(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
2019 年 4 月 25 日 (25.04.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/076000 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2018/081774

(22) 国际申请日: 2018 年 4 月 3 日 (03.04.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
PCT/CN2017/106349
2017年10月16日 (16.10.2017) CN

(71) 申请人: **OPPO 广东移动通信有限公司 (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(72) 发明人: **唐海 (TANG, Hai)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。

(74) 代理人: **北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (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, 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,

(54) **Title:** METHOD AND DEVICE FOR IDENTIFYING ENCRYPTED DATA STREAM, STORAGE MEDIUM, AND SYSTEM

(54) **发明名称:** 一种加密数据流的识别方法、设备、存储介质及系统

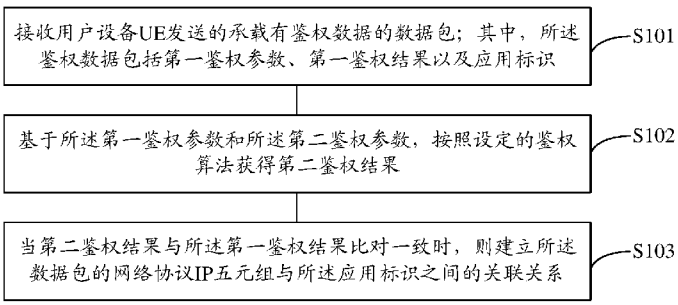

图 1

S101 RECEIVE A DATA PACKET BEARING AUTHENTICATION DATA AND SENT BY A USER EQUIPMENT (UE), WHEREIN THE AUTHENTICATION DATA COMPRISES A FIRST AUTHENTICATION PARAMETER, A FIRST AUTHENTICATION RESULT, AND AN APPLICATION IDENTIFICATION

S102 ACQUIRE A SECOND AUTHENTICATION RESULT ACCORDING TO A SET AUTHENTICATION ALGORITHM ON THE BASIS OF THE FIRST AUTHENTICATION PARAMETER AND A SECOND AUTHENTICATION PARAMETER

S103 WHEN THE SECOND AUTHENTICATION RESULT IS CONSISTENT WITH THE FIRST AUTHENTICATION RESULT ACCORDING TO A COMPARISON, ESTABLISH AN ASSOCIATION RELATIONSHIP BETWEEN A NETWORK PROTOCOL IP QUINTUPLE OF THE DATA PACKET AND THE APPLICATION IDENTIFICATION

(57) **Abstract:** The embodiments of the present invention provide a method and device for identifying an encrypted data stream, a readable storage medium, and a system. The method can be applied to a core network device. The method comprises: receiving a data packet bearing authentication data and sent by a user equipment (UE), wherein the authentication data comprises a first authentication parameter, a first authentication result, and an application identification; acquiring a second authentication result according to a set authentication algorithm on the basis of the first authentication parameter and a second authentication parameter, wherein the second authentication parameter is a pre-stored authentication parameter corresponding to the application identification; and when the second authentication result is consistent with the first authentication result according to a comparison, establishing an association relationship

WO 2019/076000 A1

[见续页]

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))。

between characteristic information of the data packet and the application identification, wherein the association relationship is used for subsequently identifying an encrypted data stream which is sent by the UE and corresponds to the application identification.

(57) 摘要：本发明实施例提供了一种加密数据流的识别方法、设备、可读存储介质及系统；该方法可以应用于核心网设备，所述方法包括：接收用户设备 UE发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识；基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别。

一种加密数据流的识别方法、设备、存储介质及系统

相关申请的交叉引用

本申请基于国际申请号为 PCT/CN2017/106349、国际申请日为 2017 年 10 月 16 日、发明名称为“一种加密数据流的识别方法、设备、存储介质及系统”的 PCT 国际申请提出，并要求该 PCT 国际申请的优先权，该 PCT 国际申请的全部内容在此引入本申请作为参考。

