(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
2013 年 11 月 14 日 (14.11.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/166918 A1

(51) 国际专利分类号:
H04L 12/24 (2006.01)

(21) 国际申请号: PCT/CN2013/074764

(22) 国际申请日: 2013 年 4 月 26 日 (26.04.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210138354.3 2012 年 5 月 7 日 (07.05.2012) CN

(71) 申请人: **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **熊春山 (XIONG, Chunshan)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **周卫华 (ZHOU, Weihua)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **胡华东 (HU, Huadong)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, 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))。

(54) **Title**: DATA PROCESSING METHOD, DEVICE AND SYSTEM

(54) **发明名称** : 一种数据处理的方法、设备及系统

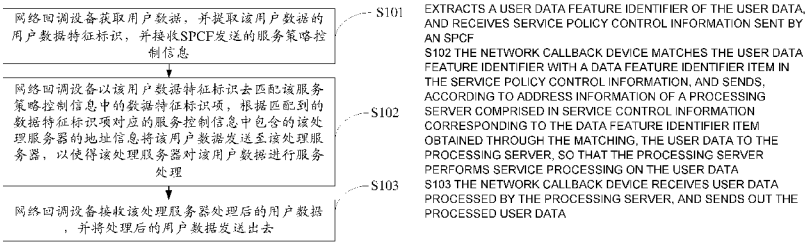

图 1 / Fig. 1

(57) **Abstract**: The present invention relates to the field of network communications, and provides a data processing method, device and system, so as to solve a problem that openness of performing content processing on user data in an existing communication system is poor. The method comprises: a network callback device obtaining user data on a user data transmission channel, extracting a user data feature identifier of the user data, and receiving service policy control information sent by a service policy control function (SPCF); matching the user data feature identifier with a data feature identifier item in the service policy control information, and sending, according to address information of a processing server comprised in service control information corresponding to the data feature identifier item obtained through the matching, the user data to the processing server, so that the processing server performs service processing on the user data; and receiving user data processed by the processing server, and sending out the processed user data. The present invention is used for data processing.

(57) **摘要**: 本发明实施例提供一种数据处理的方法、设备及系统，涉及网络通信领域，以解决现有通信系统中对用户数据进行内容处理的开放性差的问题，该方法包括：网络回调设备获取用户数据传输通道上的用户数据，提取该用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理并接收该处理服务器处理后的用户数据，并将该处理后的用户数据发送出去。本发明用于数据处理。

WO 2013/166918 A1

一种数据处理的方法、设备及系统

本申请要求于2012年5月7日提交中国专利局、申请号为201210138354.3、发明名称为“一种数据处理的方法、设备及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及网络通信领域，尤其涉及一种数据处理的方法、设备及系统。

背景技术

近年来，无线数据业务出现了高速的增长，为了提高用户使用无线通信系统的体验，增强无线通信系统的能力与扩大无线通信系统的容量，无线运营商与无线设备提供商提出了 SMBB（Smart Mobile BroadBand，智能移动宽带）的概念，即在增强无线传输速率的同时，提高无线通信系统的智能。

现有技术中，运营商大多通过在无线通信系统中的接入侧设备，例如基站中，增加具有内容处理功能的单元，其中，内容处理功能可以是对用户数据进行病毒查杀，或者对用户数据进行监控等功能。

为了实现内容处理功能，需要在基站上增加具有内容处理功能的单元，由于基站设置的数量庞大，因此在内容处理功能的开发、维护以及管理上非常困难而且复杂，且由于不同提供商提供的基站实现内容处理功能的方式各不相同，使得不同提供商提供的基站对用户数据的内容处理出现不一致性，因此具有一定的局限性。

发明内容

本发明的实施例提供一种数据处理的方法、设备及系统，以解决现有通信系统中对用户数据进行内容处理的开放性差的问题。

提供一种数据处理的方法，包括:

网络回调设备获取用户数据传输通道上的用户数据，并提取所述

用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

所述网络回调设备以所述用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理；

所述网络回调设备接收所述处理服务器处理后的用户数据，并将所述处理后的用户数据发送出去。

提供一种数据处理的方法，包括：

服务策略控制设备 SPCF 向网络回调设备发送服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息，以使得所述网络回调设备获取用户数据的用户数据特征标识，并以所述用户数据特征标识分别去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理。

提供一种数据处理的方法，包括：

网络回调设备获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

所述网络回调设备以所述用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处

理;

当设置的定时器到达或者超过预设时间时，所述网络回调设备如果没有接收到所述处理服务器发送的处理后的所述用户数据，将保存的所述用户数据发送出去。

提供一种数据处理的方法，包括:

网络回调设备获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息;

所述网络回调设备以所述用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器;

所述网络回调设备接收所述处理服务器发送的指示消息，所述指示消息携带有不需要进行处理的用户数据的第二数据特征标识，根据所述指示消息将后续接收到的携带有所述第二数据特征标识的用户数据发送出去。

提供一种网络回调设备，包括:

第一获取单元，用于获取用户数据，并提取所述用户数据的用户数据特征标识;

第一接收单元，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息;

第一匹配单元，用于以所述第一获取单元提取的用户数据特征标识去匹配所述第一接收单元接收的服务策略控制信息中的数据特征标识项;

第一发送单元，用于根据所述第一匹配单元匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述

用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理；

第一用户数据接收单元，用于接收所述处理服务器处理后的用户数据；

第一处理数据发送单元，用于将所述第一用户数据接收单元接收的处理后的用户数据发送出去。

提供一种服务策略控制设备 SPCF，包括：

第二发送单元，用于向网络回调设备发送服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息，以使得所述网络回调设备获取用户数据的用户数据特征标识，并以所述用户数据特征标识分别去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理。

提供一种处理服务器，包括：

第三接收单元，用于接收网络回调设备发送的用户数据；

功能处理单元，用于对所述第三接收单元接收的用户数据进行服务处理；

第三发送单元，用于将所述功能处理单元处理后的用户数据发送至所述网络回调设备。

提供一种网络回调设备，包括：

第四获取单元，用于获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识；

第四接收单元，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

第四匹配单元，用于以所述第四获取单元提取的用户数据特征标

识去匹配所述第四接收单元接收的服务策略控制信息中的数据特征标识项；

第四发送单元，用于根据所述第四匹配单元匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理；

定时器，用于记录预设时间，并根据所述第四发送单元根据所述服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器确定启动，且在到达或者超过所述预设时间时停止；

第四用户数据发送单元，用于当所述定时器到达或者超过预设时间时，所述网络回调设备如果没有接收到所述处理服务器发送的处理后的所述用户数据，将保存的所述用户数据发送出去。

提供一种网络回调设备，包括：

第五获取单元，用于获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识；

第五接收单元，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

第五匹配单元，用于以所述第五获取单元提取的用户数据特征标识去匹配所述第五接收单元接收的服务策略控制信息中的数据特征标识项；

第五发送单元，用于根据所述第五匹配单元匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器；

第五指示消息接收单元，用于接收所述处理服务器发送的指示消息，所述指示消息携带有不需要进行处理的用户数据的第二数据特征标识；

第五用户数据发送单元，用于根据所述指示消息将后续接收到的

携带有所述第二数据特征标识的用户数据发送出去。

提供一种数据处理的系统，包括：网络回调设备、服务策略控制设备 SPCF、处理服务器，

所述网络回调设备，用于获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息，以所述用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，接收所述处理服务器处理后的用户数据，并将所述处理后的用户数据发送出去；

所述 SPCF，用于向网络回调设备发送服务策略控制信息；

所述处理服务器，用于接收所述网络回调设备发送的用户数据，对所述用户数据进行服务处理，并将所述处理后的用户数据发送至所述网络回调设备。

本发明实施例提供一种数据处理的方法、设备及系统，通过将接入侧设备或者核心网设备中的功能处理单元设置到处理服务器中，使得处理服务器对用户数据进行相应的服务处理，这样，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的内容处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，

在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例提供的一种数据处理的方法示意图；

图 2 为本发明实施例提供的另一种数据处理的方法示意图；

图 3 为本发明实施例提供的另一种数据处理的方法示意图；

图 4 为本发明实施例提供的一种数据处理的方法的流程示意图；

图 5 为本发明实施例提供的一种网络回调设备的结构示意图；

图 6 为本发明实施例提供的一种网络回调设备的结构示意图；

图 7 为本发明实施例提供的另一种网络回调设备的结构示意图；

图 8 为本发明实施例提供的另一种网络回调设备的结构示意图；

图 9 为本发明实施例提供的一种 SPCF 的结构示意图；

图 10 为本发明实施例提供的另一种 SPCF 的结构示意图；

图 11 为本发明实施例提供的另一种 SPCF 的结构示意图；

图 12 为本发明实施例提供的一种处理服务器的结构示意图；

图 13 为本发明实施例提供的一种网络回调设备的结构示意图；

图 14 为本发明实施例提供的一种网络回调设备的结构示意图；

图 15 为本发明实施例提供的一种数据处理系统的结构示意图；

图 16 为本发明实施例提供的另一种数据处理系统的结构示意图；

图 17 为本发明实施例提供的一种无线通信网络场景下数据处理系统的参考示意图；

图 18 为本发明实施例提供的另一种无线通信网络场景下数据处理系统的参考示意图；

图 19 为本发明实施例提供的另一种无线通信网络场景下数据处理系统的参考示意图；

图 20 为本发明实施例提供的一种固网场景下数据处理系统的参考示意图；

图 21 为本发明实施例提供的一种无线通信网络和固网融合场景下数据处理系统的参考示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例提供一种数据处理的方法，如图 1 所示，该实施例的执行主体为网络回调设备，该方法包括:

S101、网络回调设备获取用户数据，并提取该用户数据的用户数据特征标识，并接收 SPCF 发送的服务策略控制信息。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项分别对应的服务控制信息，该服务控制信息中包含有对用户数据进行服务处理的处理服务器的地址信息。

进一步地，该用户数据包括用户上行数据和/或用户下行数据。

具体地，网络回调设备接收 SPCF 发送的不同用户和/或同一用户不同的数据流的服务策略控制信息，这些服务策略控制信息在网络回调设备中组成集合，网络回调设备存储该集合。

S102、网络回调设备以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理;

进一步地，根据该服务策略控制信息中的数据特征标识项的优先级，按照高优先级至低优先级的顺序，以该用户数据特征标识分别去匹配该服务策略控制信息中的数据特征标识项。

更进一步地，若该用户数据特征标识不能匹配集合中所有的数据特征标识项，则将该用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络

节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

具体地，用户数据特征标识及服务策略控制信息中的数据特征标识项分别由以下 a 至 i 中的至少一个 IP 包特征标识和/或承载特征标识组成:

a、源 IP 地址或者源 IP 地址的区间或列表;

b、目标 IP 地址或者目标 IP 地址的区间或列表;

c、源端口号或者源端口号的区间或列表;

d、目的端口号或者目的端口号的区间或列表;

e、传输协议号或者传输协议号区间或列表;

f、IP 头字段中的 DSCP（Differentiated Services Code Point，差分服务码点）或 TOS（Terms Of Service，服务类型）;

g、IPv6（Internet Protocol Version 6，第六代互联网协议）头字段中的流标签;

h、若用户数据使用了 IPsec（Internet Protocol Security，互联网协议安全）保护，IPsec 报文中的 SPI（Security parameter Index 安全参数索引）;

i、对于 3GPP（The 3rd Generation Partnership Project，第三代合作项目）网络，还可以根据承载的参数 QCI（QoS Class Identifier， QoS 类型标识），ARP(Allocation Retention Priority ，分配与保留优先级)，承载的类型，GBR（Guaranteed Bit Rate，保证比特速率）速率区间，MBR（Maximum Bit Rate，最大比特速率）速率区间等参数及其组合。

网络回调设备提取该用户数据的用户数据特征标识就是从用户的 IP 数据包中提取出上述 a 至 i 中的 IP 包特征标识。一个最常用的数据特征标识是 IP 五元组，即源 IP 地址，目标 IP 地址，源端口，目标端口，协议类型，分别对应上述的 a,b,c,d,e 这五个 IP 包特征标识。

用户数据特征标识匹配该服务策略控制信息中的数据特征标识项的过程是一个 DPI（Deep Packet Inspection 深度包检测）过程中的匹配部分，它是一个简单的逻辑运算与判断过程。例如，网络回调设备提取到该用户数据的用户数据特征标识为：

{源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，源端口为 1234,目标端口为 80,协议类型为 TCP}；

而服务策略控制信息中的数据特征标识项有三个，并且分别是：

项 1={源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80}；

项 2={源 IP 地址 3.3.3.3，目标 IP 地址为 4.4.4.4，源端口为 4321,目标端口为 80,协议类型为 TCP }；

项 3={源 IP 地址 1.1.1.0 到 3.3.3.3 的所有 IP 地址，目标 IP 地址为 5.5.5.5，源端口为 1234,目标端口为 80,协议类型为 TCP }。

显然，用户数据特征标识中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2 及目标端口为 80 均与项 1 中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80 匹配。但用户数据特征标识中源端口为 1234 及协议类型为 TCP 在项 1 中未作限定，由于源端口及协议类型未作限定表示任意的源端口及协议类型的值都匹配，因此，用户数据的用户数据特征标识是匹配服务策略控制信息中的项 1 的。而用户数据特征标识中的源 IP 地址及目标 IP 地址与项 2 中的值不匹配，因此用户数据特征标识不匹配项 2。同样的，用户数据特征标识中的目标 IP 地址与项 3 中的目标 IP 地址值不匹配，因此用户数据特征标识不匹配项 3。

另外，上述服务控制信息中还包括：用户数据的传输方式，以便该网络回调设备还可以根据该用户数据传输方式将该用户数据发送至该处理服务器，上述的用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP（Encapsulating Security Payload，封装安全负载）隧道方式，本发明实施例并不局限于此。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体可以是，网络回调设备为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送

至该处理服务器，该用户数据包括不同用户设备的用户数据，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应，该方式是将所有的用户数据都在同一个传输隧道内传输，例如一个网络回调设备与一个处理服务器之间使用同一个 IPsec 隧道来传输不同的用户的 IP 数据包，并使用 GRE（Generic Routing Encapsulation，通用路由封装）来封装用户 IP 数据包，GRE 扩展头中的四字节的 Key 的不同值来区分不同的用户。使用同一个 IPsec 隧道可以使得多个用户共享一个共同的 IPsec 隧道及其安全保证，这个 IPsec 隧道不会随着用户数据数目的变化而变化，因此，具有很好的可扩展性，并且也大大地简化了安全过程。但是，当这个安全隧道被破解后，所有的用户的数据均可被攻击者看到。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体还可以是，网络回调设备为该不同用户设备的用户数据分配不同的第一隧道标识，通过与该不同的第一隧道标识对应的不同的隧道将该不同用户设备的用户数据发送至该处理服务器，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应，在该方式中，各个用户数据分别在各自的隧道内进行传输，例如，一个网络回调设备与一个处理服务器之间为不同的用户数据建立并使用不同的 IPsec 隧道来传输此 IP 数据包，这样的好处是，当一个用户数据所使用的 IPsec 隧道被破解后（例如，攻击可破解并得到隧道内传输的明文数据），其它用户数据的 IPsec 隧道仍然是安全的。这个方法的缺点是由于用户数据的动态变化，如用户重新增加了一个 TCP 数据连接，IPsec 隧道的建立与删除过程比较频繁，引入较大的隧道建立时延。

在实际应用中，处理服务器需要处理的用户数据可能非常庞大，而且处理服务器与网络回调设备之间的数据传输通道也可能因为大量的

传输数据而发生拥塞，从而造成用户数据服务处理的时延，以使得网络回调设备无法及时接收到处理服务器处理后的用户数据，因此，本发明实施例还包括以下步骤:

在根据服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器之前，网络回调设备保存该用户数据，并启动定时器，该定时器记录有预设时间;

当该定时器到达或者超过预设时间时，该网络回调设备如果没有接收到该处理服务器发送的处理后的该用户数据，将该用户数据发送出去，这样，能够保证该用户数据的正常传输，而不会因为处理服务器数据处理的时延造成系统通信数据传输的中断。

上述网络回调设备和处理服务器之间的隧道为该网络回调设备和处理服务器之间的数据传输信道。

S103、网络回调设备接收该处理服务器处理后的用户数据，并将处理后的用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为终端 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

进一步地，在该处理服务器确认该用户数据不需要进行处理后，接收该处理服务器发送的指示消息，该指示消息携带有不需要进行处理的用户数据的第二数据特征标识，根据该指示消息将后续接收到的携带有该第二数据特征标识的用户数据发送出去，这样，对于一些处理服务器确认不需要进行处理的用户数据，网络回调设备就不在将后续的不需要进行处理的用户数据发送至云服务，而直接发送出去，节约了网络资源，减少了用户数据传输的时延，同时降低了处理服务器

对用户数据处理的损耗，由于目前的一些 IP 协议不支持这里所定义的命令指示，因此需要将使用的 IP 协议中添加或扩展一些标识位，如在 TCP 头中使用 Reserved 部分来扩展定义这个指示或使用扩展的 TCP 头选项来定义这个指示消息。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

本实施例提供的数据处理的方法，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供另一种数据处理的方法，如图 2 所示，该实施例的执行主体为网络回调设备，该方法包括：

S201、网络回调设备获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息。

进一步地，该用户数据包括用户上行数据和/或用户下行数据。

S202、网络回调设备以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理。

具体地，用户数据特征标识及服务策略控制信息包含的数据特征标识项分别由以下 a 至 i 中的至少一个 IP 包特征标识和/或承载特征标识组成：

a、源 IP 地址或者源 IP 地址的区间或列表;

b、目标 IP 地址或者目标 IP 地址的区间或列表;

c、源端口号或者源端口号的区间或列表;

d、目的端口号或者目的端口号的区间或列表;

e、传输协议号或者传输协议号区间或列表;

f、IP 头字段中的 DSCP（Differentiated Services Code Point，差分服务码点）或 TOS（Terms Of Service，服务类型）;

g、IPv6（Internet Protocol Version 6，第六代互联网协议）头字段中的流标签;

h、若用户数据使用了 IPsec（Internet Protocol Security，互联网协议安全）保护，IPsec 报文中的 SPI（Security parameter Index 安全参数索引）;

i、对于 3GPP（The 3rd Generation Partnership Project，第三代合作项目）网络，还可以根据承载的参数 QCI（QoS Class Identifier， QoS 类型标识），ARP(Allocation Retention Priority ，分配与保留优先级)，承载的类型，GBR（Guaranteed Bit Rate，保证比特速率）速率区间，MBR（Maximum Bit Rate，最大比特速率）速率区间等参数及其组合。

网络回调设备提取该用户数据的用户数据特征标识就是从用户的 IP 数据包中提取出上述 a 至 i 中的 IP 包特征标识。一个最常用的数据特征标识是 IP 五元组，即源 IP 地址，目标 IP 地址，源端口，目标端口，协议类型，分别对应上述的 a,b,c,d,e 这五个 IP 包特征标识。

用户数据特征标识匹配该服务策略控制信息中的数据特征标识项的过程是一个 DPI（Deep Packet Inspection 深度包检测）过程中的匹配部分，它是一个简单的逻辑运算与判断过程。例如，网络回调设备提取到该用户数据的用户数据特征标识为:

{源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，源端口为 1234,目标端口为 80,协议类型为 TCP};

而服务策略控制信息中的数据特征标识项有三个，并且分别是:

项 1={源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80};

