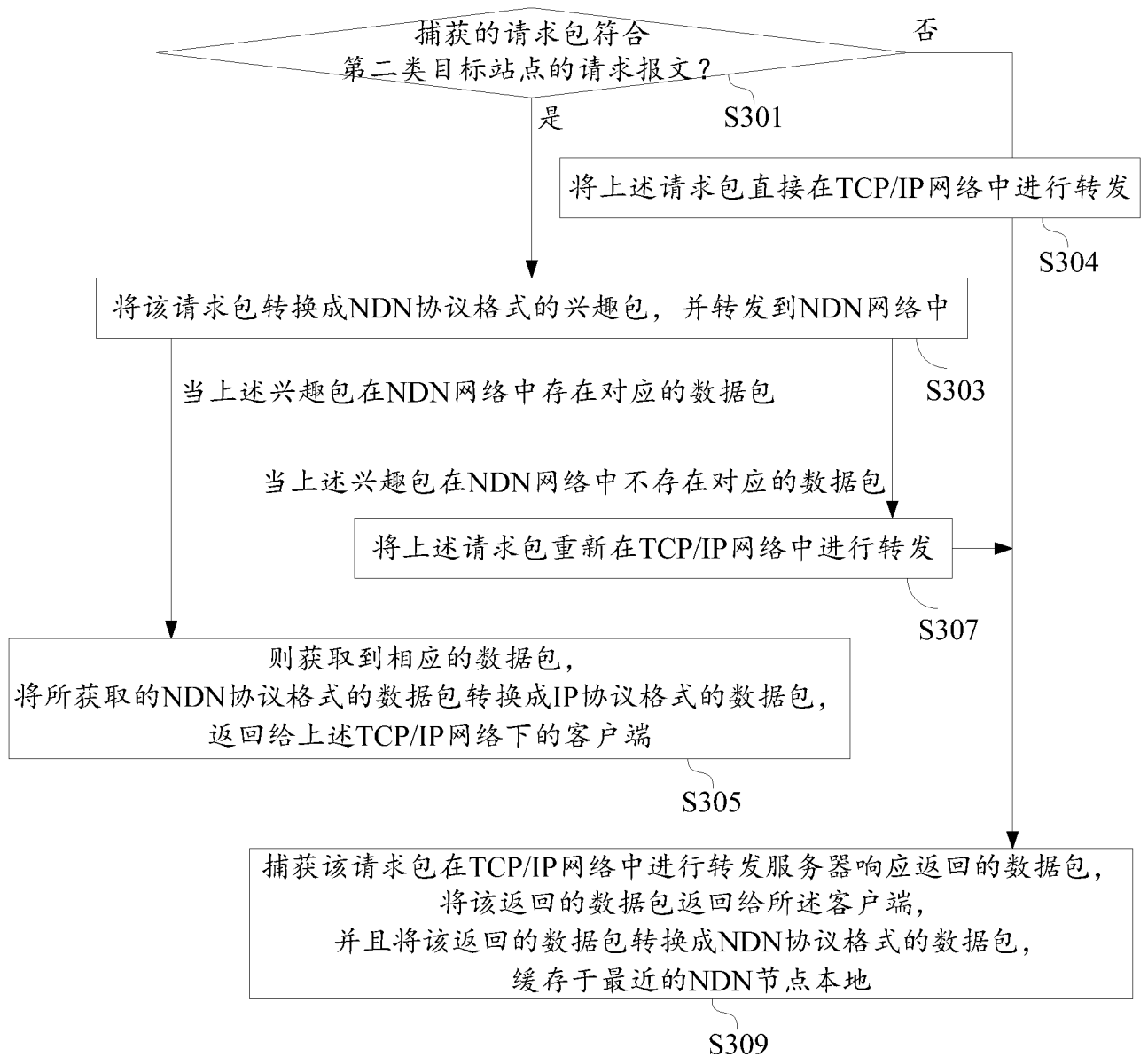


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/096996

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04N 21/266 (2011.01) i
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
CNPAT, CNKI, WPI, EPODOC: 命名数据网络, 互联网, 兴趣包, 数据包, 映射表, 替换, 转发, 符合, 禁止, 内容, 视频, NDN, TCP/IP, interest, data, map, replace, forward, accord, forbid, content, video

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	CN 107634935 A (PEKING UNIVERSITY SHENZHEN GRADUATE SCHOOL), 26 January 2018 (26.01.2018), claims 1-10	1-10
A	CN 103237024 A (PEKING UNIVERSITY SHENZHEN GRADUATE SCHOOL), 07 August 2013 (07.08.2013), description, paragraphs [0031]-[0044]	1-10
A	CN 105763438 A (TSINGHUA UNIVERSITY), 13 July 2016 (13.07.2016), description, paragraphs [0026]-[0027]	1-10
A	CN 106487837 A (PEKING UNIVERSITY SHENZHEN GRADUATE SCHOOL), 08 March 2017 (08.03.2017), entire document	1-10
A	WO 2017000131 A1 (QUALCOMM INCORPORATED), 05 January 2017 (05.01.2017), entire document	1-10
A	雷凯 等, “命名数据网络内容分发机制研究与探讨”, 电信科学, number 9, 30 September 2014 (30.09.2014), entire document, (LEI, Kai et al., “Content Distribution Mechanisms of Named Data Networking”, Telecommunications Science)	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 09 February 2018	Date of mailing of the international search report 26 April 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer YAN, Sai Telephone No. (86-10) 62413293

International application No.
PCT/CN2017/096996

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2017/096996

A. 主题的分类 H04L 29/06 (2006.01) i; H04N 21/266 (2011.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L; H04N 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNPAT, CNKI, WPI, EPODOC: 命名数据网络, 互联网, 兴趣包, 数据包, 映射表, 替换, 转发, 符合, 禁止, 内容, 视频, NDN, TCP/IP, interest, data, map, replace, forward, accord, forbid, content, video		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
E	CN 107634935 A (北京大学深圳研究生院) 2018年 1月 26日 (2018 - 01 - 26) 权利要求1-10	1-10
A	CN 103237024 A (北京大学深圳研究生院) 2013年 8月 7日 (2013 - 08 - 07) 说明书第[0031]-[0044]段	1-10
A	CN 105763438 A (清华大学) 2016年 7月 13日 (2016 - 07 - 13) 说明书第[0026]-[0027]段	1-10
A	CN 106487837 A (北京大学深圳研究生院) 2017年 3月 8日 (2017 - 03 - 08) 全文	1-10
A	WO 2017000131 A1 (QUALCOMM INCORPORATED) 2017年 1月 5日 (2017 - 01 - 05) 全文	1-10
A	雷凯 等. “命名数据网络内容分发机制研究与探讨” 电信科学, 第9期, 2014年 9月 30日 (2014 - 09 - 30), 全文	1-10
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2018年 2月 9日		国际检索报告邮寄日期 2018年 4月 26日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 阎赛 电话号码 (86-10)62413293

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/096996

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	107634935	A	2018年 1月 26日	无	
CN	103237024	A	2013年 8月 7日	无	
CN	105763438	A	2016年 7月 13日	无	
CN	106487837	A	2017年 3月 8日	WO 2017031947 A1	2017年 3月 2日
WO	2017000131	A1	2017年 1月 5日	无	