技术领域

本发明实施例涉及网络安全技术领域，尤其涉及一种加密数据流的识别方法、设备、可读存储介质及系统。

背景技术

超文本传输协议(HTTP, HyperText Transfer Protocol)2.0 版本出现之后，所有的 HTTP 层及 HTTP 层以上的应用层数据流均能够通过安全传输层协议（TLS，Transport Layer Security Protocol）协议进行加密，而运营商所提供的网络设备无法对加密数据流进行识别。

针对该问题，目前通常采用 TLS 层的某些明文标识在 TLS 协议的握手过程中对应用的加密数据流进行识别。但是，由于明文标识容易被破解，具有不安全的隐患，并且后续的 TLS 协议中不再支持明文标识。基于此，当前相关技术中并没有提出不依赖于明文标识对加密数据流进行识别的方案和机制。

发明内容

为解决上述技术问题，本发明实施例期望提供一种加密数据流的识别方法、设备、可读存储介质及系统；能够不依赖于明文标识就可以对加密数据流进行识别，提升了识别的安全性。

本发明实施例的技术方案可以如下实现：

第一方面，本发明实施例提供了一种加密数据流的识别方法，所述方法应用于核心网设备，所述方法包括：

接收用户设备 UE 发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识；

基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；

当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别。

第二方面，本发明实施例提供了一种加密数据流的识别方法，所述方法应用于用户设备 UE，所述方法包括：发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识。

第三方面，本发明实施例提供了一种核心网设备，包括：第一接收部分、鉴权部分和建立部分；其中，所述第一接收部分，配置为接收用户设备 UE 发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识；

所述鉴权部分，配置为基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；

所述建立部分，配置为当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别。

第四方面，本发明实施例提供了一种用户设备 UE，其中，所述 UE 包括：第二发送部分，配置为发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识。

第五方面，本发明实施例提供了一种核心网设备，其中，第一网络接口，第一存储器和第一处理器；其中，

所述第一网络接口，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

所述第一存储器，用于存储能够在所述第一处理器上运行的计算机程序；

所述第一处理器，用于在运行所述计算机程序时，执行第一方面中所述方法的步骤。

第六方面，本发明实施例提供了一种用户设备 UE，其中，所述 UE 包括：第二网络接口、第二存储器和第二处理器；其中，所述第二网络接口，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

所述第二存储器，用于存储能够在第二处理器上运行的计算机程序；

所述第二处理器，用于在运行所述计算机程序时，执行第二方面所述方法的步骤。

第七方面，本发明实施例提供了一种计算机可读介质，所述计算机可读介质存储有接入链路的管理程序，所述接入链路的管理程序被至少一个处理器执行时实现第一方面或第二方面所述的方法的步骤。

第八方面，本发明实施例提供了一种加密流量的识别系统，包括核心网设备以及用户设备，其中，所述用户设备，配置为发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识；

所述核心网设备，配置为接收用户设备 UE 发送的承载有鉴权数据的数据包；

基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；

当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别。

本发明实施例提供了一种加密数据流的识别方法、设备、可读存储介质及系统；核心网设备在 UE 与 OTT 服务器进行 TLS 握手过程中或握手完成后与 UE 进行鉴权，从而建立用于对加密数据流进行识别的关联关系，以实现对加密数据流的检测和统计，无需依赖明文标识，更无需进行复杂的 IP 地址配置和维护，提高了安全性并减少了配置和维护所需的计算资源。