项 2={源 IP 地址 3.3.3.3，目标 IP 地址为 4.4.4.4，源端口为 4321，目标端口为 80,协议类型为 TCP };

项 3={源 IP 地址 1.1.1.0 到 3.3.3.3 的所有 IP 地址，目标 IP 地址为 5.5.5.5，源端口为 1234,目标端口为 80,协议类型为 TCP }。

显然，用户数据特征标识中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2 及目标端口为 80 均与项 1 中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80 匹配。但用户数据特征标识中源端口为 1234 及协议类型为 TCP 在项 1 中未作限定，由于源端口及协议类型未作限定表示任意的源端口及协议类型的值都匹配，因此，用户数据的用户数据特征标识是匹配服务策略控制信息中的项 1 的。而用户数据特征标识中的源 IP 地址及目标 IP 地址与项 2 中的值不匹配，因此用户数据特征标识不匹配项 2。同样的，用户数据特征标识中的目标 IP 地址与项 3 中的目标 IP 地址值不匹配，因此用户数据特征标识不匹配项 3。

另外，上述服务控制信息中还包括：用户数据的传输方式，以便该网络回调设备还可以根据该用户数据传输方式将该用户数据发送至该处理服务器，上述的用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP（Encapsulating Security Payload，封装安全负载）隧道方式，本发明实施例并不局限于此。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体可以是，网络回调设备为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应，该方式是将所有的用户数据都在同一个传输隧道内传输，例如一个网络回调设备与一个处理服务器之间使用同一个 IPsec 隧道来传输不同的用户的 IP 数据包，并使用 GRE（Generic Routing Encapsulation，通用路由封装）来封装用户 IP 数据包，GRE 扩

展头中的四字节的 Key 的不同值来区分不同的用户。使用同一个 IPsec 隧道可以使得多个用户共享一个共同的 IPsec 隧道及其安全保证，这个 IPsec 隧道不会随着用户数据数目的变化而变化，因此，具有很好的可扩展性，并且也大大地简化了安全过程。但是，当这个安全隧道被破解后，所有的用户的数据均可被攻击者看到。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体还可以是，网络回调设备为该不同用户设备的用户数据分配不同的第一隧道标识，通过与该不同的第一隧道标识对应的不同的隧道将该不同用户设备的用户数据发送至该处理服务器，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应，在该方式中，各个用户数据分别在各自的隧道内进行传输，例如，一个网络回调设备与一个处理服务器之间为不同的用户数据建立并使用不同的 IPsec 隧道来传输此 IP 数据包，这样的好处是，当一个用户数据所使用的 IPsec 隧道被破解后（例如，攻击可破解并得到隧道内传输的明文数据），其它用户数据的 IPsec 隧道仍然是安全的。这个方法的缺点是由于用户数据的动态变化，如用户重新增加了一个 TCP 数据连接，IPsec 隧道的建立与删除过程比较频繁，引入较大的隧道建立时延。

S203、当设置的定时器到达或者超过预设时间时，该网络回调设备如果没有接收到该处理服务器发送的处理后的该用户数据，将保存的该用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行

的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为终端 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

本实施例提供的数据处理的方法，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供另一种数据处理的方法，如图 3 所示，该实施例的执行主体为网络回调设备，该方法包括:

S301、网络回调设备获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息。

进一步地，该用户数据包括用户上行数据和/或用户下行数据。

S302、网络回调设备以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器。

具体地，用户数据特征标识及服务策略控制信息包含的数据特征标识项分别由以下 a 至 i 中的至少一个 IP 包特征标识和/或承载特征标识组成:

a、源 IP 地址或者源 IP 地址的区间或列表;

b、目标 IP 地址或者目标 IP 地址的区间或列表;

c、源端口号或者源端口号的区间或列表;

d、目的端口号或者目的端口号的区间或列表;

e、传输协议号或者传输协议号区间或列表;

f、IP 头字段中的 DSCP（Differentiated Services Code Point，差分服务码点）或 TOS（Terms Of Service，服务类型）;

g、IPv6（Internet Protocol Version 6，第六代互联网协议）头字段中的流标签;

h、若用户数据使用了 IPsec（Internet Protocol Security，互联网协议安全）保护，IPsec 报文中的 SPI（Security parameter Index 安全参数索引）;

i、对于 3GPP（The 3rd Generation Partnership Project，第三代合作项目）网络，还可以根据承载的参数 QCI（QoS Class Identifier， QoS 类型标识），ARP(Allocation Retention Priority ，分配与保留优先级)，承载的类型，GBR（Guaranteed Bit Rate，保证比特速率）速率区间，MBR（Maximum Bit Rate，最大比特速率）速率区间等参数及其组合。

网络回调设备提取该用户数据的用户数据特征标识就是从用户的 IP 数据包中提取出上述 a 至 i 中的 IP 包特征标识。一个最常用的数据特征标识是 IP 五元组，即源 IP 地址，目标 IP 地址，源端口，目标端口，协议类型，分别对应上述的 a,b,c,d,e 这五个 IP 包特征标识。

用户数据特征标识匹配该服务策略控制信息中的数据特征标识项的过程是一个 DPI（Deep Packet Inspection 深度包检测）过程中的匹配部分，它是一个简单的逻辑运算与判断过程。例如，网络回调设备提取到该用户数据的用户数据特征标识为:

{源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，源端口为 1234,目标端口为 80,协议类型为 TCP};

而服务策略控制信息中的数据特征标识项有三个，并且分别是:

项 1={源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80};

项 2={源 IP 地址 3.3.3.3，目标 IP 地址为 4.4.4.4，源端口为 4321，目标端口为 80,协议类型为 TCP };

项 3={源 IP 地址 1.1.1.0 到 3.3.3.3 的所有 IP 地址，目标 IP 地址为 5.5.5.5，源端口为 1234,目标端口为 80,协议类型为 TCP }。

显然，用户数据特征标识中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2 及目标端口为 80 均与项 1 中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80 匹配。但用户数据特征标识中源端口为 1234 及协议类型为 TCP 在项 1 中未作限定，由于源端口及协议类型未作限定表示任意的源端口及协议类型的值都匹配，因此，用户数据的用户数据特征标识是匹配服务策略控制信息中的项 1 的。而用户数据特征标识中的源 IP 地址及目标 IP 地址与项 2 中的值不匹配，因此用户数据特征标识不匹配项 2。同样的，用户数据特征标识中的目标 IP 地址与项 3 中的目标 IP 地址值不匹配，因此用户数据特征标识不匹配项 3。

另外，上述服务控制信息中还包括：用户数据的传输方式，以便该网络回调设备还可以根据该用户数据传输方式将该用户数据发送至该处理服务器，上述的用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP（Encapsulating Security Payload，封装安全负载）隧道方式，本发明实施例并不局限于此。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体可以是，网络回调设备为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应，该方式是将所有的用户数据都在同一个传输隧道内传输，例如一个网络回调设备与一个处理服务器之间使用同一个 IPsec 隧道来传输不同的用户的 IP 数据包，并使用 GRE（Generic Routing Encapsulation，通用路由封装）来封装用户 IP 数据包，GRE 扩

展头中的四字节的 Key 的不同值来区分不同的用户。使用同一个 IPsec 隧道可以使得多个用户共享一个共同的 IPsec 隧道及其安全保证，这个 IPsec 隧道不会随着用户数据数目的变化而变化，因此，具有很好的可扩展性，并且也大大地简化了安全过程。但是，当这个安全隧道被破解后，所有的用户的数据均可被攻击者看到。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体还可以是，网络回调设备为该不同用户设备的用户数据分配不同的第一隧道标识，通过与该不同的第一隧道标识对应的不同的隧道将该不同用户设备的用户数据发送至该处理服务器，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应，在该方式中，各个用户数据分别在各自的隧道内进行传输，例如，一个网络回调设备与一个处理服务器之间为不同的用户数据建立并使用不同的 IPsec 隧道来传输此 IP 数据包，这样的好处是，当一个用户数据所使用的 IPsec 隧道被破解后（例如，攻击可破解并得到隧道内传输的明文数据），其它用户数据的 IPsec 隧道仍然是安全的。这个方法的缺点是由于用户数据的动态变化，如用户重新增加了一个 TCP 数据连接，IPsec 隧道的建立与删除过程比较频繁，引入较大的隧道建立时延。

S303、在该处理服务器确认该用户数据不需要进行处理后，该网络回调设备接收该处理服务器发送的指示消息，该指示消息携带有不需要进行处理的用户数据的第二数据特征标识，根据该指示消息将后续接收到的携带有该第二数据特征标识的用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为终端 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

本实施例提供的数据处理的方法，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种数据处理的方法，该实施例的执行主体为 SPCF，该方法包括：

SPCF 向网络回调设备发送服务策略控制信息。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息。

该网络回调设备获取用户数据的用户数据特征标识，并以该用户数据特征标识分别去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理。

示例地，该 SPCF 向网络回调设备发送服务策略控制信息之前，本实施例还包括：

SPCF 接收 AF（Application Functions，应用功能服务器）发送的数

据特征标识项，并确定该数据特征标识项所对应的用户标识。

例如，若 AF 是 IMS(IP Multimedia Subsystems，IP 多媒体子系统)中的 P-CSCF（Proxy-Call Session Control Function，代理呼叫会话控制功能），则 AF 可以通过 IMS 中的标识识别出 UE 的 MSISDN（Mobile Subscriber ISDN Number，移动用户综合业务数据网）号码。另一个方法是 SPCF 从 AF 提供的用户 IP 地址（对于上行用户数据，则是源 IP 地址，对于下行用户数据，则是目标 IP 地址），然后 SPCF 通过查询 AF 对应的 PDN(Public Data Network，公用数据网)连接的 PGW(Packet Data Network Gateway，分组数据网网关)或 GGSN（Gateway GPRS Support Node，GPRS 网关支持节点）或 PCRF(Policy and Charging Rules Function，策略与计费控制服务器）就可以得到 UE 的 MSISDN 标识。

SPCF 根据该用户标识从 SPR（Subscription Profile Repository，签约信息服务器）中获取与该用户标识对应的服务控制信息，并根据该用户标识确定该用户标识所对应的网络回调设备。

其中，SPCF 确定该用户标识所对应的网络回调设备的方法有很多种，例如，SPCF 可以根据运营商所配置的规则来定义网络回调设备类型，如网络回调设备是 PGW 或 GGSN，或 RAN(Radio Access Network，无线接入网)节点上的设备，如 RNC（Radio Network Controller，无线网络控制器）或 eNB(evolved Node B，演进形基站）或 BSC(Base Station Controller，基站控制器），或其它设备如 SGSN（Serving GPRS Support Node，服务支持节点）或 SGW（Serving Gateway，服务网关）。若网络回调设备类型是 PGW 或 GGSN，则 SPCF 通过用户 IP 地址或 AF 对应的 PDN 连接就可确定网络回调设备类型 PGW 或 GGSN 的 IP 地址，这种对应关系通常是静态的，而且通常是配置在 SPCF 中的。若网络回调设备类型是 RNC 或 eNB 或 BSC，或其它设备如 SGSN 或 SGW，则 SPCF 首先确定 PGW 或 GGSN，然后通过查询 PGW 或 GGSN 得到 UE

当前所在的 RNC 或 eNB 或 BSC，或 SGSN 或 SGW 标识，并通过 DNS 或查询配置的方法得到这个回调设备类型的 IP 地址。另一个方法是 SPCF通过查询事先确定的PGW或GGSN直接得到UE当前所在的RNC 或 eNB 或 BSC，或 SGSN 或 SGW 的 IP 地址。若网络回调设备是 RNC 或 eNB 或 BSC，网络需要开启位置报告功能，这样当 UE 移动时，UE 当前所在的 RNC 或 eNB 或 BSC 才能报告其标识给 PGW 或 GGSN。还有一种方法是，PGW 或 GGSN 将 UE 当前所在的网络回调设备，如（RNC 或 eNB 或 BSC） 和/或（SGSN 或 SGW） 和/或 （PGW 或 GGSN）的标识上报给 AF，SPCF 直接从 AF 中得到此 UE 的网络回调设备标识（如 IP 地址）。

则 SPCF 向网络回调设备发送服务策略控制信息，包括：

该 SPCF 向该用户标识所对应的网络回调设备发送包括该数据特征标识项与该用户标识对应的服务控制信息的服务策略控制信息。

示例地，本实施例还包括：

该 SPCF 根据自身配置的数据特征标识项，确定对所有的用户数据进行特定服务处理的处理服务器的地址信息，然后向网络中所有网络回调设备发送该服务策略控制信息。通常的，这是运营商根据当地（如法律或法规）的要求所采取的配置，如有些国家不允许其居民访问一些特定 IP 地址或特定域名的网站。

进一步地，SPCF 根据该用户标识确定该用户数据传输方式，将该用户数据传输方式承载在该服务控制信息中，该用户数据传输方式用于指示该网络回调设备通过该用户数据传输方式将该用户数据发送给该处理服务器。

示例地，该用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP 隧道方式。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

本实施例提供的数据处理的方法，对用户数据的处理不再受接入

侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种数据处理的方法，如图 4 所示，该实施例中的处理服务器为云服务器，该方法具体步骤包括:

S401、SPCF 接收 AF 发送的数据特征标识项，并确定该数据特征标识项所对应的用户标识。

例如，若 AF 是 IMS 中的 P-CSCF，则 AF 可以通过 IMS 中的标识识别出 UE 的 MSISDN 号码。另一个方法是 SPCF 从 AF 提供的用户 IP 地址（对于上行用户数据，则是源 IP 地址，对于下行用户数据，则是目标 IP 地址），然后 SPCF 通过查询 AF 对应的 PDN 连接的 PGW 或 GGSN 或 PCRF 就可以得到 UE 的 MSISDN 标识。

S402、SPCF 根据该用户标识从 SPR 中获取与该用户标识对应的服务控制信息，并根据该用户标识确定该用户标识所对应的网络回调设备。

其中，该用户数据包括用户上行数据和/或用户下行数据，该服务控制信息可以是对用户数据的病毒查杀、视频数据或者音频数据的转码、网页翻译的缓存或对用户数据的监控等功能信息，用户签约的服务控制信息并不局限于一个，同一个用户可以签约多个服务控制信息。

SPCF 确定该用户标识所对应的网络回调设备的方法有很多种，例如，SPCF 可以根据运营商所配置的规则来定义网络回调设备类型，如网络回调设备是 PGW 或 GGSN，或 RAN 节点上的设备，如 RNC 或 eNB 或 BSC，或其它设备如 SGSN 或 SGW。若网络回调设备类型是 PGW 或 GGSN，则 SPCF 通过用户 IP 地址或 AF 对应的 PDN 连接就可确定网络回调设备类型 PGW 或 GGSN 的 IP 地址，这种对应关系通常是静态的，而且通常是配置在 SPCF 中的。若网络回调设备类型是 RNC 或 eNB 或 BSC，或其它设备如 SGSN 或 SGW，则 SPCF 首先确定 PGW 或 GGSN，

然后通过查询PGW或GGSN得到UE当前所在的RNC或eNB或BSC，或SGSN或SGW标识，并通过DNS或查询配置的方法得到这个回调设备类型的IP地址。另一个方法是SPCF通过查询事先确定的PGW或GGSN直接得到UE当前所在的RNC或eNB或BSC，或SGSN或SGW的IP地址。若网络回调设备是RNC或eNB或BSC，网络需要开启位置报告功能，这样当UE移动时，UE当前所在的RNC或eNB或BSC才能报告其标识给PGW或GGSN。还有一种方法是，PGW或GGSN将UE当前所在的网络回调设备，如（RNC或eNB或BSC）和/或（SGSN或SGW）和/或（PGW或GGSN）的标识上报给AF，SPCF直接从AF中得到此UE的网络回调设备标识（如IP地址）。

另外，该SPCF还可以根据自身配置的数据特征标识项，确定对所有的用户数据进行特定服务处理的云服务器的地址信息，然后向网络中所有的的网络回调设备发送该服务策略控制信息。通常的，这是运营商根据当地（如法律或法规）的要求所采取的配置，如有些国家不允许其居民访问一些特定IP地址或特定域名的网站。

S403、网络回调设备接收SPCF发送的服务策略控制信息。

具体地，网络回调设备接收SPCF发送的不同用户和/或同一用户不同的数据流的服务策略控制信息，这些服务策略控制信息在网络回调设备中组成集合，网络回调设备存储该集合。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项分别对应的服务控制信息，该服务控制信息中包含有对用户数据进行服务处理的云服务器的地址信息及用户数据传输方式，该用户数据传输方式可以采用IPsec的加密与完整性保护的ESP（Encapsulating Security Payload，封装安全负载）隧道方式，该用户数据包括用户上行数据和/或用户下行数据。

S404、网络回调设备获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识。

需要说明的是，步骤S404并不局限于在步骤S403之后进行，由于步骤S404中网络回调设备获取用户数据的过程和步骤S401至步骤S403中网络回调设备接收SPCF发送的服务策略控制信息的过程是相对独立的过程并不存在绝对的先后顺序，因此，步骤S404只需在步骤

S405 之前进行即可。

S405、网络回调设备以该用户数据特征标识分别去匹配该服务策略控制信息中的数据特征标识项。

进一步地，网络回调设备根据该服务策略控制信息中的数据特征标识项的优先级，按照高优先级至低优先级的顺序，以该用户数据特征标识分别去匹配该服务策略控制信息中的数据特征标识项。

具体地，用户数据特征标识及服务策略控制信息中的数据特征标识项分别由以下 a 至 i 中的至少一个 IP 包特征标识和/或承载特征标识组成:

a、源 IP 地址或者源 IP 地址的区间或列表;

b、目标 IP 地址或者目标 IP 地址的区间或列表;

c、源端口号或者源端口号的区间或列表;

d、目的端口号或者目的端口号的区间或列表;

e、传输协议号或者传输协议号区间或列表;

f、IP 头字段中的 DSCP 或 TOS;

g、IPv6 头字段中的流标签;

h、若用户数据使用了 IPsec 保护，IPsec 报文中的 SPI;

i、对于 3GPP 网络，还可以根据承载的参数 QCI，ARP，承载的类型，GBR 速率区间，MBR 速率区间等参数及其组合。

网络回调设备提取该用户数据的用户数据特征标识就是从用户的 IP 数据包中提取出上述 a 至 i 中的 IP 包特征标识。一个最常用的数据特征标识是 IP 五元组，即源 IP 地址，目标 IP 地址，源端口，目标端口，协议类型，分别对应上述的 a,b,c,d,e 这五个 IP 包特征标识。

用户数据特征标识匹配该集合中的数据特征标识项的过程是一个 DPI 过程中的匹配部分，它是一个简单的逻辑运算与判断过程。例如，网络回调设备提取到该用户数据的用户数据特征标识为:

{源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，源端口为 1234,目标端口为 80,协议类型为 TCP};

而服务策略控制信息集合中的各个数据特征标识项有三个，并且分别是：

项 1={源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80}；

项 2={源 IP 地址 3.3.3.3，目标 IP 地址为 4.4.4.4，源端口为 4321，目标端口为 80,协议类型为 TCP }；

项 3={源 IP 地址 1.1.1.0 到 3.3.3.3 的所有 IP 地址，目标 IP 地址为 5.5.5.5，源端口为 1234,目标端口为 80,协议类型为 TCP }。

显然，用户数据特征标识中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2 及目标端口为 80 均与项 1 中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80 匹配。但用户数据特征标识中源端口为 1234 及协议类型为 TCP 在项 1 中未作限定，由于源端口及协议类型未作限定表示任意的源端口及协议类型的值都匹配，因此，用户数据的用户数据特征标识是匹配服务策略控制信息集合中的项 1 的。而用户数据特征标识中的源 IP 地址及目标 IP 地址与项 2 中的值不匹配，因此用户数据特征标识不匹配项 2。同样的，用户数据特征标识中的目标 IP 地址与项 3 中的目标 IP 地址值不匹配，因此用户数据特征标识不匹配项 3。

优选地，在根据服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器之前，网络回调设备保存该用户数据，并启动定时器，该定时器记录有预设时间。

当该定时器到达或者超过预设时间时，该网络回调设备如果没有接收到该处理服务器发送的处理后的该用户数据，将该用户数据发送出去，这样，能够保证该用户数据的正常传输，而不会因为处理服务器数据处理的时延造成系统通信数据传输的中断。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行

的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

S406、网络回调设备根据匹配到的数据特征标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器。

上述服务控制信息中还包括：用户数据的传输方式，以便该网络回调设备还可以根据该用户数据传输方式将该用户数据发送至该处理服务器，上述的用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP（Encapsulating Security Payload，封装安全负载）隧道方式，本发明实施例并不局限于此。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体可以是，网络回调设备为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应，该方式是将所有的用户数据都在同一个传输隧道内传输，例如一个网络回调设备与一个处理服务器之间使用同一个 IPsec 隧道来传输不同的用户的 IP 数据包，并使用 GRE（Generic Routing Encapsulation，通用路由封装）来封装用户 IP 数据包，GRE 扩展头中的四字节的 Key 的不同值来区分不同的用户。使用同一个 IPsec 隧道可以使得多个用户共享一个共同的 IPsec 隧道及其安全保证，这个 IPsec 隧道不会随着用户数据数目的变化而变化，因此，具有很好的可扩展性，并且也大大地简化了安全过程。但是，当这个安全隧道被破解后，所有的用户的数据均可被攻击者看到。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体还可以是，网络回调设备为该不同用户设备的用户数据分配不同的第一隧道标识，通过

与该不同的第一隧道标识对应的不同的隧道将该不同用户设备的用户数据发送至该处理服务器，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应，在该方式中，各个用户数据分别在各自的隧道内进行传输，例如，一个网络回调设备与一个处理服务器之间为不同的用户数据建立并使用不同的 IPsec 隧道来传输此 IP 数据包，这样的好处是，当一个用户数据所使用的 IPsec 隧道被破解后（例如，攻击可破解并得到隧道内传输的明文数据），其它用户数据的 IPsec 隧道仍然是安全的。这个方法的缺点是由于用户数据的动态变化，如用户重新增加了一个 TCP 数据连接，IPsec 隧道的建立与删除过程比较频繁，引入较大的隧道建立时延。

进一步地，若该用户数据特征标识不能匹配集合中所有的数据特征标识项，则将该用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

需要说明的是，云服务器在对该用户数据进行服务处理之前，确认该用户数据是否需要进行服务处理，如果该用户数据需要进行服务处理，则执行步骤 S407 至步骤 S409;

如果该用户数据不需要进行服务处理，则执行步骤 S410 至 S411。

S407、该云服务器对该用户数据进行服务处理。

S408、云服务器将处理后的用户数据发送至网络回调设备。

示例地，若网络回调设备是通过在用户数据上添加数据标识将用户数据发送至云服务器时，网络回调设备接收该云服务器处理后的用户数据后，可以根据该数据标识区别出各个不同的用户数据。

若网络回调设备是通过在用户数据上添加隧道标识，使得网络回调设备将各个用户数据分别通过各自的隧道传输至云服务器时，网络回调设备通过各个用户数据的隧道接收云服务器处理后的用户数据。

上述网络回调设备和云服务器之间的隧道为该网络回调设备和云服务器之间的数据传输信道。

S409、网络回调设备将该处理后的用户数据发送出去。

S410、网络回调设备接收该云服务器发送的指示消息。

其中，该指示消息携带有不需要进行处理的用户数据的第二数据特征标识。

另外，由于目前的一些 IP 协议不支持这里所定义的命令指示，因此需要将使用的 IP 协议中添加或扩展一些标识位，如在 TCP 头中使用 Reserved 部分来扩展定义这个指示或使用扩展的 TCP 头选项来定义这个指示消息。

S411、网络回调设备根据该指示消息将后续接收到的携带有该第二数据特征标识的用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

本实施例提供的数据处理的方法，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需

要在云服务器中升级新的功能处理单元，就可以实现对与该云服务器相连的所有用户的服务控制功能的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种网络回调设备 500，如图 5 所示，包括：

第一获取单元 501，用于获取用户数据，并提取该用户数据的用户数据特征标识。

第一接收单元 502，用于接收 SPCF 发送的服务策略控制信息。

其中，服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息。

第一匹配单元 503，用于以该第一获取单元 501 提取的用户数据特征标识去匹配该第一接收单元 502 接收的服务策略控制信息中的数据特征标识项。

具体地，用户数据特征标识及服务策略控制信息中的数据特征标识项分别由以下 a 至 i 中的至少一个 IP 包特征标识和/或承载特征标识组成：

a、源 IP 地址或者源 IP 地址的区间或列表；

b、目标 IP 地址或者目标 IP 地址的区间或列表；

c、源端口号或者源端口号的区间或列表；

d、目的端口号或者目的端口号的区间或列表；

e、传输协议号或者传输协议号区间或列表；

f、IP 头字段中的 DSCP 或 TOS；

g、IPv6 头字段中的流标签；

h、若用户数据使用了 IPsec 保护，IPsec 报文中的 SPI；

i、对于 3GPP 网络，还可以根据承载的参数 QCI，ARP，承载的类型，GBR 速率区间，MBR 速率区间等参数及其组合。

网络回调设备提取该用户数据的用户数据特征标识就是从用户的 IP 数据包中提取出上述 a 至 i 中的 IP 包特征标识。一个最常用的数据

特征标识是 IP 五元组，即源 IP 地址，目标 IP 地址，源端口，目标端口，协议类型，分别对应上述的 a,b,c,d,e 这五个 IP 包特征标识。

用户数据特征标识匹配该集合中的数据特征标识项的过程是一个 DPI 过程中的匹配部分，它是一个简单的逻辑运算与判断过程。例如，网络回调设备提取到该用户数据的用户数据特征标识为：

{源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，源端口为 1234,目标端口为 80,协议类型为 TCP}；

而服务策略控制信息集合中的各个数据特征标识项有三个，并且分别是：

项 1={源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80}；

项 2={源 IP 地址 3.3.3.3，目标 IP 地址为 4.4.4.4，源端口为 4321，目标端口为 80,协议类型为 TCP }；

项 3={源 IP 地址 1.1.1.0 到 3.3.3.3 的所有 IP 地址，目标 IP 地址为 5.5.5.5，源端口为 1234,目标端口为 80,协议类型为 TCP }。

显然，用户数据特征标识中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2 及目标端口为 80 均与项 1 中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80 匹配。但用户数据特征标识中源端口为 1234 及协议类型为 TCP 在项 1 中未作限定，由于源端口及协议类型未作限定表示任意的源端口及协议类型的值都匹配，因此，用户数据的用户数据特征标识是匹配服务策略控制信息集合中的项 1 的。而用户数据特征标识中的源 IP 地址及目标 IP 地址与项 2 中的值不匹配，因此用户数据特征标识不匹配项 2。同样的，用户数据特征标识中的目标 IP 地址与项 3 中的目标 IP 地址值不匹配，因此用户数据特征标识不匹配项 3。

进一步地，该第一匹配单元 503，具体用于根据该服务策略控制信息中的数据特征标识项的优先级，按照高优先级至低优先级的顺序，以该用户数据特征标识分别去匹配该服务策略控制信息中的数据特征标识项。

第一发送单元 504，用于根据该第一匹配单元 503 匹配到的数据特征标识项对应的服务控制信息中包含的该处理服务器的地址信息将该

用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理。

第一用户数据接收单元 505，用于接收该处理服务器处理后的用户数据。

第一处理数据发送单元 506，用于将该第一用户数据接收单元 505 接收的处理后的用户数据发送出去。

进一步地，如图 6 所示，该网络回调设备 500 还包括：第一数据发送单元 507，用于若该用户数据特征标识不能匹配服务策略控制信息中所有的数据特征标识项，则将该用户数据发送出去。

更进一步地，第一发送单元 504，还用于根据该用户数据传输方式将该用户数据发送至该处理服务器。

该用户数据传输方式采用 IPsec 的加密与完整性保护的 ESP 隧道方式，该用户数据包括用户上行数据和/或用户下行数据。

示例地，该第一发送单元 504，具体用于为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据。

该第一接收单元 502，具体用于接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应。

示例地，该第一发送单元 504，具体用于为该不同用户设备的用户数据分配不同的第一隧道标识，通过与该不同的第一隧道标识对应的不同的隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据；

该第一接收单元 502，具体用于接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应。

优选地，如图 7 所示，该网络回调设备 500 还包括:

第一保存单元 508，用于保存该用户数据;

定时器 509，用于记录预设时间，并根据第一发送单元根据该服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器确定启动，且在到达或者超过该预设时间时停止。

第一定时数据发送单元 510，用于当该定时器 509 到达或者超过预设时间时，该网络回调设备如果没有接收到该处理服务器发送的处理后的该用户数据，将该第一保存单元 508 保存的用户数据发送出去。

这样，通过设置定时器，当该定时器到达或者超过预设时间时，该网络回调设备在没有接收到该处理服务器发送的处理后的用户数据的情况下，将该用户数据发送出去，能够保证该用户数据的正常传输，而不会因为处理服务器数据处理的时延造成系统通信数据传输的中断。

优选地，如图 8 所示，该网络回调设备 500 还包括：第一指示消息接收单元 511，用于在该处理服务器确认该用户数据不需要进行处理后，接收该处理服务器发送的指示消息。

其中，该指示消息携带有不需要进行处理的用户数据的第二数据特征标识。

第一用户数据发送单元 512，用于在第一指示消息接收单元 511 接收到该指示消息后，根据该指示消息将后续接收到的携带有该第二数据特征标识的用户数据发送出去。

这样，对于一些处理服务器确认不需要进行处理的用户数据，网路回调设备就不在将后续的该不需要进行处理的用户数据发送至云服务，而直接发送出去，节约了网络资源，减少了用户数据传输的时延，同时降低了处理服务器对用户数据处理的损耗，由于目前的一些 IP 协议不支持这里所定义的命令指示，因此需要将使用的 IP 协议中添加或扩展一些标识位，如在 TCP 头中使用 Reserved 部分来扩展定义这个指示或使用扩展的 TCP 头选项来定义这个指示消息。

需要说明的是，上述将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例

如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

采用上述实施例提供的网络回调设备，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的服务控制功能的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种服务策略控制设备 SPCF90，如图 9 所示，包括：

第二发送单元 91，用于向网络回调设备发送服务策略控制信息。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息，以使得该网络回调设备获取用户数据的用户数据特征标识，并以该用户数据特征标识分别去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理。

进一步地，如图 10 所示，该 SPCF90 还包括：

第二接收单元 92，用于接收 AF 发送的数据特征标识项。

例如，若 AF 是 IMS 中的 P-CSCF，则 AF 可以通过 IMS 中的标识识别出 UE 的 MSISDN 号码。另一个方法是 SPCF 从 AF 提供的用户 IP 地址（对于上行用户数据，则是源 IP 地址，对于下行用户数据，则是目标 IP 地址），然后 SPCF 通过查询 AF 对应的 PDN 连接的 PGW 或 GGSN 或 PCRF 就可以得到 UE 的 MSISDN 标识。

第二标识确定单元 93，用于根据第二接收单元 92 接收的该数据特征标识项确定对应的用户标识。

第二获取单元 94，用于根据该第二标识确定单元 93 确定的用户标识从 SPR 中获取与该用户标识对应的服务控制信息，并根据该用户标识确定该用户标识所对应的网络回调设备。

其中，SPCF 确定该用户标识所对应的网络回调设备的方法有很多种，例如，SPCF 可以根据运营商所配置的规则来定义网络回调设备类型，如网络回调设备是 PGW 或 GGSN，或 RAN 节点上的设备，如 RNC 或 eNB 或 BSC，或其它设备如 SGSN 或 SGW。若网络回调设备类型是 PGW 或 GGSN，则 SPCF 通过用户 IP 地址或 AF 对应的 PDN 连接就可确定网络回调设备类型 PGW 或 GGSN 的 IP 地址,这种对应关系通常是静态的，而且通常是配置在 SPCF 中的。若网络回调设备类型是 RNC 或 eNB 或 BSC，或其它设备如 SGSN 或 SGW，则 SPCF 首先确定 PGW 或 GGSN，然后通过查询 PGW 或 GGSN 得到 UE 当前所在的 RNC 或 eNB 或 BSC，或 SGSN 或 SGW 标识，并通过 DNS 或查询配置的方法得到这个回调设备类型的 IP 地址。另一个方法是 SPCF 通过查询事先确定的 PGW 或 GGSN 直接得到 UE 当前所在的 RNC 或 eNB 或 BSC，或 SGSN 或 SGW 的 IP 地址。若网络回调设备是 RNC 或 eNB 或 BSC，网络需要开启位置报告功能，这样当 UE 移动时，UE 当前所在的 RNC 或 eNB 或 BSC 才能报告其标识给 PGW 或 GGSN。还有一种方法是，PGW 或 GGSN 将 UE 当前所在的网络回调设备，如（RNC 或 eNB 或 BSC） 和/或（SGSN 或 SGW） 和/或 （PGW 或 GGSN）的标识上报给 AF，SPCF 直接从 AF 中得到此 UE 的网络回调设备标识（如 IP 地址）。

当然，若该 SPCF 根据自身配置的数据特征标识项，确定对所有的用户数据进行特定服务处理的处理服务器的地址信息，然后向网络中所有网络回调设备发送该服务策略控制信息，通常的，这是运营商根据当地（如法律或法规）的要求所采取的配置，如有些国家不允许其居民访问一些特定 IP 地址或特定域名的网站。

该第二发送单元 91，还用于向该用户标识所对应的网络回调设备发送包括该数据特征标识项与该用户标识对应的服务控制信息的服务策略控制信息。

更进一步地，如图 11 所示，该 SPCF90 还包括:

第二传输方式确定单元 95，用于根据该第二标识确定单元 93 确定的用户标识确定该用户数据的传输方式，将该用户数据的传输方式承载在该服务控制信息中，该用户数据的传输方式用于指示该网络回调设备通过该用户数据的传输方式将该用户数据发送给该处理服务器。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

采用上述实施例提供的 SPCF，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的服务控制功能的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种处理服务器 120，如图 12 所示，包括:

第三接收单元 1201，用于接收网络回调设备发送的用户数据.

功能处理单元 1202，用于对该第三接收单元 1201 接收的用户数据进行服务处理。

第三发送单元 1203，用于将该功能处理单元 1202 处理后的用户数

据发送至该网络回调设备。

进一步地，该功能处理单元 1202，还用于确认该用户数据不需要进行处理后，向所述网络回调设备发送指示消息，所述指示消息携带有不需要进行处理的用户数据的第二数据特征标识，所述指示消息用于指示所述网络回调设备将后续接收到的携带有所述第二数据特征标识的用户数据发送出去。

需要说明的是，该处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

采用上述实施例提供的处理服务器，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的服务控制功能的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种网络回调设备 130，如图 13 所示，包括:

第四获取单元 1301，用于获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识。

第四接收单元 1302，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息。

第四匹配单元 1303，用于以该第四获取单元 1301 提取的用户数据特征标识去匹配该第四接收单元 1302 接收的服务策略控制信息中的数据特征标识项。

具体地，用户数据特征标识及服务策略控制信息包含的数据特征

标识项分别由以下 a 至 i 中的至少一个 IP 包特征标识和/或承载特征标识组成:

a、源 IP 地址或者源 IP 地址的区间或列表;

b、目标 IP 地址或者目标 IP 地址的区间或列表;

c、源端口号或者源端口号的区间或列表;

d、目的端口号或者目的端口号的区间或列表;

e、传输协议号或者传输协议号区间或列表;

f、IP 头字段中的 DSCP（Differentiated Services Code Point，差分服务码点）或 TOS（Terms Of Service，服务类型）;

g、IPv6（Internet Protocol Version 6，第六代互联网协议）头字段中的流标签;

h、若用户数据使用了 IPsec（Internet Protocol Security，互联网协议安全）保护，IPsec 报文中的 SPI（Security parameter Index 安全参数索引）;

i、对于 3GPP（The 3rd Generation Partnership Project，第三代合作项目）网络，还可以根据承载的参数 QCI（QoS Class Identifier， QoS 类型标识），ARP(Allocation Retention Priority ，分配与保留优先级)，承载的类型，GBR（Guaranteed Bit Rate，保证比特速率）速率区间，MBR（Maximum Bit Rate，最大比特速率）速率区间等参数及其组合。

网络回调设备提取该用户数据的用户数据特征标识就是从用户的 IP 数据包中提取出上述 a 至 i 中的 IP 包特征标识。一个最常用的数据特征标识是 IP 五元组，即源 IP 地址，目标 IP 地址，源端口，目标端口，协议类型，分别对应上述的 a,b,c,d,e 这五个 IP 包特征标识。

用户数据特征标识匹配该服务策略控制信息中的数据特征标识项的过程是一个 DPI（Deep Packet Inspection 深度包检测）过程中的匹配部分，它是一个简单的逻辑运算与判断过程。例如，网络回调设备提取到该用户数据的用户数据特征标识为:

{源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，源端口为 1234,目标端口为 80,协议类型为 TCP};

而服务策略控制信息中的数据特征标识项有三个，并且分别是：

项 1={源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80}；

项 2={源 IP 地址 3.3.3.3，目标 IP 地址为 4.4.4.4，源端口为 4321，目标端口为 80,协议类型为 TCP }；

项 3={源 IP 地址 1.1.1.0 到 3.3.3.3 的所有 IP 地址，目标 IP 地址为 5.5.5.5，源端口为 1234,目标端口为 80,协议类型为 TCP }。

显然，用户数据特征标识中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2 及目标端口为 80 均与项 1 中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80 匹配。但用户数据特征标识中源端口为 1234 及协议类型为 TCP 在项 1 中未作限定，由于源端口及协议类型未作限定表示任意的源端口及协议类型的值都匹配，因此，用户数据的用户数据特征标识是匹配服务策略控制信息中的项 1 的。而用户数据特征标识中的源 IP 地址及目标 IP 地址与项 2 中的值不匹配，因此用户数据特征标识不匹配项 2。同样的，用户数据特征标识中的目标 IP 地址与项 3 中的目标 IP 地址值不匹配，因此用户数据特征标识不匹配项 3。

第四发送单元 1304，用于根据第四匹配单元 1303 匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理。

其中，上述服务控制信息中还包括：用户数据的传输方式，以便该网络回调设备还可以根据该用户数据传输方式将该用户数据发送至该处理服务器，上述的用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP（Encapsulating Security Payload，封装安全负载）隧道方式，本发明实施例并不局限于此。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体可以是，网络回调设备为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务