附图说明

图 1 为本发明实施例提供的一种加密数据流的识别方法流程示意图；

图 2 为本发明实施例提供的另一种加密数据流的识别方法流程示意图；

图 3 为本发明实施例提供的一种网络架构示意图；

图 4 为本发明实施例提供的一种加密数据流的识别方法的具体示例流程示意图；

图 5 为本发明实施例提供的另一种加密数据流的识别方法的具体示例流程示意图；

图 6A 为本发明实施例提供的又一种加密数据流的识别方法的具体示例流程示意图；

图 6B 为本发明实施例提供的一种加密数据流的传输方法流程示意图；

图 7A 为本发明实施例提供的一种核心网设备的组成示意图；

图 7B 为本发明实施例提供的另一种核心网设备的组成示意图；

图 7C 为本发明实施例提供的又一种核心网设备的组成示意图；

图 8 为本发明实施例提供的一种核心网设备的具体硬件结构示意图；

图 9 为本发明实施例提供的一种用户设备的组成示意图；

图 10 为本发明实施例提供的另一种用户设备的组成示意图；

图 11 为本发明实施例提供的一种用户设备的具体硬件结构示意图；

图 12 为本发明实施例提供的再一种核心网设备的组成示意图；

图 13 为本发明实施例提供了又一种核心网设备的具体硬件结构示意图；

图 14 为本发明实施例提供的又一种用户设备的组成示意图；

图 15 为本发明实施例提供的又一种用户设备的具体硬件结构示意图；

图 16 为本发明实施例提供的一种加密流量的识别系统组成示意图。

具体实施方式

为了能够更加详尽地了解本发明实施例的特点与技术内容，下面结合附图对本发明实施例的实现进行详细阐述，所附附图仅供参考说明之用，并非用来限定本发明实施例。

目前，在第三代合作伙伴计划（3GPP，3rd Generation Partnership Project）的业务和系统方面工作组 2（SA2，Service and System Aspects Working Group）中定义了应用级别数据，用于对应用的流

量进行识别。基于此，第三方 OTT（Over The Top）服务商可以主动向运营商网络发起针对应用流量的识别规则进行安装或更新或删除的操作，从而使运营商网络具备识别业务的能力。但是，仍然没有针对业务的加密数据流进行识别的相关机制

基于上述内容，提出以下实施例。

实施例一

参见图 1，其示出了本发明实施例提供的一种加密数据流的识别方法，该方法可以应用于核心网设备中，可以理解地，本实施例所述的核心网设备，包括用户面和控制面两个部分；因此，本实施例所述的核心网设备既可以是包括用户面和控制面两个部分的单一实体设备，也可以是由用户面和控制面两个实体形成的核心网中的逻辑网元设备，本实施例对此不做具体限定，图 1 所示的方法可以包括：

S101：接收用户设备 UE 发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识；

S102：基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；

其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；可以理解地，第二鉴权参数可以由 OTT 服务器生成，并预先配置在核心网设备中；而第一鉴权参数也可以由 OTT 服务器生成，预先配置在 UE 中；而设定的鉴权算法可以静态地预先配置在 UE 和核心网设备中。

S103：当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；

其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别。

并且，所述数据包的特征信息可以包括以下至少一项或多项：网络协议 IP 源地址、IP 源端口号、IP 目的地址、IP 目的端口号、媒体接入控制（MAC，Media Access Control）源地址、IP 源端口号、MAC 目的地址、MAC 目的端口号、协议类型以及虚拟局域网（VLAN，Virtual Local Area Network）标签。

通过图 1 所示的技术方案，核心网设备能够通过上述关联关系针对应用标识所表示的应用程序的加密数据流进行识别，从而进一步地实现对加密数据流的检测和统计，无需依赖明文标识，更无需进行复杂的 IP 地址配置和维护，提高了安全性并减少了配置和维护所需的计算资源。

可以理解地，基于所述数据包的特征信息可能包含层 3 特征，即 IP 源地址、IP 源端口号、IP 目的地址、IP 目的端口号、IP 源端口号；也可能包含层 2 特征，即媒体接入控制（MAC，Media Access Control）源地址、MAC 目的地址、MAC 目的端口号、协议类型以及虚拟局域网（VLAN，Virtual Local Area Network）标签；上述关联关系不仅是数据包层 3 特征与应用标识之间的关联关系，而且也可以是层 2 特征与应用标识之间的关联关系，由此可知，当数据包通过非 IP 数据包传输时，仍然可以通过该关联关系针对应用标识所表示的应用程序的加密数据流进行识别。

对于图 1 所示的技术方案，在第一种可能的实现方式中，图 1 所示的技术方案可以在 UE 与 OTT 服务器建立 TLS 握手过程中进行实施，因此，所述接收用户设备 UE 发送的承载有鉴权数据的数据包，包括：

在应用层会话建立的 TLS 握手过程中，所述核心网设备的用户面接收所述 UE 发送的首次 TLS 握手请求；其中，所述鉴权数据承载于所述首次 TLS 握手请求中的明文字段。

具体来说，对于上述实现方式，UE 可以在首次 TLS 握手请求中新增加一个明文字段，并将鉴权数据加入该新增的明文字段。

相应于上述实现方式，在接收用户设备 UE 发送的承载有鉴权数据的数据包后，所述方法还包括：

所述核心网设备的用户面从所述首次 TLS 握手请求中的明文字段检测到所述鉴权数据后，将所述鉴权数据传输至所述核心网设备的控制面。

需要说明的是，核心网设备的控制面在获取到所述鉴权数据后，就能够按照鉴权数据来执行图 1 所示方案中的 S102，并且将所述第二鉴权结果与所述第一鉴权结果进行比对后向核心网设备用户面发送比对结果，从而核心网设备用户面根据比对结果确定是否执行 S103，可以理解地，当所述第二鉴权结果与所述第一鉴权结果比对不一致时，则忽略该比对结果。

对于图 1 所示的技术方案，在第二种可能的实现方式中，图 1 所示的技术方案可以在 UE 与 OTT 服务器之间完成 TLS 握手后进行实施，因此，所述接收用户设备 UE 发送的承载有鉴权数据的数据包，包括：

在完成 TLS 握手后，所述核心网设备的用户面接收所述 UE 通过基站发送的鉴权请求；其中，

所述鉴权数据承载于所述鉴权请求中的 GTP-U 扩展字段。

具体来说，对于上述实现方式，鉴权请求是在完成了应用层 TLS 握手后，由 UE 主动发起的。UE 可以将鉴权数据承载于扩展的 PDCP 字段中发送给基站侧，而基站侧则可以将 PDCP 扩展字段中的鉴权数据转换成 GTP-U 扩展字段，继续发送给核心网设备用户面。

相应于上述实现方式，在接收用户设备 UE 发送的承载有鉴权数据的数据包后，所述方法还包括:

所述核心网设备的用户面从鉴权请求中的 GTP-U 扩展字段检测到所述鉴权数据后，将所述鉴权数据传输至所述核心网设备的控制面。

同理于上述实现方式，需要说明的是，核心网设备的控制面在获取到所述鉴权数据后，就能够按照鉴权数据来执行图 1 所示方案中的 S102，并且将所述第二鉴权结果与所述第一鉴权结果进行比对后向核心网设备用户面发送比对结果，从而核心网设备用户面根据比对结果确定是否执行 S103，可以理解地，当所述第二鉴权结果与所述第一鉴权结果比对不一致时，则忽略该比对结果。

针对上述两种实现方式，优选地，所述第一鉴权参数包括随机数，所述第二鉴权参数包括公共密钥 Ka；或者，所述第一鉴权参数包括公共密钥 Ka，所述第二鉴权参数包括随机数。

对于随机数，需要说明的是，该随机数可以是基于预设的随机数生成策略所生成的随机数；除此之外，该随机数还可以是随着当前时间和/或 UE 当前所在地点相应变更的数，从而实现每个随机数之间都是不同的。举例来说，通常 UE 当前所在的地点与 UE 的 IP 地址之间具有相关性，不同 UE 之间，其 IP 地址也相应不同。因此，随机数可以由当前时间戳与 UE 的 IP 地址组成得到，从而能够实现当 UE、时间以及地点中至少一项不同时，其对应的随机数也是不同。也就实现了每个随机数之间都是不同的效果。

可以理解地，在本发明实施例中，后续关于随机数的具体生成过程可以按照上述说明实现，不再赘述。

针对上述两种实现方式，优选地，所述基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果，包括:

所述核心网设备的控制面基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果。

针对上述两种实现方式，优选地，当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系，包括:

当所述第二鉴权结果与所述第一鉴权结果比对一致时，所述核心网设备的控制面将比对结果传输至所述核心网用户面;