器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应，该方式是将所有的用户数据都在同一个传输隧道内传输，例如一个网络回调设备与一个处理服务器之间使用同一个 IPsec 隧道来传输不同的用户的 IP 数据包，并使用 GRE（Generic Routing Encapsulation，通用路由封装）来封装用户 IP 数据包，GRE 扩展头中的四字节的 Key 的不同值来区分不同的用户。使用同一个 IPsec 隧道可以使得多个用户共享一个共同的 IPsec 隧道及其安全保证，这个 IPsec 隧道不会随着用户数据数目的变化而变化，因此，具有很好的可扩展性，并且也大大地简化了安全过程。但是，当这个安全隧道被破解后，所有的用户的数据均可被攻击者看到。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体还可以是，网络回调设备为该不同用户设备的用户数据分配不同的第一隧道标识，通过与该不同的第一隧道标识对应的不同的隧道将该不同用户设备的用户数据发送至该处理服务器，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应，在该方式中，各个用户数据分别在各自的隧道内进行传输，例如，一个网络回调设备与一个处理服务器之间为不同的用户数据建立并使用不同的 IPsec 隧道来传输此 IP 数据包，这样的好处是，当一个用户数据所使用的 IPsec 隧道被破解后（例如，攻击可破解并得到隧道内传输的明文数据），其它用户数据的 IPsec 隧道仍然是安全的。这个方法的缺点是由于用户数据的动态变化，如用户重新增加了一个 TCP 数据连接，IPsec 隧道的建立与删除过程比较频繁，引入较大的隧道建立时延。

定时器 1305，用于记录预设时间，并根据所述第四发送单元根据该服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器确定启动，且在到达或者超过该预设时间时停止。

第四用户数据发送单元 1306，用于当该定时器 1305 到达或者超过

预设时间时，该网络回调设备如果没有接收到该处理服务器发送的处理后的该用户数据，将保存的该用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为终端 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

采用本实施例提供的网络回调设备，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种网络回调设备 140，如图 14 所示，包括：

第五获取单元 1401，用于获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识；

第五接收单元 1402，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息。

其中，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息。

进一步地，该用户数据包括用户上行数据和/或用户下行数据。

第五匹配单元 1403，用于以该第五获取单元 1401 提取的用户数据特征标识去匹配该第五接收单元 1402 接收的服务策略控制信息中的数据特征标识项。

具体地，用户数据特征标识及服务策略控制信息包含的数据特征标识项分别由以下 a 至 i 中的至少一个 IP 包特征标识和/或承载特征标识组成：

a、源 IP 地址或者源 IP 地址的区间或列表；

b、目标 IP 地址或者目标 IP 地址的区间或列表；

c、源端口号或者源端口号的区间或列表；

d、目的端口号或者目的端口号的区间或列表；

e、传输协议号或者传输协议号区间或列表；

f、IP 头字段中的 DSCP（Differentiated Services Code Point，差分服务码点）或 TOS（Terms Of Service，服务类型）；

g、IPv6（Internet Protocol Version 6，第六代互联网协议）头字段中的流标签；

h、若用户数据使用了 IPsec（Internet Protocol Security，互联网协议安全）保护，IPsec 报文中的 SPI（Security parameter Index 安全参数索引）；

i、对于 3GPP（The 3rd Generation Partnership Project，第三代合作项目）网络，还可以根据承载的参数 QCI（QoS Class Identifier， QoS 类型标识），ARP(Allocation Retention Priority ，分配与保留优先级)，承载的类型，GBR（Guaranteed Bit Rate，保证比特速率）速率区间，MBR（Maximum Bit Rate，最大比特速率）速率区间等参数及其组合。

网络回调设备提取该用户数据的用户数据特征标识就是从用户的 IP 数据包中提取出上述 a 至 i 中的 IP 包特征标识。一个最常用的数据特征标识是 IP 五元组，即源 IP 地址，目标 IP 地址，源端口，目标端口，协议类型，分别对应上述的 a,b,c,d,e 这五个 IP 包特征标识。

用户数据特征标识匹配该服务策略控制信息中的数据特征标识项

的过程是一个 DPI（Deep Packet Inspection 深度包检测）过程中的匹配部分，它是一个简单的逻辑运算与判断过程。例如，网络回调设备提取到该用户数据的用户数据特征标识为：

{源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，源端口为 1234,目标端口为 80,协议类型为 TCP}；

而服务策略控制信息中的数据特征标识项有三个，并且分别是：

项 1={源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80}；

项 2={源 IP 地址 3.3.3.3，目标 IP 地址为 4.4.4.4，源端口为 4321,目标端口为 80,协议类型为 TCP }；

项 3={源 IP 地址 1.1.1.0 到 3.3.3.3 的所有 IP 地址，目标 IP 地址为 5.5.5.5，源端口为 1234,目标端口为 80,协议类型为 TCP }。

显然，用户数据特征标识中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2 及目标端口为 80 均与项 1 中的源 IP 地址 1.1.1.1，目标 IP 地址为 2.2.2.2，目标端口为 80 匹配。但用户数据特征标识中源端口为 1234 及协议类型为 TCP 在项 1 中未作限定，由于源端口及协议类型未作限定表示任意的源端口及协议类型的值都匹配，因此，用户数据的用户数据特征标识是匹配服务策略控制信息中的项 1 的。而用户数据特征标识中的源 IP 地址及目标 IP 地址与项 2 中的值不匹配，因此用户数据特征标识不匹配项 2。同样的，用户数据特征标识中的目标 IP 地址与项 3 中的目标 IP 地址值不匹配，因此用户数据特征标识不匹配项 3。

第五发送单元 1404，用于根据该第五匹配单元 1403 匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器。

其中，上述服务控制信息中还包括：用户数据的传输方式，以便该网络回调设备还可以根据该用户数据传输方式将该用户数据发送至该处理服务器，上述的用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP（Encapsulating Security Payload，封装安全负载）隧道方式，本发明实施例并不局限于此。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体可以是，网络回调

设备为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应，该方式是将所有的用户数据都在同一个传输隧道内传输，例如一个网络回调设备与一个处理服务器之间使用同一个 IPsec 隧道来传输不同的用户的 IP 数据包，并使用 GRE（Generic Routing Encapsulation，通用路由封装）来封装用户 IP 数据包，GRE 扩展头中的四字节的 Key 的不同值来区分不同的用户。使用同一个 IPsec 隧道可以使得多个用户共享一个共同的 IPsec 隧道及其安全保证，这个 IPsec 隧道不会随着用户数据数目的变化而变化，因此，具有很好的可扩展性，并且也大大地简化了安全过程。但是，当这个安全隧道被破解后，所有的用户的数据均可被攻击者看到。

示例地，网络回调设备将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体还可以是，网络回调设备为该不同用户设备的用户数据分配不同的第一隧道标识，通过与该不同的第一隧道标识对应的不同的隧道将该不同用户设备的用户数据发送至该处理服务器，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应，在该方式中，各个用户数据分别在各自的隧道内进行传输，例如，一个网络回调设备与一个处理服务器之间为不同的用户数据建立并使用不同的 IPsec 隧道来传输此 IP 数据包，这样的好处是，当一个用户数据所使用的 IPsec 隧道被破解后（例如，攻击可破解并得到隧道内传输的明文数据），其它用户数据的 IPsec 隧道仍然是安全的。这个方法的缺点是由于用户数据的动态变化，如用户重新增加了一个 TCP 数据连接，IPsec 隧道的建立与删除过程比较频繁，引入较大的隧道建立时延。

第五指示消息接收单元 1405，用于在该处理服务器确认该用户数据不需要进行处理后，接收该处理服务器发送的指示消息，该指示消息携带有不需要进行处理的用户数据的第二数据特征标识；

第五用户数据发送单元 1406，用于根据该第五指示消息接收单元 1405 接收的指示消息将后续接收到的携带有该第二数据特征标识的用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为终端 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

采用本实施例提供的数据处理的网络回调设备，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

本发明实施例提供一种数据处理的系统，如图 15 所示，包括网络回调设备 150、SPCF151 和处理服务器 152，其中，

该网络回调设备 150，用于获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识，并接收服务策略控制设备

SPCF 发送的服务策略控制信息，该服务策略控制信息包含有数据特征标识项和与该数据特征标识项对应的服务控制信息，该服务控制信息中包含有对该用户数据进行服务处理的处理服务器的地址信息，以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，接收该处理服务器处理后的用户数据，并将该处理后的用户数据发送出去；

该 SPCF151，用于向网络回调设备发送服务策略控制信息；

该处理服务器 152，用于接收该网络回调设备发送的用户数据，对该用户数据进行服务处理，并将该处理后的用户数据发送至该网络回调设备。

进一步地，如图 16 所示，该系统还包括：AF153 和 SPR154，

该 AF153，用于向该 SPCF111 发送数据特征标识项。

该 SPR154，用于存储该用户签约的服务控制信息。

另外，若该 SPCF 根据自身配置的数据特征标识项，确定对所有的用户数据进行特定服务处理的处理服务器的地址信息及用户数据传输方式，然后向网络中所有网络回调设备发送该服务策略控制信息。通常的，这是运营商根据当地（如法律或法规）的要求所采取的配置，如有些国家不允许其居民访问一些特定 IP 地址或特定域名的网站。

进一步地，该网络回调设备 150，还用于根据该服务策略控制信息中的数据特征标识项的优先级，按照高优先级至低优先级的顺序，以该用户数据特征标识分别去匹配该服务策略控制信息中的数据特征标识项。

另外，该网络回调设备 150，还用于若该用户数据特征标识不能匹配服务策略控制信息中所有的数据特征标识项，则将该用户数据发送出去。

其中，上述的将该用户数据发送出去具体为：若该用户数据包括用户上行数据，将该用户上行数据发送至上行的网络节点，例如：若该网络回调设备为 eNB，则对应该网络回调设备的上行网络节点为 SGW。若该网络回调设备为 RNC，则对应该网络回调设备的上行网络

节点为 SGW 或 SGSN。

若该用户数据包括用户下行数据，将该用户下行数据发送至下行的网络节点，例如，若该网络回调设备为 eNB，则对应该网络回调设备的下行网络节点为 UE。若该网络回调设备为 RNC，则对应该网络回调设备的下行网络节点为 NodeB。

进一步地，述服务控制信息中还包括：用户数据的传输方式，以便该网络回调设备还可以根据该用户数据传输方式将该用户数据发送至该处理服务器，上述的用户数据传输方式可以是采用 IPsec 的加密与完整性保护的 ESP（Encapsulating Security Payload，封装安全负载）隧道方式，本发明实施例并不局限于此。

示例地，该网络回调设备 150，具体用于将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体可以是，网络回调设备为该不同用户设备的用户数据分配同一个第一隧道标识，通过与该第一隧道标识对应的同一条隧道将该不同用户设备的用户数据发送至该处理服务器，该用户数据包括不同用户设备的用户数据，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器通过同一条隧道发送的，该同一条隧道对应于该处理服务器为该不同用户设备的用户数据分配的同一个第二隧道标识，该第二隧道标识与该第一隧道标识相对应，该方式是将所有的用户数据都在同一个传输隧道内传输，例如一个网络回调设备与一个处理服务器之间使用同一个 IPsec 隧道来传输不同的用户的 IP 数据包，并使用 GRE（Generic Routing Encapsulation，通用路由封装）来封装用户 IP 数据包，GRE 扩展头中的四字节的 Key 的不同值来区分不同的用户。使用同一个 IPsec 隧道可以使得多个用户共享一个共同的 IPsec 隧道及其安全保证，这个 IPsec 隧道不会随着用户数据数目的变化而变化，因此，具有很好的可扩展性，并且也大大地简化了安全过程。但是，当这个安全隧道被破解后，所有的用户的数据均可被攻击者看到。

示例地，该网络回调设备 150，具体用于将该用户数据以服务控制信息中所确定的用户数据传输方式发送至该处理服务器的方法具体还可以是，网络回调设备为该不同用户设备的用户数据分配不同的第一隧道标识，通过与该不同的第一隧道标识对应的不同的隧道将该不同用户

设备的用户数据发送至该处理服务器，并接收该处理服务器处理后的用户数据，该处理后的用户数据为该处理服务器根据为该不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为该同一用户设备的用户数据的第一隧道标识对应，在该方式中，各个用户数据分别在各自的隧道内进行传输，例如，一个网络回调设备与一个处理服务器之间为不同的用户数据建立并使用不同的 IPsec 隧道来传输此 IP 数据包，这样的好处是，当一个用户数据所使用的 IPsec 隧道被破解后（例如，攻击可破解并得到隧道内传输的明文数据），其它用户数据的 IPsec 隧道仍然是安全的。这个方法的缺点是由于用户数据的动态变化，如用户重新增加了一个 TCP 数据连接，IPsec 隧道的建立与删除过程比较频繁，引入较大的隧道建立时延。

优选地，该网络回调设备 150，还用于保存该用户数据，并启动定时器，该定时器记录有预设时间。

当该定时器到达或者超过预设时间时，该网络回调设备如果没有接收到该处理服务器发送的处理后的该用户数据，将该用户数据发送出去，这样，能够保证该用户数据的正常传输，而不会因为处理服务器数据处理的时延造成系统通信数据传输的中断。

进一步地，该网络回调设备 150，还用于在该处理服务器确认该用户数据不需要进行处理后，接收该处理服务器发送的指示消息，该指示消息携带有不需要进行处理的用户数据的第二数据特征标识，根据该指示消息将后续接收到的携带有该第二数据特征标识的用户数据发送出去，这样，对于一些处理服务器确认不需要进行处理的用户数据，网络回调设备就不在将后续的不需要进行处理的用户数据发送至云服务，而直接发送出去，节约了网络资源，减少了用户数据传输的时延，同时降低了处理服务器对用户数据处理的损耗，由于目前的一些 IP 协议不支持这里所定义的命令指示，因此需要将使用的 IP 协议中添加或扩展一些标识位，如在 TCP 头中使用 Reserved 部分来扩展定义这个指示或使用扩展的 TCP 头选项来定义这个指示消息。

需要说明的是，上述实施例中描述的网络回调设备和 SPCF 在实际

的网络架构部署中，优选为设置在同一地理区域内的所有网络回调设备都与一个 SPCF 相连接，这样，不仅减少了部署网络架构的成本，而且网络系统的结构也得到简化，减少了网络架构部署的难度。

另外，由于不同的地理区域（如中国不同的省）连接不同的 SPCF，因此当用户从一个地理区域移动至另一个地理区域内时，如从省 A 移动到省 B，可以将不同地理区域连接的 SPCF 的参数配置为相同的参数或者在各个 SPCF 之间建立相互通信的信道以实现参数的同步，从而保证了不同的 SPCF 对用户采用相同的处理方式，也就是同一个处理服务器服务于很大的地理区域，即同时服务于省 A 与省 B。

同样地，上述实施例中描述的网络回调设备和处理服务器在实际的网络架构部署中，也优选为设置在同一地理区域内的所有网络回调设备都与一个处理服务器相连接，这样，不仅减少了部署网络架构的成本，而且网络系统的结构也得到简化，减少了网络架构部署的难度。

当然，由于不同的地理区域网络回调设备分别连接其对应区域的处理服务器，例如省 A 的网络回调设备与省 A 中的处理服务器相连，省 B 的网络回调设备与省 B 中的处理服务器相连。因此当用户从一个地理区域移动至另一个地理区域内时，如从省 A 移动到省 B，可以将不同地理区域内的处理服务器的参数配置为相同的参数或者在各个不同地理区域的处理服务器之间建立相互通信的通道以实现参数的同步，从而保证了不同地理区域的处理服务器对用户采用相同的服务控制处理。

需要说明的是，该系统可应用于多个场景中，具体地，该系统应用在无线通信网络的场景下，该网络回调设备可以是接入侧设备，如 eNB、RNC、BSC 和 AP（Access Point，访问接入点）中的至少一个，或者，可以是核心网设备，如 SGSN、GGSN、SGW、PGW、CSN（Connection Service Network,连接服务网）和移动 IP 本地代理中的至少一个，还可以是上述接入侧设备和核心网设备中的至少一个。

该系统应用在固网的场景下，该网络回调设备可以是 BRAS（Broadband Remote Access Server，宽带远程接入服务器）、路由器、防火墙、和 NAT（Network Address Translation，网络地址转换）服务

器中的至少一个。

该系统在无线通信网络与固网的融合网络的场景下，该网络回调设备为无线通信网络中的是 eNB、RNC、BSC、AP、SGSN、GGSN、SGW、PGW、CSN、移动 IP 本地代理中的至少一个和 BRAS、路由器、防火墙和网络地址转换 NAT 服务器中的至少一个。

优选地，若该网络回调设备为至少两个网络回调设备，则该至少两个网络回调设备与同一个 SPCF 相连，同样地，该至少两个网络回调设备也与同一个处理服务器相连，在实际应用中的具体的架构参考图 17、图 18、图 19、图 20 和图 21 所示，其中，图 17 至图 19 为无线通信网络场景下的网络架构，图 20 为固网场景下的网络架构，图 21 为无线通信网络与固网的融合网络场景下的网络架构，图 17 中接入侧设备作为网络回调设备，图 18 中核心网设备作为网络回调设备，图 19 中接入侧设备和核心网设备共同作为网络回调设备，图 20 中防火墙和 BRAS 作为网络回调设备，图 21 中接入侧设备、路由器和核心网设备作为网络回调设备，本发明实施例并不局限于此。

这样，多个不同的网络回调设备可以共同使用同一个处理服务器，使得对不同网络回调设备的服务控制处理集中在同一个处理服务器上，并且当更新处理服务器中的服务控制功能时，也只需要更新一个处理服务器中的功能控制单元就可以实现对所有网络回调设备服务控制功能的更新，从而非常方便的扩展了系统的服务控制功能。

进一步地，在同一网络场景中，不同的网络回调设备可以具有不同的服务控制功能。

另外，该 SPCF 可以是一独立设备，也可以将现有系统中的 PCRF 进行功能扩展，使其包含 SPCF 功能，还可以将现有系统中的 OAM（Operation Administration and Maintenance，操作管理维护服务器）进行功能扩展，使其包含 SPCF 功能。

需要说明的是，上述的处理服务器可优选为云服务器，由于云服务器使用了云计算技术，而云计算技术整合了计算、网络、存储等各种软件和硬件技术，因此能够提高服务器对用户数据处理的效率，并且保证用户数据的安全性和可靠性。

采用本实施例提供的数据处理的系统，对用户数据的处理不再受接入侧设备或者核心网设备的限制，从而实现了对用户数据进行开放式的智能处理，另外，当提供商需要增加一个新的服务控制功能时，只需要在处理服务器中升级新的功能处理单元，就可以实现对与该处理服务器相连的所有用户的升级，从而非常方便的扩展了系统的服务控制功能。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

权 利 要 求

1、一种数据处理的方法，其特征在于，所述方法包括:

网络回调设备获取用户数据传输通道上的用户数据，并提取所述用户数据的第一用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息;

所述网络回调设备以所述第一用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理;

所述网络回调设备接收所述处理服务器处理后的用户数据，并将所述处理后的用户数据发送出去。

2、根据权利要求 1 所述的方法，其特征在于，所述数据特征标识项包括下述项中的至少一个:

源 IP 地址或者源 IP 地址的区间或列表;

目标 IP 地址或者目标 IP 地址的区间或列表;

源端口号或者源端口号的区间或列表;

目的端口号或者目的端口号的区间或列表; 和

传输协议号或者传输协议号区间或列表中的至少一个。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述用户数据包括用户上行数据和/或用户下行数据。

4、根据权利要求 1 至 3 任一权利要求所述的方法，其特征在于，所述以所述第一用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，包括:

根据所述服务策略控制信息中的数据特征标识项的优先级，按照高优先级至低优先级的顺序，以所述第一用户数据特征标识分别去匹配所述服务策略控制信息中的数据特征标识项。

5、根据权利要求 1 至 4 任一权利要求中所述的方法，其特征在于，所述方法还包括:

18、根据权利要求 16 或 17 所述的设备，其特征在于，所述第一获取单元获取的所述用户数据包括用户上行数据和/或用户下行数据。

19、根据权利要求 16 所述的设备，其特征在于，所述第一匹配单元具体用于按如下方式以所述第一用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项：根据所述服务策略控制信息中的数据特征标识项的优先级，按照高优先级至低优先级的顺序，以所述第一用户数据特征标识分别去匹配所述服务策略控制信息中的数据特征标识项。

20、根据权利要求 16 或 17 所述的设备，其特征在于，所述设备还包括：

第一数据发送单元，用于若所述第一匹配单元以所述用户数据特征标识不能匹配服务策略控制信息中所有的数据特征标识项，则将所述用户数据发送出去。

21、根据权利要求 16 至 19 任一权利要求中所述的设备，其特征在于，所述第一发送单元具体用于按如下方式根据所述第一匹配单元匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器：根据所述第一匹配单元匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息，以及根据用户数据传输方式将所述用户数据发送至所述处理服务器，其中，所述服务控制信息还包括所述用户数据传输方式。

22、根据权利要求 21 所述的设备，其特征在于，所述用户数据包括不同用户设备的用户数据；

所述第一发送单元具体用于按如下方式根据用户数据传输方式将所述用户数据发送至所述处理服务器：为所述不同用户设备的用户数据分配同一个第一隧道标识，通过与所述第一隧道标识对应的同一条隧道将所述不同用户设备的用户数据发送至所述处理服务器；

所述第一接收单元接收的所述处理服务器处理后的用户数据，为所述处理服务器通过同一条隧道发送的，所述同一条隧道对应于所述处理服务器为所述不同用户设备的用户数据分配的同一个第二隧道标识，所述第二隧道标识与所述第一隧道标识相对应。

若所述第一用户数据特征标识不能匹配服务策略控制信息中所有的数据特征标识项，则将所述用户数据发送出去。

6、根据权利要求 1 至 5 任一权利要求中所述的方法，其特征在于，所述服务控制信息中还包括：用户数据传输方式；

所述根据匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述服务器，包括：

根据所述匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息，以及根据所述用户数据传输方式将所述用户数据发送至所述处理服务器。

7、根据权利要求 6 所述的方法，其特征在于，所述用户数据包括不同用户设备的用户数据，所述根据所述用户数据传输方式将所述用户数据发送至所述处理服务器，包括：

为所述不同用户设备的用户数据分配同一个第一隧道标识，通过与所述第一隧道标识对应的同一条隧道将所述不同用户设备的用户数据发送至所述处理服务器；

所述接收所述处理服务器处理后的用户数据，包括：

接收所述处理服务器处理后的用户数据，所述处理后的用户数据为所述处理服务器通过同一条隧道发送的，所述同一条隧道对应于所述处理服务器为所述不同用户设备的用户数据分配的同一个第二隧道标识，所述第二隧道标识与所述第一隧道标识相对应。

8、根据权利要求 6 所述的方法，其特征在于，所述用户数据包括不同用户设备的用户数据，所述根据用户数据传输方式将所述用户数据发送至所述处理服务器，包括：

为所述不同用户设备的用户数据分配不同的第一隧道标识，通过与所述不同的第一隧道标识对应的不同的隧道将所述不同用户设备的用户数据发送至所述处理服务器；

所述接收所述处理服务器处理后的用户数据，包括：

接收所述处理服务器处理后的用户数据，所述处理后的用户数据为所述处理服务器根据为所述不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为所述同一用户设备的用户数据的第一隧道标识

对应。

9、根据权利要求 7 或 8 所述的方法，其特征在于，所述根据所述匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器之前，还包括：

保存所述用户数据，并启动定时器，所述定时器记录有预设时间；

当所述定时器到达或者超过预设时间时，所述网络回调设备如果没有接收到所述处理服务器发送的处理后的所述用户数据，将所述用户数据发送出去。

10、根据权利要求 7 或 8 所述的方法，其特征在于，还包括：

接收所述处理服务器发送的指示消息，所述指示消息携带有不需要进行处理的用户数据的第二用户数据特征标识，根据所述指示消息将后续接收到的携带有所述第二用户数据特征标识的用户数据发送出去。

11、一种数据处理的方法，其特征在于，包括：

服务策略控制设备 SPCF 向网络回调设备发送服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息，以使得所述网络回调设备获取用户数据的用户数据特征标识，并以所述用户数据特征标识分别去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理。

12、根据权利要求 11 所述的方法，其特征在于，所述在所述 SPCF 向网络回调设备发送服务策略控制信息之前，还包括：

接收应用功能 AF 服务器发送的数据特征标识项；

确定所述数据特征标识项所对应的用户标识；

根据所述用户标识从签约信息服务器 SPR 中获取与所述用户标识对应的服务控制信息，并根据所述用户标识确定所述用户标识所对应的网络回调设备；

所述 SPCF 向网络回调设备发送服务策略控制信息，包括：

所述 SPCF 向所述用户标识所对应的网络回调设备发送所述服务策略控制信息，所述服务策略控制信息包括所述数据特征标识项与所述用户标识对应的服务控制信息的服务策略控制信息。

13、根据权利要求 12 所述的方法，其特征在于，所述方法还包括：

SPCF 根据所述用户标识确定所述用户数据传输方式，将所述用户数据传输方式承载在所述服务控制信息中，所述用户数据传输方式用于指示所述网络回调设备通过所述用户数据传输方式将所述用户数据发送给所述处理服务器。

14、一种数据处理的方法，其特征在于，包括：

网络回调设备获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

所述网络回调设备以所述用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理；

当设置的定时器到达或者超过预设时间时，所述网络回调设备如果没有接收到所述处理服务器发送的处理后的所述用户数据，将保存的所述用户数据发送出去。

15、一种数据处理的方法，其特征在于，包括：

网络回调设备获取用户数据传输通道上的用户数据，并提取所述用户数据的第一用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

所述网络回调设备以所述第一用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数

据发送至所述处理服务器；

所述网络回调设备接收所述处理服务器发送的指示消息，所述指示消息携带有不需要进行处理的用户数据的第二用户数据特征标识，根据所述指示消息将后续接收到的携带有所述第二用户数据特征标识的用户数据发送出去。

16、一种网络回调设备，其特征在于，包括：

第一获取单元，用于获取用户数据，并提取所述用户数据的第一用户数据特征标识；

第一接收单元，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

第一匹配单元，用于以所述第一获取单元提取的第一用户数据特征标识去匹配所述第一接收单元接收的服务策略控制信息中的数据特征标识项；

第一发送单元，用于根据所述第一匹配单元匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理；

第一用户数据接收单元，用于接收所述处理服务器处理后的用户数据；

第一处理数据发送单元，用于将所述第一用户数据接收单元接收的处理后的用户数据发送出去。

17、根据权利要求 16 所述的设备，其特征在于，所述第一接收单元接收的所述服务策略控制信息中包含的所述数据特征标识项包括下述项中的至少一个：

源 IP 地址或者源 IP 地址的区间或列表；

目标 IP 地址或者目标 IP 地址的区间或列表；

源端口号或者源端口号的区间或列表；

目的端口号或者目的端口号的区间或列表；和

传输协议号或者传输协议号区间或列表中的至少一个。

23、根据权利要求 21 所述的设备，其特征在于，所述用户数据包括不同用户设备的用户数据，所述第一发送单元具体用于按如下方式根据用户数据传输方式将所述用户数据发送至所述处理服务器：为所述不同用户设备的用户数据分配不同的第一隧道标识，通过与所述不同的第一隧道标识对应的不同的隧道将所述不同用户设备的用户数据发送至所述处理服务器；

所述第一接收单元接收的所述处理服务器处理后的用户数据，为所述处理服务器根据为所述不同用户设备的用户数据分配的不同的第二隧道标识确定的不同隧道发送的，为同一用户设备的用户数据分配的第二隧道标识与为所述同一用户设备的用户数据的第一隧道标识对应。

24、根据权利要求 22 或 23 所述的设备，其特征在于，还包括：

第一保存单元，用于保存所述用户数据；

定时器，用于记录预设时间，并根据所述第一发送单元将所述用户数据发送至所述处理服务器确定启动，且在到达或者超过所述预设时间时停止；

第一定时数据发送单元，用于当所述定时器到达或者超过预设时间时，如果所述第一用户数据接收单元没有接收到所述处理服务器发送的处理后的所述用户数据，将所述第一保存单元保存的用户数据发送出去。

25、根据权利要求 22 或 23 所述的设备，其特征在于，还包括：

第一指示消息接收单元，用于接收所述处理服务器发送的指示消息，所述指示消息携带有不需要进行处理的用户数据的第二用户数据特征标识；

第一用户数据发送单元，用于在第一指示消息接收单元接收到所述指示消息后，根据所述指示消息将后续接收到的携带有所述第二用户数据特征标识的用户数据发送出去。

26、一种服务策略控制设备 SPCF，其特征在于，包括：

第二发送单元，用于向网络回调设备发送服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进

行服务处理的处理服务器的地址信息，以使得所述网络回调设备获取用户数据的用户数据特征标识，并以所述用户数据特征标识分别去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理。

27、根据权利要求 26 所述的 SPCF，其特征在于，还包括：第二接收单元，用于接收应用功能 AF 服务器发送的数据特征标识项；

第二标识确定单元，用于确定所述数据特征标识项所对应的用户标识；

第二获取单元，用于根据所述第二标识确定单元确定的用户标识从签约信息服务器 SPR 中获取与所述用户标识对应的服务控制信息，并根据所述用户标识确定所述用户标识所对应的网络回调设备；

所述第二发送单元，还用于向所述用户标识所对应的网络回调设备发送包括所述数据特征标识项与所述用户标识对应的服务控制信息的服务策略控制信息。

28、根据权利要求 27 所述的 SPCF，其特征在于，还包括：

第二传输方式确定单元，用于根据所述第二标识确定单元确定的用户标识确定所述用户数据的传输方式，将所述用户数据的传输方式承载在所述服务控制信息中，所述用户数据的传输方式用于指示所述网络回调设备通过所述用户数据的传输方式将所述用户数据发送给所述处理服务器。

29、一种处理服务器，其特征在于，包括：

第三接收单元，用于接收网络回调设备发送的用户数据；

功能处理单元，用于对所述第三接收单元接收的用户数据进行服务处理；

第三发送单元，用于将所述功能处理单元处理后的用户数据发送至所述网络回调设备。

30、根据权利要求 29 所述的设备，其特征在于，所述功能处理单元，还用于确认所述用户数据不需要进行处理后，向所述网络回调设备发送指示消息，所述指示消息携带有不需要进行处理的用户数据的

用户数据特征标识，所述指示消息用于指示所述网络回调设备将后续接收到的携带有所述用户数据特征标识的用户数据发送出去。

31、一种网络回调设备，其特征在于，包括：

第四获取单元，用于获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识；

第四接收单元，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

第四匹配单元，用于以所述第四获取单元提取的用户数据特征标识去匹配所述第四接收单元接收的服务策略控制信息中的数据特征标识项；

第四发送单元，用于根据所述第四匹配单元匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息，将所述用户数据发送至所述处理服务器，以使得所述处理服务器对所述用户数据进行服务处理；

定时器，用于记录预设时间，并根据所述第四发送单元将所述用户数据发送至所述处理服务器确定启动，且在到达或者超过所述预设时间时停止；

第四用户数据发送单元，用于当所述定时器到达或者超过预设时间时，如果所述第四接收单元没有接收到所述处理服务器发送的处理后的所述用户数据，将所述用户数据发送出去。

32、一种网络回调设备，其特征在于，包括：

第五获取单元，用于获取用户数据传输通道上的用户数据，并提取所述用户数据的第一用户数据特征标识；

第五接收单元，用于接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息；

第五匹配单元，用于以所述第五获取单元提取的用户数据特征标识去匹配所述第五接收单元接收的服务策略控制信息中的数据特征标

识项；

第五发送单元，用于根据所述第五匹配单元匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息，将所述用户数据发送至所述处理服务器；

第五指示消息接收单元，用于接收所述处理服务器发送的指示消息，所述指示消息携带有不需要进行处理的用户数据的第二用户数据特征标识；

第五用户数据发送单元，用于根据所述指示消息将后续接收到的携带有所述第二用户数据特征标识的用户数据发送出去。

33、一种数据处理的系统，其特征在于，包括：网络回调设备、服务策略控制设备 SPCF、以及处理服务器，

所述网络回调设备，用于获取用户数据传输通道上的用户数据，并提取所述用户数据的用户数据特征标识，并接收服务策略控制设备 SPCF 发送的服务策略控制信息，所述服务策略控制信息包含有数据特征标识项和与所述数据特征标识项对应的服务控制信息，所述服务控制信息中包含有对所述用户数据进行服务处理的处理服务器的地址信息，以所述用户数据特征标识去匹配所述服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的所述处理服务器的地址信息将所述用户数据发送至所述处理服务器，接收所述处理服务器处理后的用户数据，并将所述处理后的用户数据发送出去；

所述 SPCF，用于向网络回调设备发送服务策略控制信息；

所述处理服务器，用于接收所述网络回调设备发送的用户数据，对所述用户数据进行服务处理，并将所述处理后的用户数据发送至所述网络回调设备。

34、根据权利要求 33 所述的系统，其特征在于，还包括：应用功能服务器 AF 和签约信息服务器 SPR，

所述 AF，用于向所述 SPCF 发送数据特征标识项；

所述 SPR，用于存储所述用户签约的服务控制信息。

35、根据权利要求 33 或 34 所述的系统，其特征在于，所述 SPCF 是策略与计费控制服务器 PCRF 或操作管理维护服务器 OAM。

36、根据权利要求 33 至 35 所述的系统，其特征在于，所述系统包括至少两个所述网络回调设备，所述至少两个所述网络回调设备与同一个所述 SPCF 相连。

37、根据权利要求 33 至 35 任一权利要求中所述的系统，其特征在于，所述系统包括至少两个所述网络回调设备，至少两个所述网络回调设备与同一个所述处理服务器相连。

38、根据权利要求 33 至 37 任一权利要求中所述的系统，其特征在于，所述系统应用在无线通信网络的场景下，所述网络回调设备是演进型基站 eNB 或无线网络控制器 RNC、基站控制器 BSC、访问接入点 AP、服务支持节点 SGSN、GPRS 网关支持节点 GGSN、服务网关 SGW、分组数据网网关 PGW、连接服务网 CSN 和移动 IP 本地代理中的至少一个。

39、根据权利要求 33 至 37 任一权利要求中所述的系统，其特征在于，所述系统应用在固网的场景下，所述网络回调设备是宽带远程接入服务器 BRAS、路由器、防火墙和网络地址转换 NAT 服务器中的至少一个。

40、根据权利要求 33 至 37 任一权利要求中所述的系统，其特征在于，所述系统应用在无线通信网络与固网的融合网络的场景下，所述网络回调设备是 eNB、RNC、BSC、AP、SGSN、GGSN、SGW、PGW、CSN、移动 IP 本地代理中的至少一个和 BRAS、路由器、防火墙和网络地址转换 NAT 服务器中的至少一个。

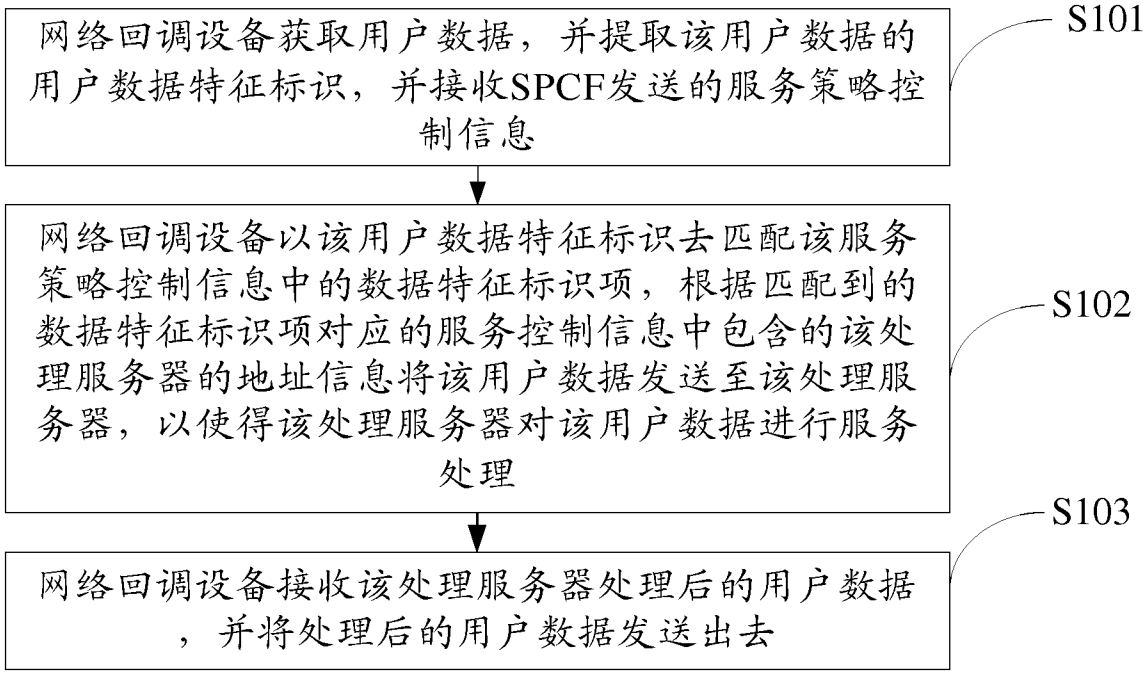
网络回调设备获取用户数据，并提取该用户数据的用户数据特征标识，并接收SPCF发送的服务策略控制信息
S101
网络回调设备以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据特征标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理
S102
网络回调设备接收该处理服务器处理后的用户数据，并将处理后的用户数据发送出去
S103

图 1

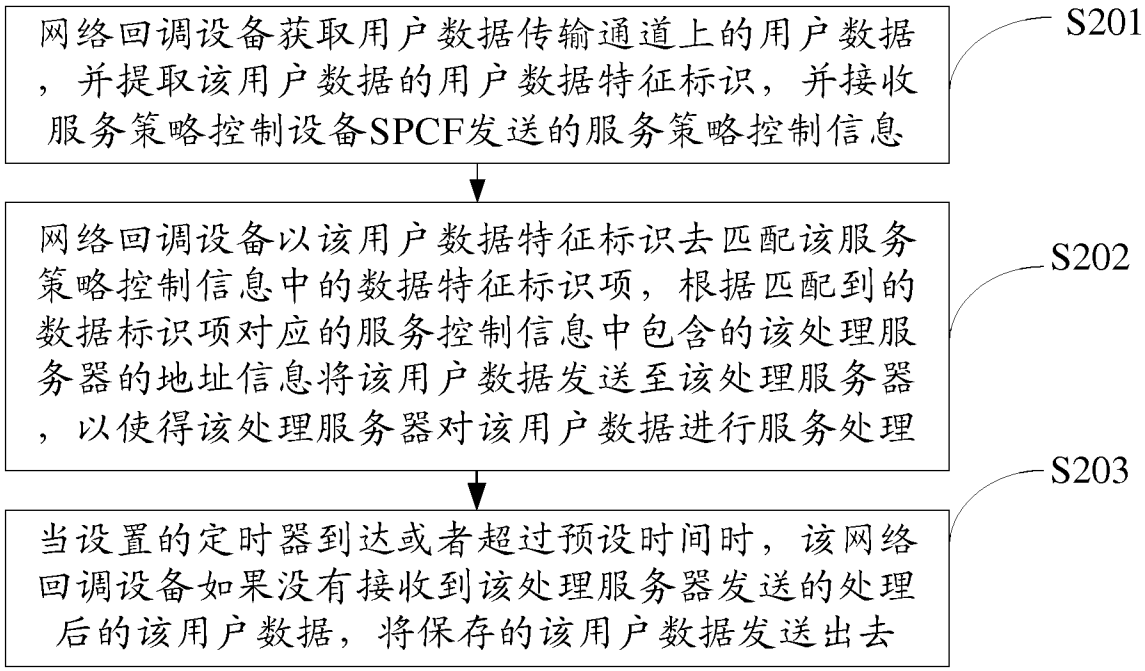
网络回调设备获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识，并接收服务策略控制设备SPCF发送的服务策略控制信息
S201
网络回调设备以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器，以使得该处理服务器对该用户数据进行服务处理
S202
当设置的定时器到达或者超过预设时间时，该网络回调设备如果没有接收到该处理服务器发送的处理后的该用户数据，将保存的该用户数据发送出去
S203