所述核心网设备的用户面建立所述数据包的特征信息与所述应用标识之间的关联关系。

对于图 1 所示的技术方案，在第三种可能的实现方式中，图 1 所示的技术方案可以在 UE 与 OTT 服务器之间完成 TLS 握手后进行实施，但与第二种实现方式不同的地方在于，鉴权请求由 UE 直接向核心网设备的控制面发送，因此，所述接收用户设备 UE 发送的承载有鉴权数据的数据包，包括:

在完成 TLS 握手后，所述核心网设备的控制面接收所述 UE 发送的非接入层会话管理 NAS-SM 消息;

其中，所述 NAS-SM 消息的扩展字段中包括：第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征信息；其中，所述第一鉴权参数包括：随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括至少一项或多项：OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

相应于上述实现方式，所述基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果，包括:

所述核心网设备的控制面根据所述第一鉴权参数中的随机数以及所述第二鉴权参数中的公共密钥按照设定的鉴权算法获得第二鉴权结果。

相应于上述实现方式，当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系，包括:

当所述第二鉴权结果与所述第一鉴权结果比对一致时，所述核心网设备的控制面根据所述 OTT 服务器的特征信息以及所述 UE 的特征信息生成所述数据包的特征信息，并将生成的所述数据包的特征信息和所述应用标识传输至所述核心网设备的用户面；具体来说，OTT 服务器的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址；UE 的特征信息包括：UE 的 IP 地址、端口和 MAC 地址。

所述核心网设备的用户面建立所述生成的数据包的特征信息和所述应用标识之间的关联关系。

对于图 1 所示的技术方案，所述基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果后，所述方法还包括:

所述核心网设备的控制面通过所述核心网设备的用户面将所述第二鉴权结果与所述第一鉴权结果的比对结果发送至所述 UE。

可以理解地，UE 在接收到比对结果之后，就能够获知核心网设备是否完成了关联关系的建立，从而决定是否继续进行与核心网设备之间的鉴权。

此外，对于图 1 所示的技术方案，数据包的特征信息与所述应用标识之间的关联关系建立完成之后，可以针对其设置生命周期，具体来说，图 1 所示的技术方案还可以包括：接收所述 UE 发送的有效时间信息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长。可以理解地，上述有效时长可以作为该关联关系的生命周期。因此，优选来说，所述方法还可以包括：当所述有效时长计时完毕后，若加密数据流传输未完成，释放所述关联关系。

另外，该关联关系还可以通过 UE 的指示进行释放，基于此，可以无需考虑生命周期即有效时长，优选来说，所述方法还包括:

在所述有效时长内或所述有效时长结束，接收所述 UE 发送的释放指示消息;

基于所述释放指示消息释放所述关联关系。

需要说明的是，上述有效时间消息以及释放指示消息均可以通过 NAS 消息进行发送。

本实施例提供了一种应用于核心网设备的加密数据流的识别方法，能够在 UE 与 OTT 服务器进行 TLS 握手过程中或握手完成后与 UE 进行鉴权，从而建立用于对加密数据流进行识别的关联关系，以实现对加密数据流的检测和统计，无需依赖明文标识，更无需进行复杂的 IP 地址配置和维护，提高了安全性并减少了配置和维护所需的计算资源。

实施例二

基于前述实施例相同的发明构思，参见图 2，其示出了本发明实施例提供的一种加密数据流的识别方法，该方法可以应用于 UE 中，图 2 所示的方法可以包括:

S201：发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识。

可以理解地，当 UE 将鉴权数据发送至核心网设备之后，核心网设备就能够按照前述实施例的技术方案进行鉴权，从而建立用于对加密数据流进行识别的关联关系，以实现对加密数据流的检测和统计，无需依赖明文标识，更无需进行复杂的 IP 地址配置和维护，提高了安全性并减少了配置和维护所需的计算资源。

对于图 2 所示的技术方案，在第一种可能的实现方式中，图 2 所示的技术方案可以在 UE 与 OTT 服务器建立 TLS 握手过程中进行实施，因此，所述发送承载有鉴权数据的数据包，包括:

在应用层会话建立的 TLS 握手过程中，将所述鉴权数据承载于首次 TLS 握手请求中的明文字段;

将所述承载有所述鉴权数据的首次 TLS 握手请求通过核心网设备的用户面透传至所述核心网设备的控制面。

对于图 2 所示的技术方案，在第二种可能的实现方式中，图 2 所示的技术方案可以在 UE 与 OTT 服务器之间完成 TLS 握手后进行实施，因此，所述发送承载有鉴权数据的数据包，包括:

在完成 TLS 握手后，将所述鉴权数据承载于扩展的 PDCP 字段的鉴权请求发送至基站，并通过基站将 PDCP 扩展字段中的鉴权数据转换成 GTP-U 扩展字段后，将所述鉴权请求继续发送至所述核心网设备用户面。

对于图 2 所示的技术方案，在第三种可能的实现方式中，图 2 所示的技术方案可以在 UE 与 OTT 服务器之间完成 TLS 握手后进行实施，但与第二种实现方式不同的地方在于，鉴权请求由 UE 直接向核心网设备的控制面发送，因此，所述发送承载有鉴权数据的数据包，包括:

在完成 TLS 握手后，向核心网设备的控制面发送非接入层会话管理 NAS-SM 消息；其中，所述 NAS-SM 消息的扩展字段中包括：第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征信息；其中，所述第一鉴权参数包括：随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括所 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

此外，对于图 2 所示的技术方案，当核心网设备建立数据包的特征信息与应用标识之间的关联关系之后，还可以通过 UE 来确定该关联关系的生命周期，基于此，优选地，所述方法还包括:

向所述核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长。

优选地，所述方法还包括:

向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

需要说明的是，上述有效时间消息以及释放指示消息均可以通过 NAS 消息进行发送。

对于图 2 所示的技术方案，当核心网设备鉴权完毕后，所述方法还包括：接收核心网设备的控制面回复的鉴权结果。可以理解地，UE 在接收到比对结果之后，就能够获知核心网设备是否完成了关联关系的建立，从而决定是否继续进行与核心网设备之间的鉴权。

实施例三

基于前述实施例相同的发明构思，本实施例通过以下具体示例对前述两个实施例的技术方案进行详细地阐述。

针对具体示例需要说明的是，具体示例引入了针对应用程序的参数组，举例来说，可以包括：公共秘钥 Ka、随机数、令牌 Token、应用标识 Application ID。其中，Ka 和随机数结合预先设定的鉴权算法来生成 Token，若以鉴权算法为 HASH 算法为例，则可以得到 Token=HASH(Ka，随机数)；因此，公共秘钥 Ka、随机数 为鉴权参数，Token 可以为鉴权结果，应用标识 Application ID 用来表示对应的应用程序。需要指出的是，Ka 和随机数由 OTT 服务器生成，鉴权算法通过 OTT 服务器静态配置在核心网设备和 UE 上。综上，本实施例的具体示例可以应用于如图 3 所示的非典型的网络架构中，在该网络架构中，UE 通过基站接入核心网，或者可以直接与核心网设备相连接，核心网设备中包括用户面和控制面两个部分，UE 通过核心网设备连接数据网络（DN，Data Network），实现与 OTT 服务器之间的信息交互。基于上述网络架构，提出以下具体示例。

具体示例一

参见图 4，其示出了本发明实施例提供的一种加密数据流的识别方法的具体示例流程，该流程可以包括:

S40A：OTT 服务器将鉴权算法预先配置在 UE 以及核心网设备中；

S40B：OTT 服务器动态生成或更新 Ka 和随机数，并发往 UE 和核心网设备；

可以理解地，UE 和核心网设备各自在接收到 Ka 和随机数后，可以按照 S40A 中配置的鉴权算法进行计算，分别得到各自的鉴权结果 Token。

S401：UE 在首次 TLS 握手请求中新增明文字段，并将自身的随机数和 Token，以及应用标识作为鉴权数据加入到新增的明文字段中；

S402：UE 将首次 TLS 握手请求发送至核心网设备的用户面；

S403：用户面在检测到首次 TLS 握手请求中包括 UE 发送的鉴权数据时，将鉴权数据透传给核心网设备的控制面；

S404：控制面根据自身的 Ka 以及 UE 的随机数按照配置的鉴权算法进行计算，并将计算结果与 UE 的 Token 进行比较；若两者一致，比较结果为鉴权成功；否则，比较结果为鉴权失败。