图 2

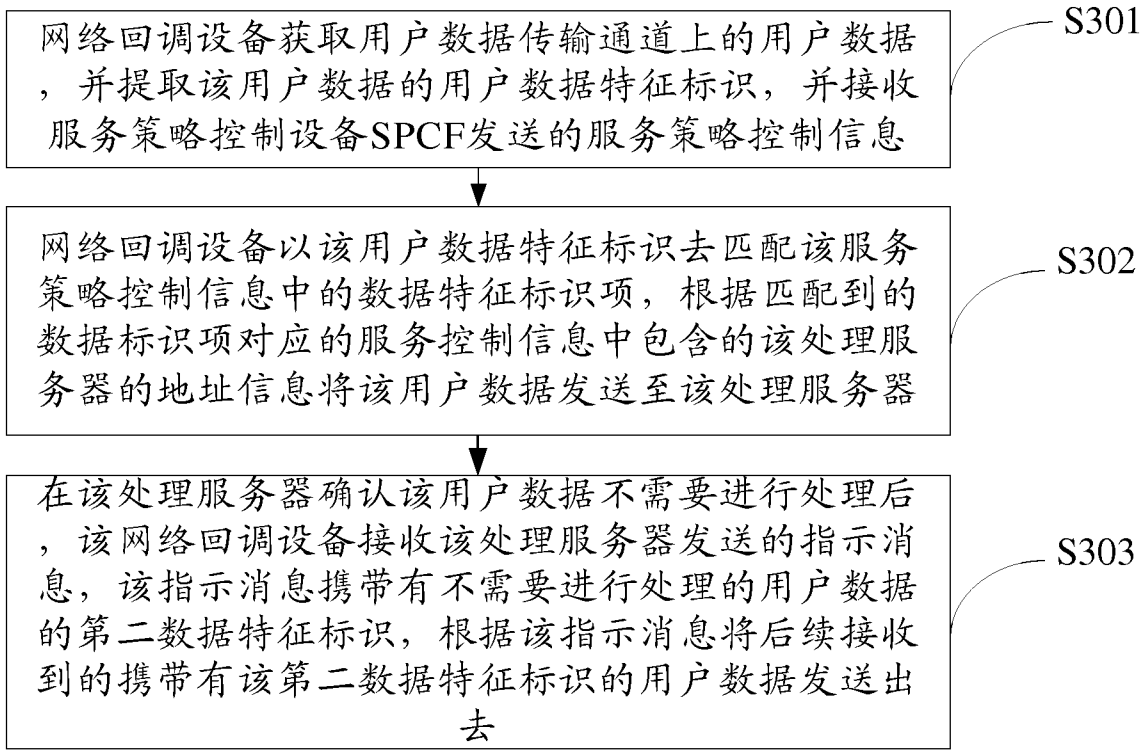
网络回调设备获取用户数据传输通道上的用户数据，并提取该用户数据的用户数据特征标识，并接收服务策略控制设备SPCF发送的服务策略控制信息
S301
网络回调设备以该用户数据特征标识去匹配该服务策略控制信息中的数据特征标识项，根据匹配到的数据标识项对应的服务控制信息中包含的该处理服务器的地址信息将该用户数据发送至该处理服务器
S302
在该处理服务器确认该用户数据不需要进行处理后，该网络回调设备接收该处理服务器发送的指示消息，该指示消息携带有不需要进行处理的用户数据的第二数据特征标识，根据该指示消息将后续接收到的携带有该第二数据特征标识的用户数据发送出去
S303

图 3

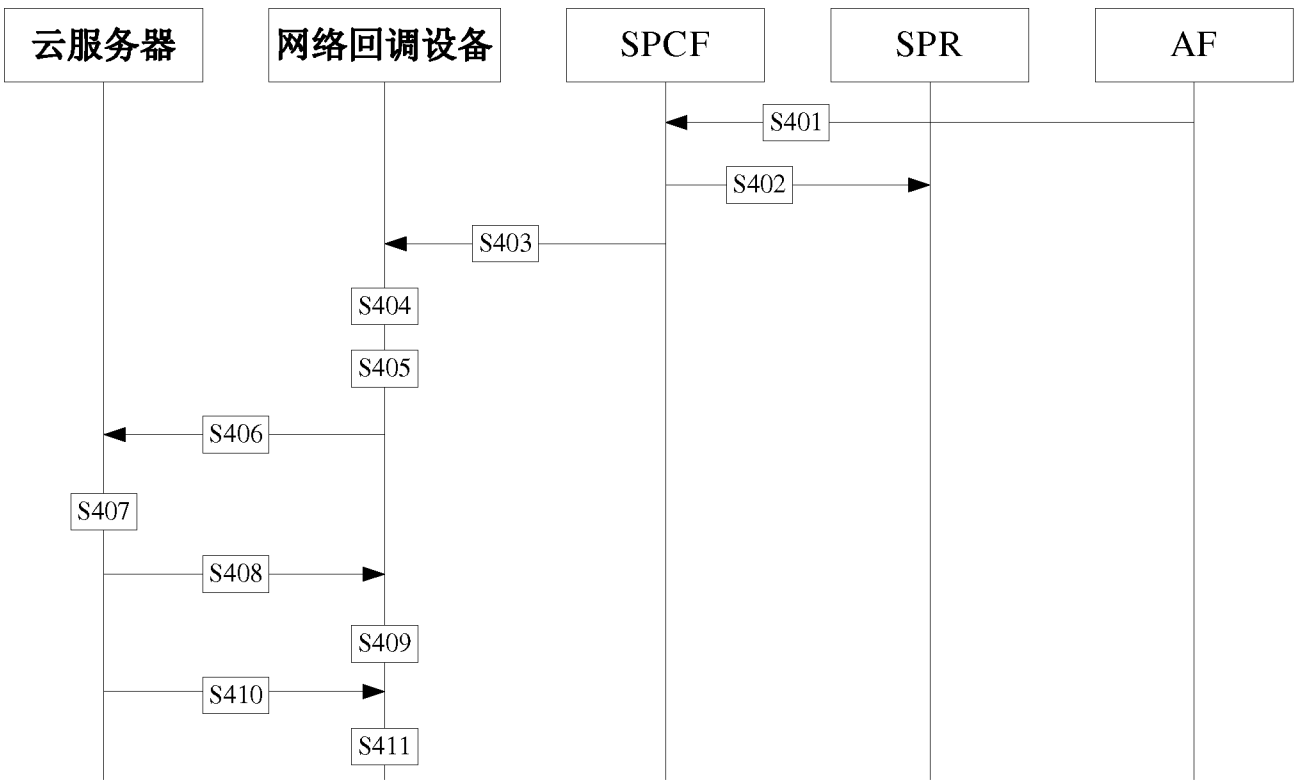
云服务器
网络回调设备
SPCF
SPR
AF
S401
S402
S403
S404
S405
S406
S407
S408
S409
S410
S411

图 4

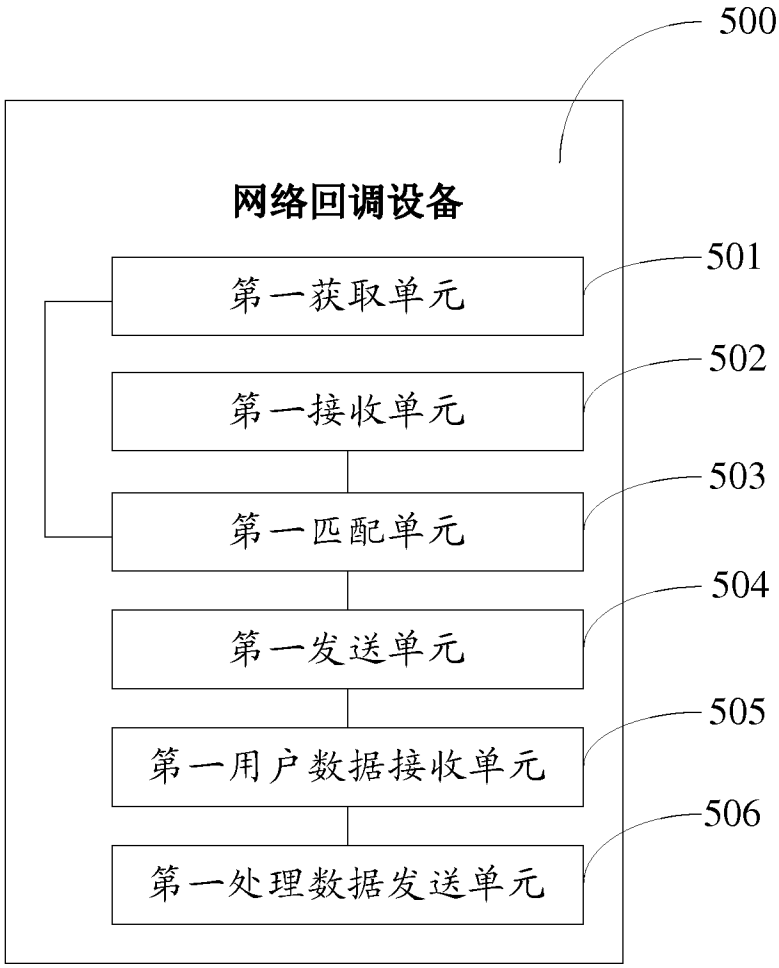
500
网络回调设备
501
第一获取单元
502
第一接收单元
503
第一匹配单元
504
第一发送单元
505
第一用户数据接收单元
506
第一处理数据发送单元

图 5

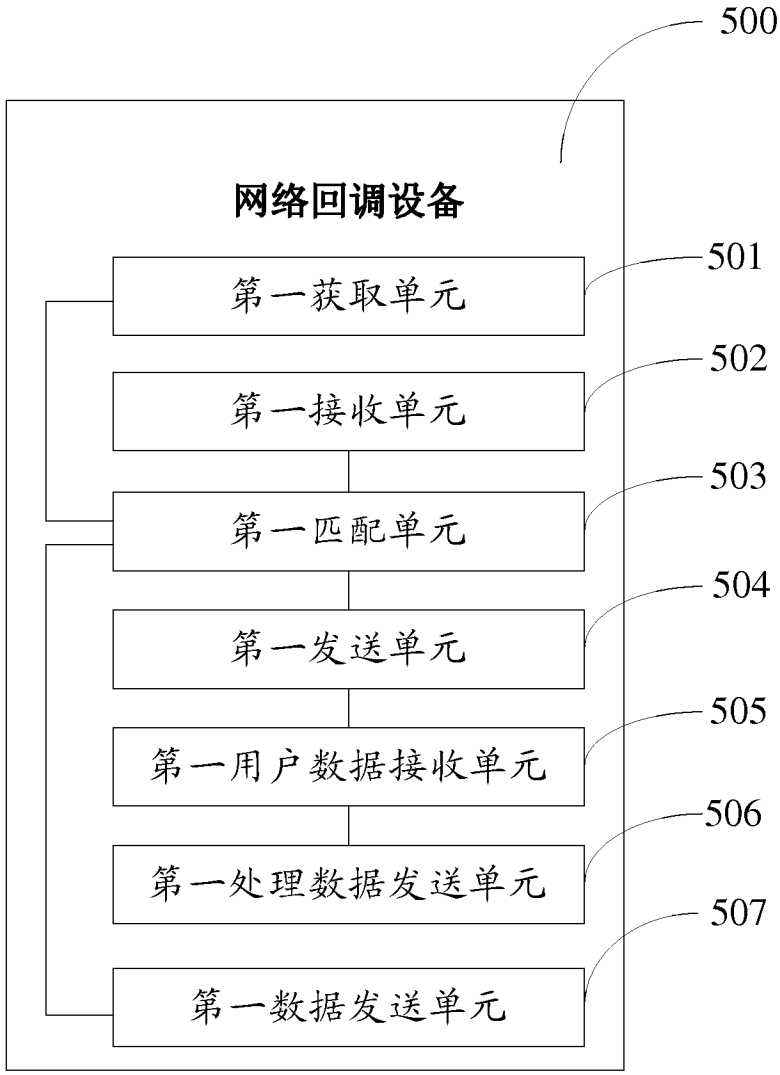
500
网络回调设备
501
第一获取单元
502
第一接收单元
503
第一匹配单元
504
第一发送单元
505
第一用户数据接收单元
506
第一处理数据发送单元
507
第一数据发送单元

图 6

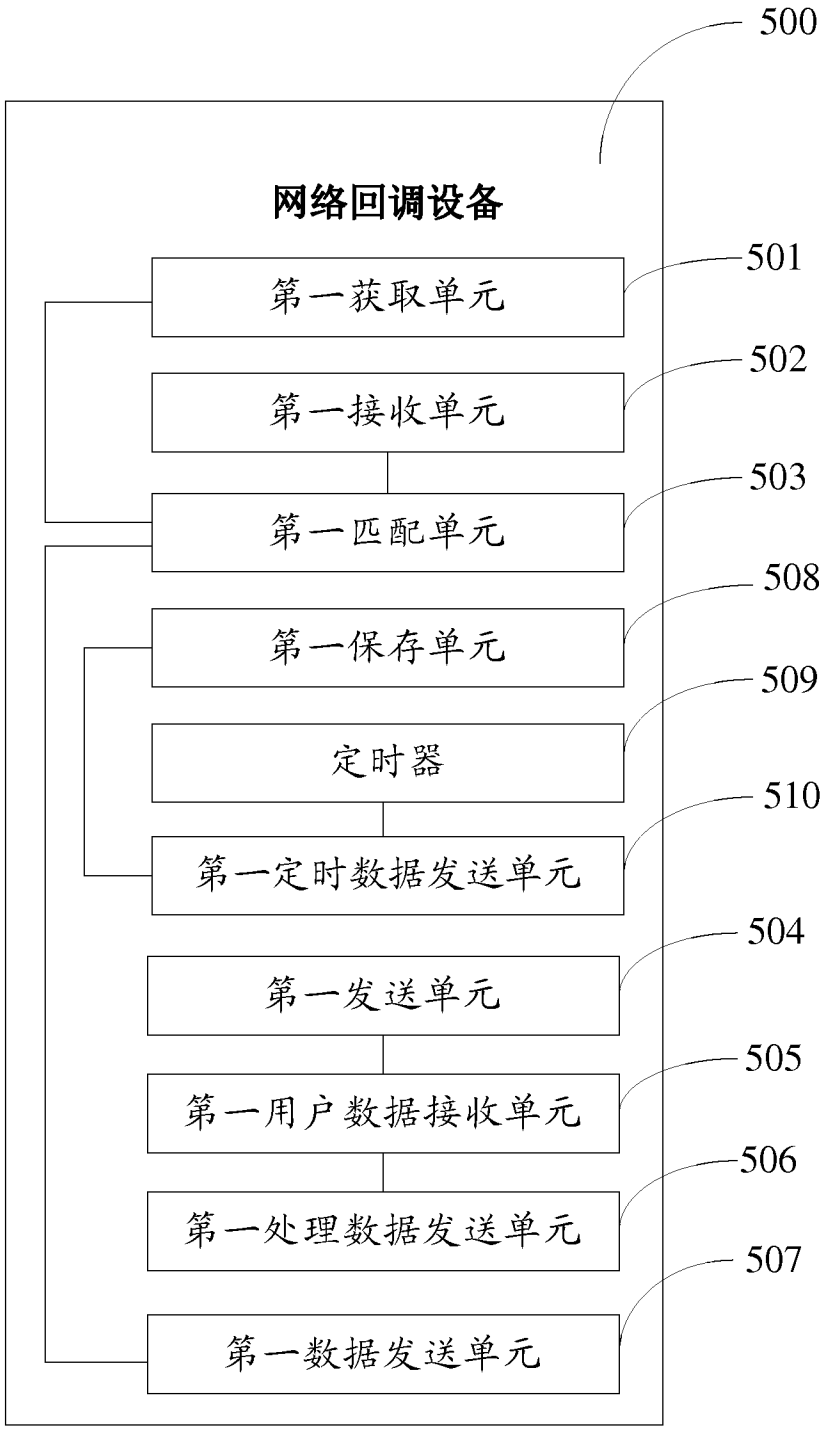
500
网络回调设备
501
第一获取单元
502
第一接收单元
503
第一匹配单元
508
第一保存单元
509
定时器
510
第一定时数据发送单元
504
第一发送单元
505
第一用户数据接收单元
506
第一处理数据发送单元
507
第一数据发送单元