S405：控制面将比较结果发送至用户面；

S406: 若鉴权成功，用户面建立首次 TLS 握手请求的特征信息与所述应用标识之间的关联关系。

可以理解地，该关联关系能够使得核心网设备识别后续该应用标识对表示的应用程序的加密数据流，并根据识别结果对加密数据流的流量进行统计。

可选地，在本实施例中，如虚线箭头所示，S407：控制面将比较结果通过用户面发送至 UE；从而使得 UE 在接收到比较结果之后，就能够获知核心网设备是否完成了关联关系的建立，从而决定是否需要继续进行与核心网设备之间的鉴权。

具体示例二

参见图 5，其示出了本发明实施例提供的一种加密数据流的识别方法的具体示例流程，该流程实施于 UE 与 OTT 服务器之间完成 TLS 握手后，该流程可以包括:

S50A：TLS 握手完成后，HTTP 内容全部加密；

S50B：OTT 服务器将向 UE 发送应用标识，随机数和 Ka；

可以理解地，OTT 向 UE 发送上述信息时，运营商网络对此不可见。

S501：UE 根据随机数与 Ka 按照预先设置的鉴权算法计算出 Token，并将自身的随机数、Token 以及应用标识作为鉴权数据承载于扩展的 PDCP 字段的鉴权请求。

S502：UE 将鉴权请求发送至基站；

S503：基站将鉴权数据转换成 GTP-U 扩展字段后，将所述鉴权请求继续发送至所述核心网设备用户面；

S504：用户面在检测到鉴权请求中包括鉴权数据后，将鉴权数据透传至核心网设备的控制面；

S505：控制面根据自身的 Ka 以及 UE 的随机数按照配置的鉴权算法进行计算，并将计算结果与 UE 的 Token 进行比较；若两者一致，比较结果为鉴权成功；否则，比较结果为鉴权失败。

S506：控制面将比较结果发送至用户面；

S507：若鉴权成功，用户面建立鉴权请求的特征信息与所述应用标识之间的关联关系。

可以理解地，该关联关系能够使得核心网设备识别后续该应用标识对表示的应用程序的加密数据流，并根据识别结果对加密数据流的流量进行统计。

可选地，在本实施例中，如虚线箭头所示，S508：控制面将比较结果通过用户面发送至 UE；从而使得 UE 在接收到比较结果之后，就能够获知核心网设备是否完成了关联关系的建立，从而决定是否需要继续进行与核心网设备之间的鉴权。

具体示例三

参见图 6A，其示出了本发明实施例提供的一种加密数据流的识别方法的具体示例流程，该流程实施于 UE 与 OTT 服务器之间完成 TLS 握手后，该流程可以包括：

S60A：TLS 握手完成后，HTTP 内容全部加密；

S60B：OTT 服务器将向 UE 发送应用标识，随机数和 Ka；

可以理解地，OTT 向 UE 发送上述信息时，运营商网络对此不可见。

S601：UE 根据随机数与 Ka 按照预先设置的鉴权算法计算出 Token，并将自身的随机数、Ka、Token、应用标识和 OTT 服务器的特征信息作为鉴权数据承载于 NAS-SM 消息的扩展字段中。

可以理解地，OTT 服务器的 IP 三元组可以包括 OTT 服务器的 IP 地址、端口号和协议类型。

S602：UE 向核心网设备的控制面发送 NAS-SM 消息，从而向控制面请求会话修改；

S603：控制面根据自身的自身的 Ka 以及 UE 的随机数按照配置的鉴权算法进行计算，并将计算结果与 UE 的 Token 进行比较；若两者一致，比较结果为鉴权成功；否则，比较结果为鉴权失败；