图 7

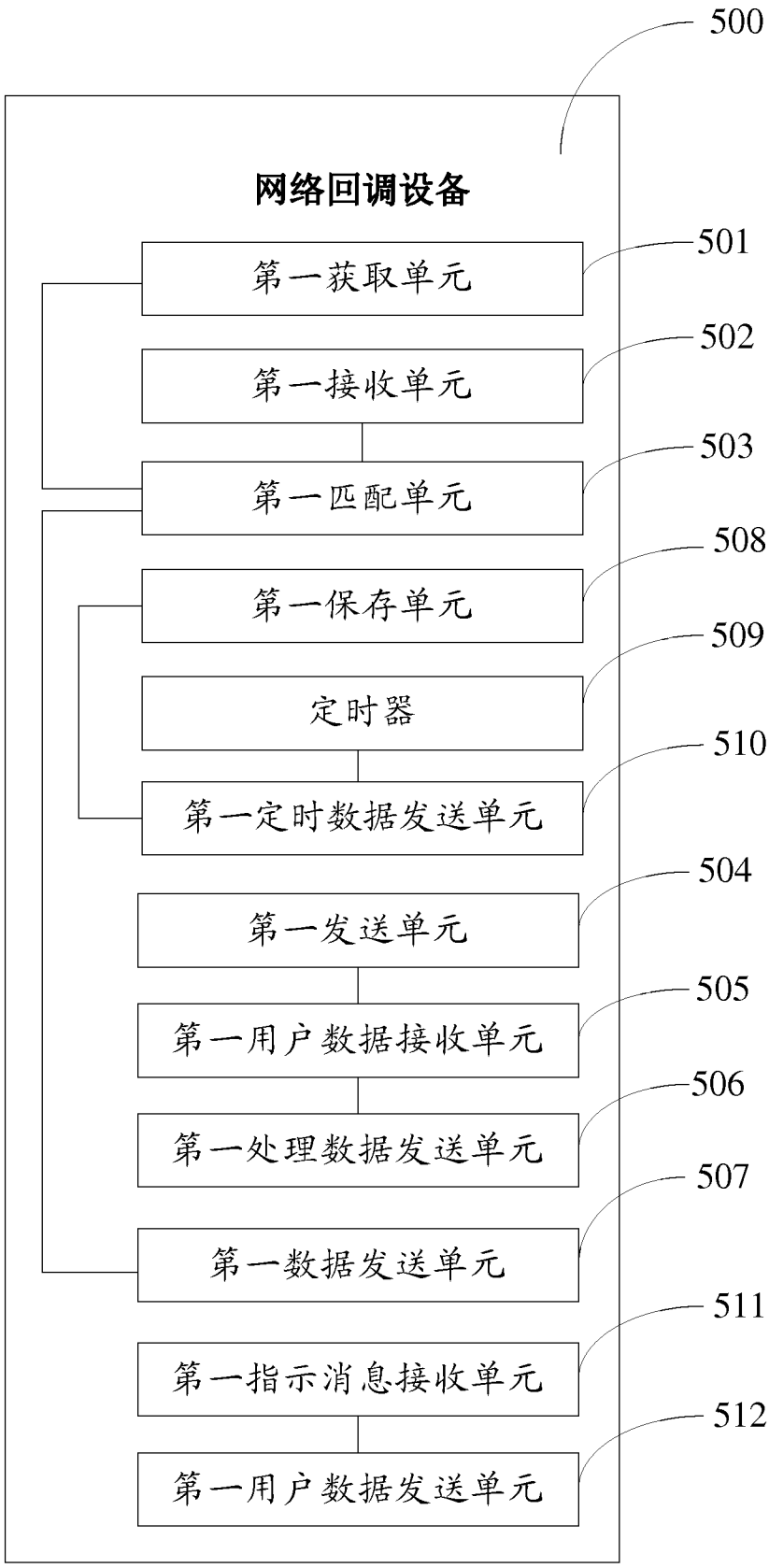
500
网络回调设备
501
第一获取单元
502
第一接收单元
503
第一匹配单元
508
第一保存单元
509
定时器
510
第一定时数据发送单元
504
第一发送单元
505
第一用户数据接收单元
506
第一处理数据发送单元
507
第一数据发送单元
511
第一指示消息接收单元
512
第一用户数据发送单元

图 8

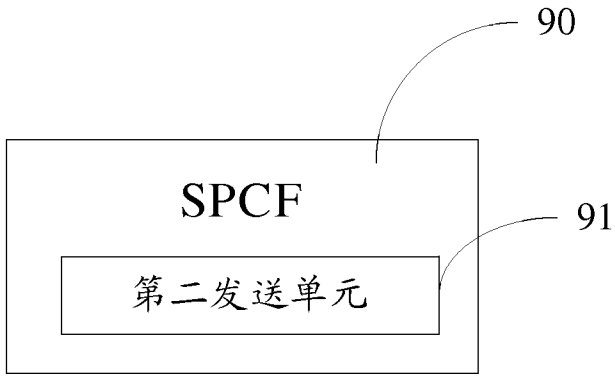
90
SPCF
91
第二发送单元

图 9

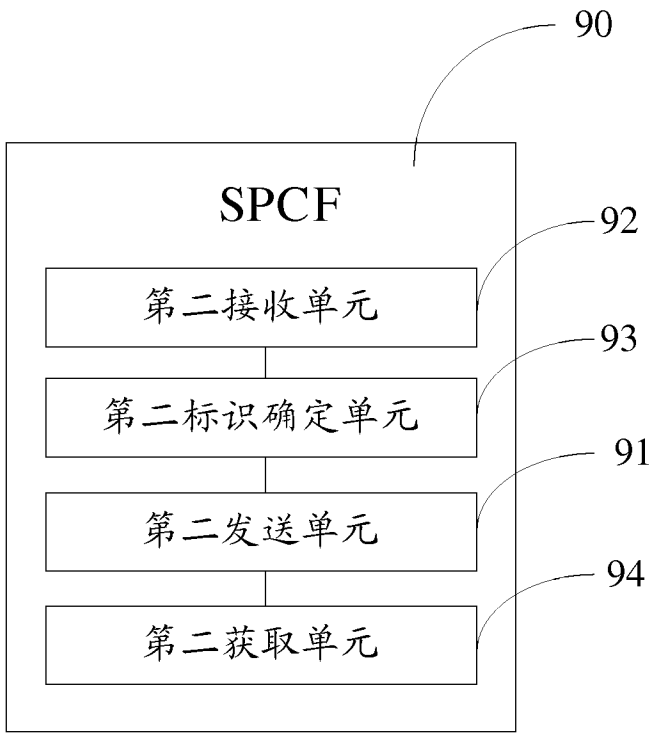
90
SPCF
92
第二接收单元
93
第二标识确定单元
91
第二发送单元
94
第二获取单元

图 10

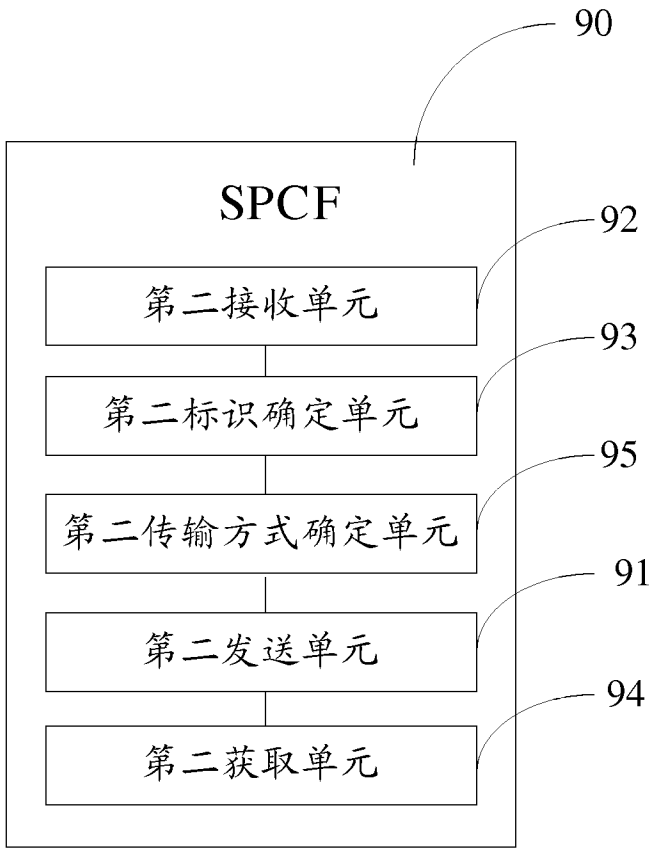
90
SPCF
92
第二接收单元
93
第二标识确定单元
95
第二传输方式确定单元
91
第二发送单元
94
第二获取单元

图 11

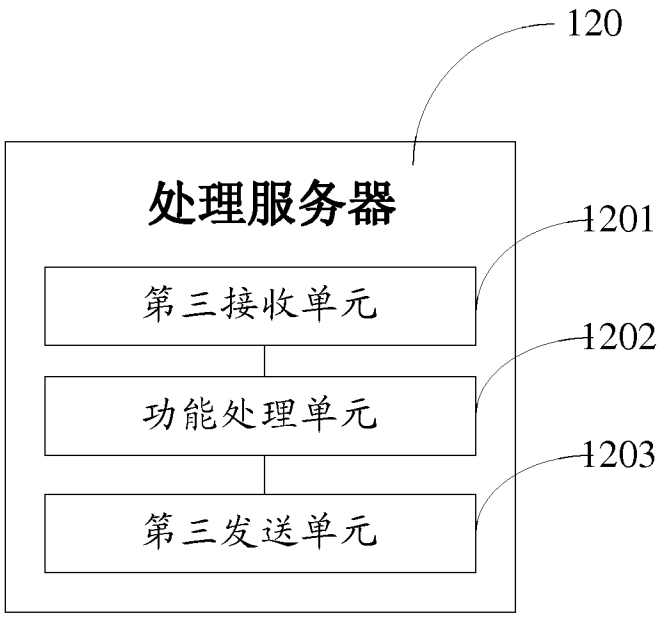
120
处理服务器
1201
第三接收单元
1202
功能处理单元
1203
第三发送单元

图 12

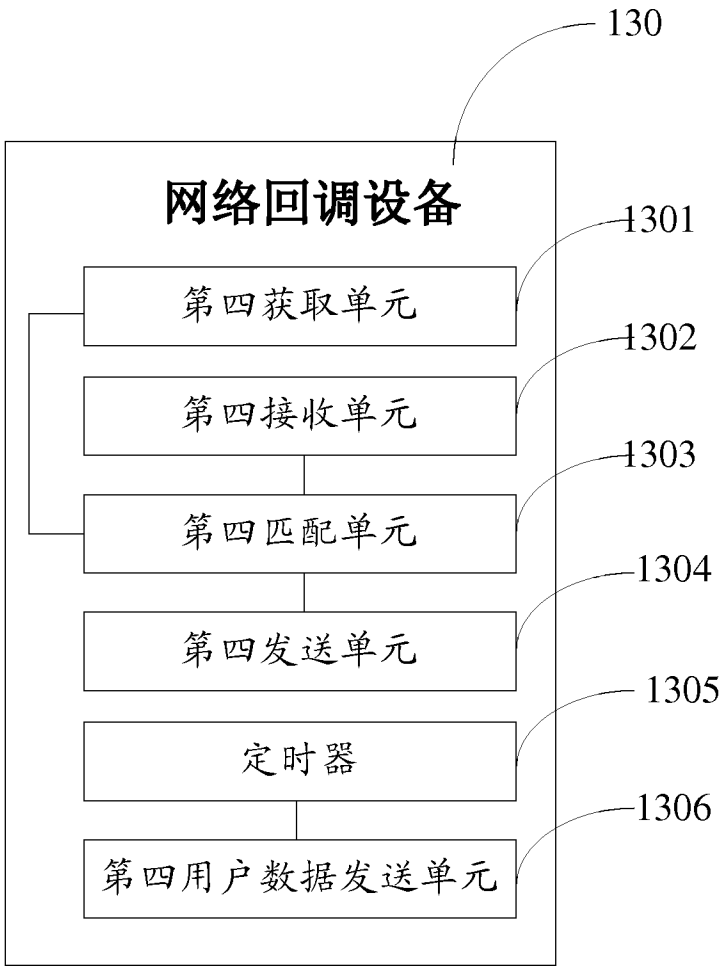
130
网络回调设备
1301
第四获取单元
1302
第四接收单元
1303
第四匹配单元
1304
第四发送单元
1305
定时器
1306
第四用户数据发送单元

图 13

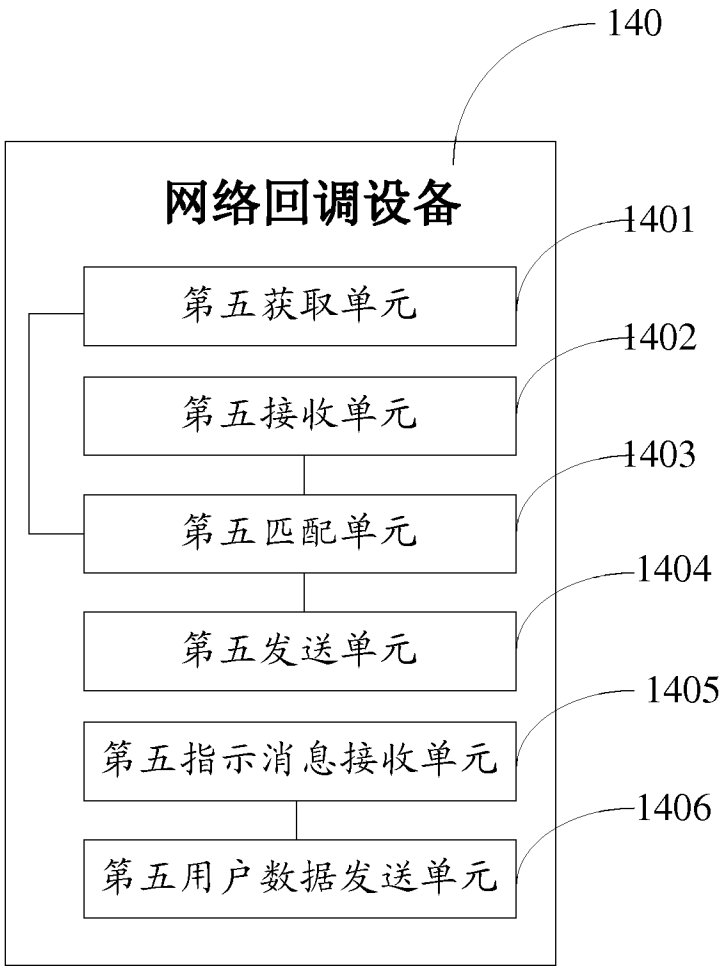
140
网络回调设备
1401
第五获取单元
1402
第五接收单元
1403
第五匹配单元
1404
第五发送单元
1405
第五指示消息接收单元
1406
第五用户数据发送单元

图 14

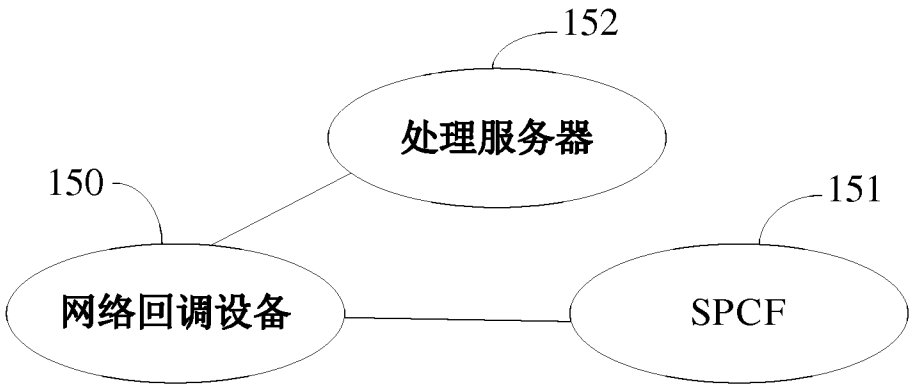
152
处理服务器
150
151
网络回调设备
SPCF

图 15

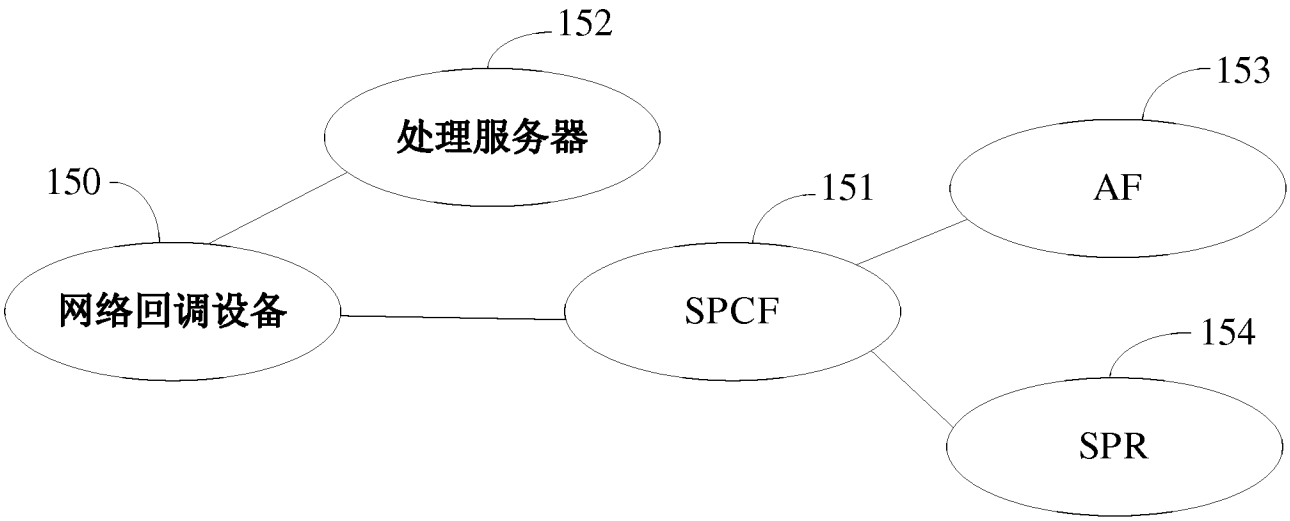
152
处理服务器
153
AF
150
151
网络回调设备
SPCF
154
SPR

图 16

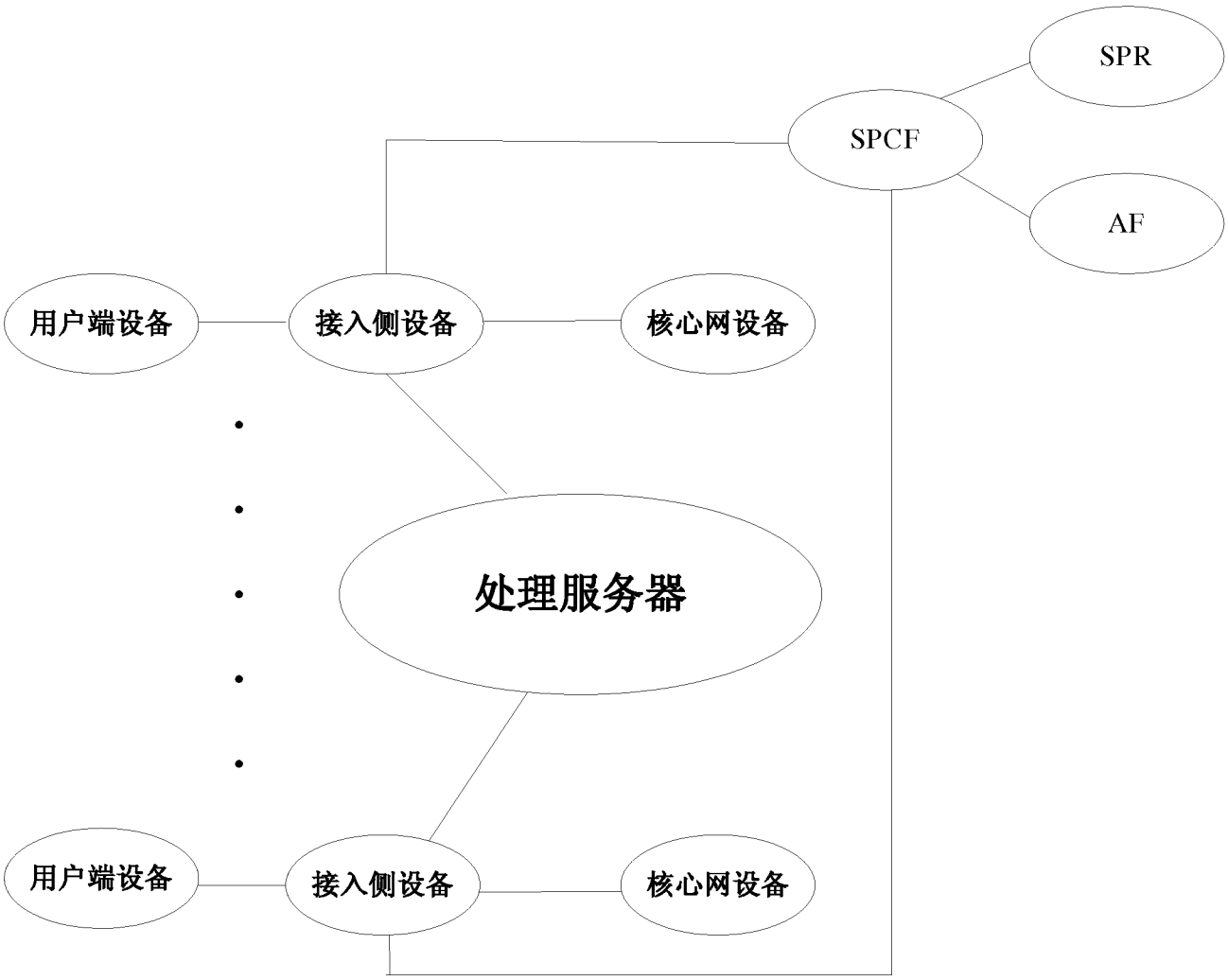
SPR
SPCF
AF
用户端设备
接入侧设备
核心网设备
处理服务器
用户端设备
接入侧设备
核心网设备

图 17

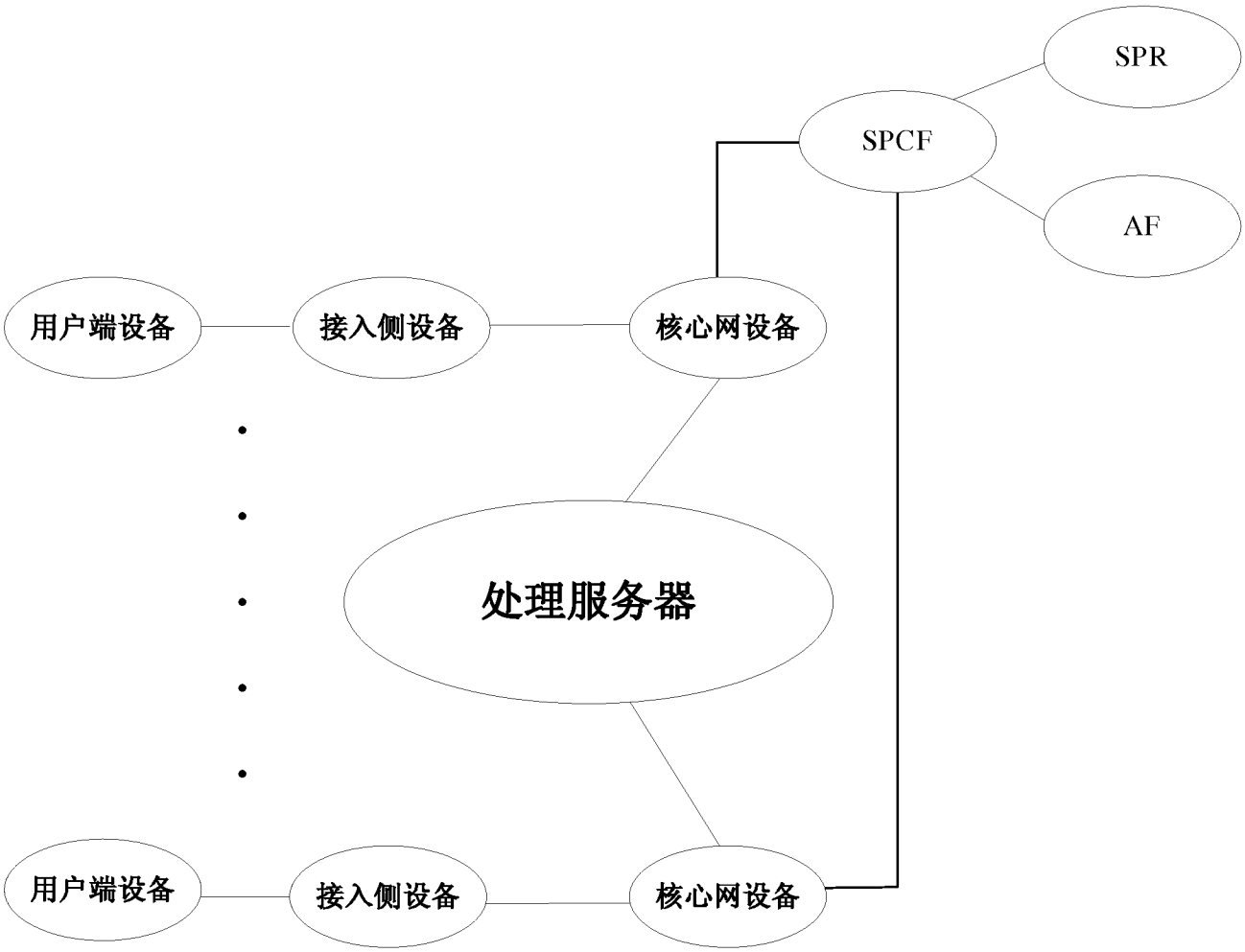

图 18

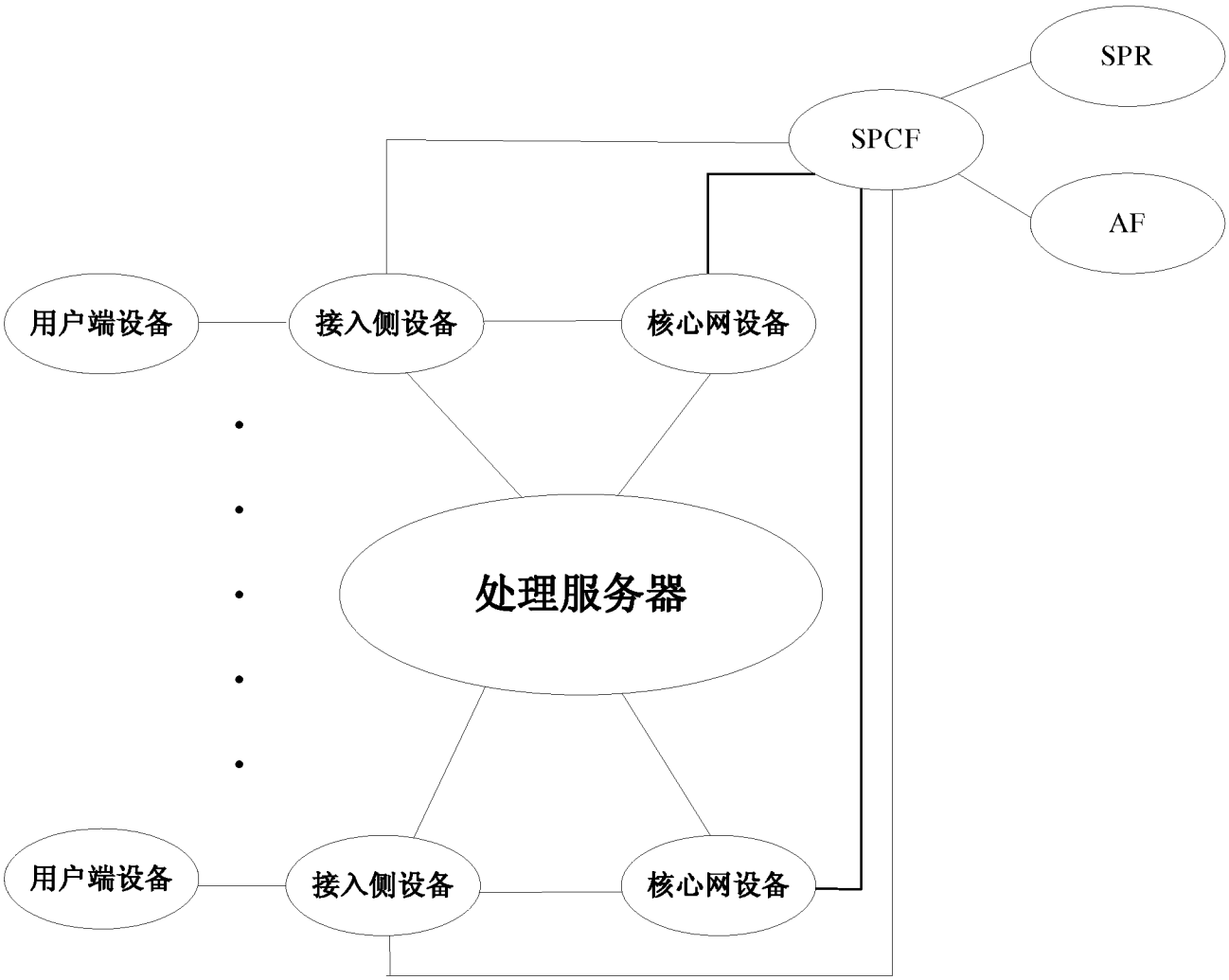

图 19

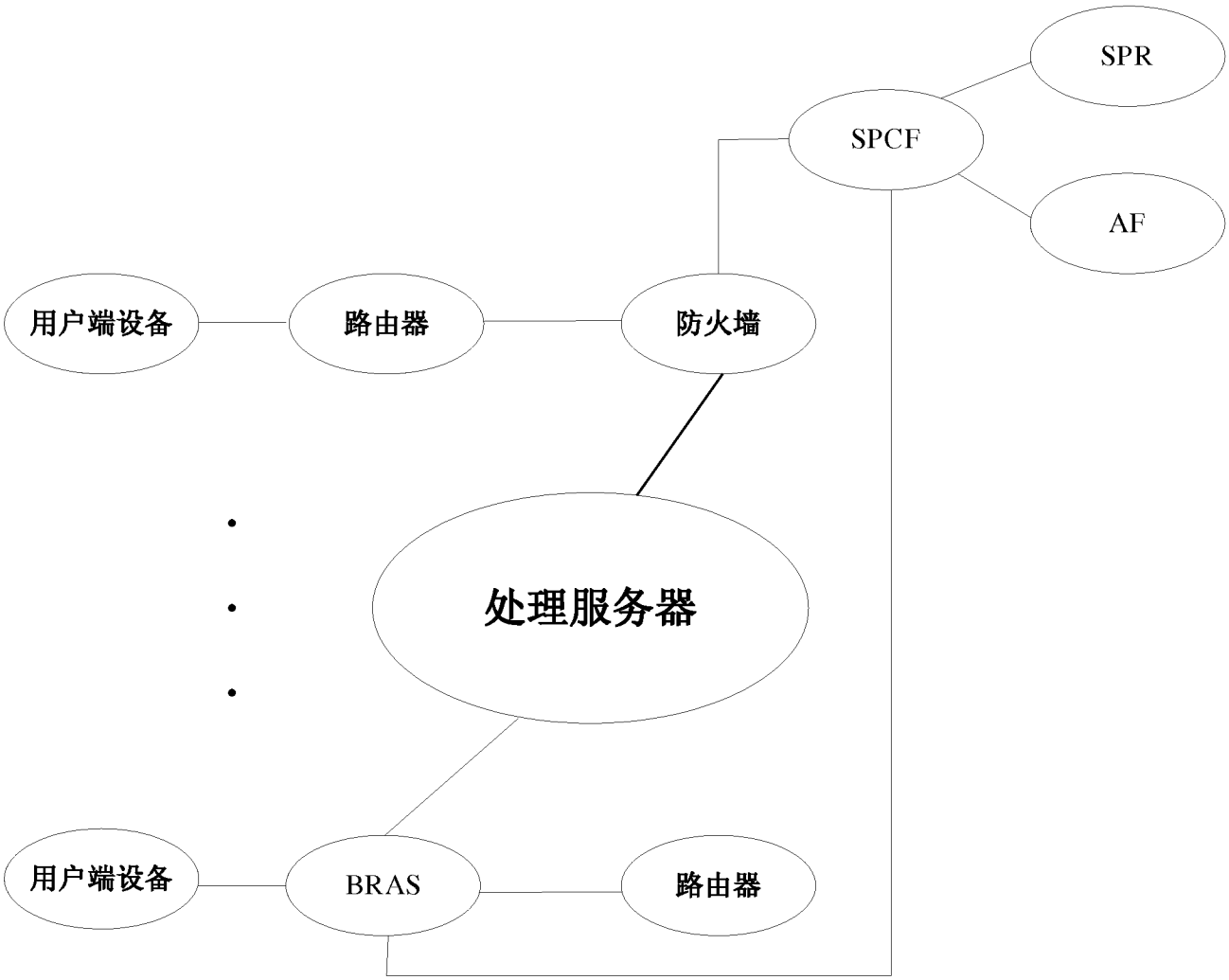

图 20

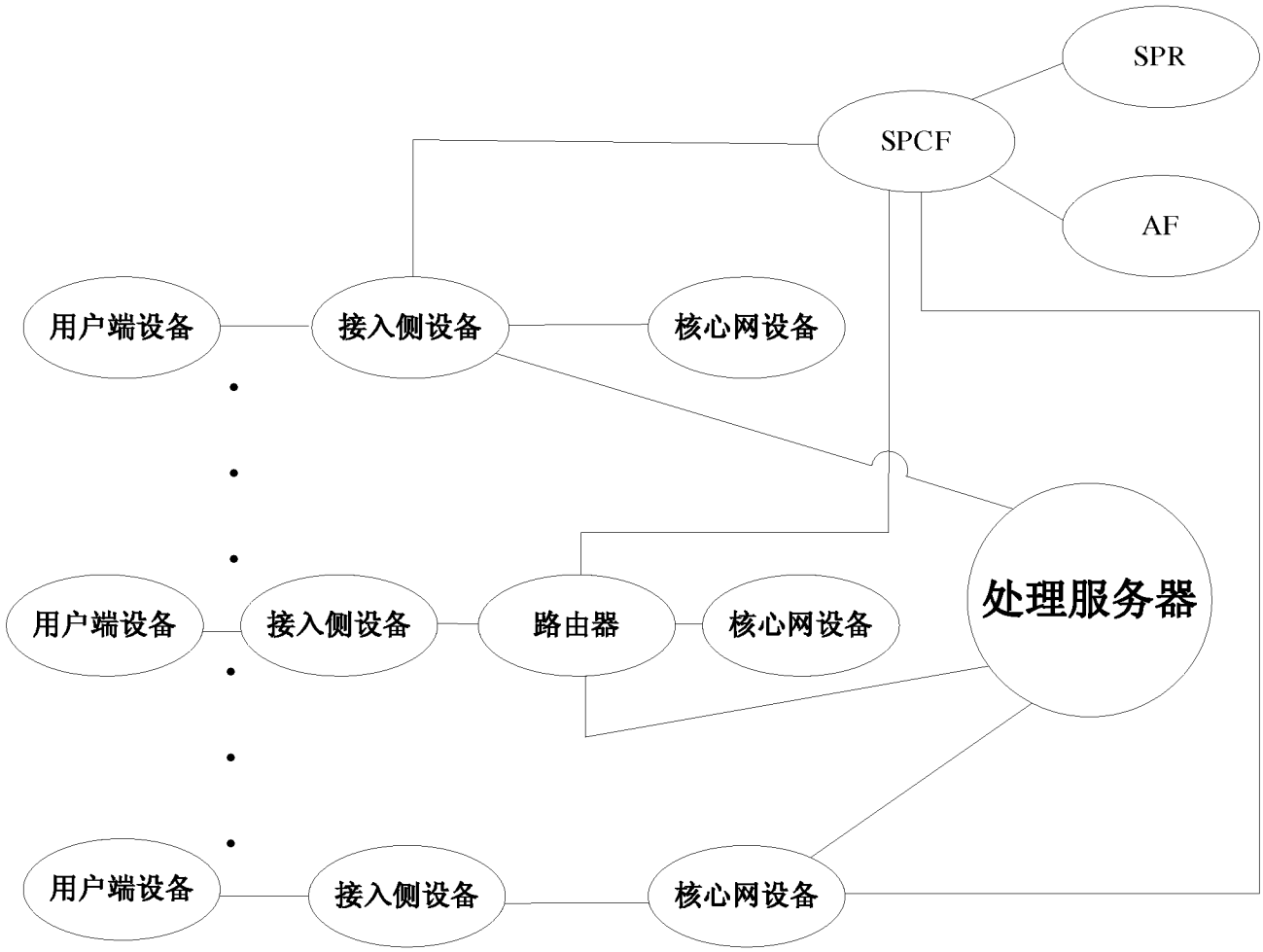
SPR
SPCF
AF
用户端设备
接入侧设备
核心网设备
用户端设备
接入侧设备
路由器
核心网设备
处理服务器
用户端设备
接入侧设备
核心网设备

图 21

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/074764

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (2006.01) 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)

IPC: H04B, H04L, H04W, G06F

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)

VEN, CNTXT, CPRSABS: acquire, extract+, obtain, identif+, match, address, send, transmit, receiv+, user w data, process, return

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102348222 A (ZTE CORP.), 08 February 2012 (08.02.2012), see description, paragraphs 0033-0043	29
A	CN 101540730 A (HUAWEI TECHNOLOGIES CO., LTD.), 23 September 2009 (23.09.2009), the whole document	1-40
A	CN 1957367 A (NOKIA CORP.), 02 May 2007 (02.05.2007), the whole document	1-40

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 July 2013 (17.07.2013)	**01 August 2013 (01.08.2013)**
Name and mailing address of the ISA/CN: 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 **LI, Qi** Telephone No.: (86-10) **62412015**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/074764

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102348222 A	08.02.2012	WO 2012016444 A1	09.02.2012
CN 101540730 A	23.09.2009	None	
CN 1957367 A	02.05.2007	US 2008032622 A1	07.02.2008
		KR 20090103959 A	01.20.2009
		KR 20070005696 A	10.01.2007
		WO 2005093622 A1	06.10.2005
		US 8060008 B2	15.11.2011
		EP 1743285 A1	17.01.2007
		US 7221902 B2	22.05.2007
		EP 1743285 B1	18.05.2011
		CN 1957367 B	22.08.2012
		BRPI 0509544 A	18.09.2007
		JP 2007531933 A	08.11.2007
		US 2005227674 A1	13.10.2005

国际检索报告

国际申请号
PCT/CN2013/074764

A. 主题的分类

H04L 12/24 (2006.01) 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)

IPC: H04B,H04L,H04W,G06F

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）)

VEN,CNTXT,CPRSABS：提取，获得，获取，标识，匹配，地址，发送，接收，用户数据，处理，返回，extract+，obtain，identif+，match，address，send，transmit，receiv+，user w data，process，return

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
X	CN 102348222 A （中兴通讯股份有限公司） 08.2 月 2012（08.02.2012）（参见说明书 0033-0043 段）	29
A	CN 101540730 A （华为技术有限公司） 23.9 月 2009（23.09.2009）全文	1-40
A	CN 1957367 A （诺基亚公司） 02.5 月 2007（02.05.2007）全文	1-40

☐ 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	国际检索报告邮寄日期
17.7 月 2013（17.07.2013）	**01.8 月 2013 (01.08.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 李祁 电话号码：(86-10) **62412015**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/074764

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 102348222 A	08.02.2012	WO 2012016444 A1	09.02.2012
CN 101540730 A	23.09.2009	无	
CN 1957367 A	02.05.2007	US 2008032622 A1	07.02.2008
		KR 20090103959 A	01.20.2009
		KR 20070005696 A	10.01.2007
		WO 2005093622 A1	06.10.2005
		US 8060008 B2	15.11.2011
		EP 1743285 A1	17.01.2007
		US 7221902 B2	22.05.2007
		EP 1743285 B1	18.05.2011
		CN1957367 B	22.08.2012
		BRPI 0509544 A	18.09.2007
		JP 2007531933 A	08.11.2007
		US 2005227674 A1	13.10.2005