S604：若鉴权成功，控制面根据所述 OTT 服务器的特征信息以及所述 UE 的特征信息生成数据包的特征信息；

S605：控制面将生成的数据包的特征信息和所述应用标识传输至所述核心网设备的用户面；

S606：用户面建立生成的数据包的特征信息和所述应用标识之间的关联关系。

S607：用户面建立完成后，通知控制面更新完成。

S608：控制面通过 NAS 消息向 UE 回复比较结果。

具体示例四

基于前述具体示例完成关联关系建立之后，还可以在加密数据传输过程中为该关联关系建立生命周期，基于此，参见图 6B 所示的加密数据流的传输方法，可以应用于 UE 与 OTT 服务器之间即将或正在传输加密数据流的过程，该方法可以包括：

S61：UE 通过 NAS 消息向核心网设备发送有效时间消息；

其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长。

可以理解地，上述有效时长表征了关联关系的生命周期，基于此，该方法还可以包括 S62：在加密数据流传输过程中，核心网设备基于关联关系设置数据流过滤器；

在该步骤中，数据流过滤器可以认为是关联关系的具体体现，因此，关联关系的生命周期与数据流过滤器的生命周期相同，可选地，参见图 6B 中虚线框所示，

S63A：在有效时间消息所指示的有效时长结束后，释放数据流过滤器。

此外，关联关系的生命周期除了上述有效时长以外，还可以通过 UE 的指示进行确定，因此，可选地，参见图 6B 中点划线框所示，

S63B：加密数据流传输结束后，UE 通过 NAS 消息向核心网设备释放指示消息；

S64B：核心网设备基于所述释放指示消息释放所述数据流过滤器。

可以理解地，当核心网设备基于 UE 发送的释放指示消息针对数据流过滤器进行释放时，可以无需考虑有效时长的限制；而且，在另一种具体实现过程中，即使有效时长结束，但是加密数据流传输还未终止的情况下，核心网设备同样不释放该数据流过滤器，直至加密数据流传输完毕才进行释放。

基于上述具体示例四，本发明实施例提供了一种应用于核心网设备的加密数据流的传输方法，所述方法包括：

在建立完成数据包的特征信息与应用标识之间的关联关系后，接收用户设备 UE 发送的有效时间消息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长；

在所述有效时长内，基于所述关联关系与所述 UE 进行加密数据流传输；

接收所述 UE 发送的释放指示消息；

基于所述释放指示消息释放所述关联关系。

在上述方案中，所述方法还包括：

在所述有效时长计时完毕后，释放所述关联关系；或者，

在所述有效时长计时完毕后，继续与所述 UE 进行加密数据流传输，直至所述加密数据流传输结束后释放所述关联关系。

此外，基于上述具体示例四，本发明实施例还提供了一种应用于 UE 的加密数据流的传输方法，所述方法应用于用户设备 UE，所述方法包括：

向核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长；

在所述有效时长内，基于所述关联关系与所述核心网设备进行加密数据流传输；

向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

实施例四

基于前述实施例相同的发明构思，参见图 7A，其示出了本发明实施例提供的一种核心网设备 70 的组成，可以包括：第一接收部分 701、鉴权部分 702 和建立部分 703；其中，

所述第一接收部分 701，配置为接收用户设备 UE 发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识；

所述鉴权部分 702，配置为基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；

所述建立部分 703，配置为当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别。

在一种可能的实现方式中，所述第一接收部分 701，配置为在应用层会话建立的 TLS 握手过程中，接收所述 UE 发送的首次 TLS 握手请求；其中，所述鉴权数据承载于所述首次 TLS 握手请求中的明文字段。

在一种可能的实现方式中，所述第一接收部分 701，配置为：在完成 TLS 握手后，所述核心网设备的用户面接收所述 UE 通过基站发送的鉴权请求；其中，所述鉴权数据承载于所述鉴权请求中的 GTP-U 扩展字段。

可以理解地，在上述两个实现方式中，第一接收部分 701 可以为核心网设备 70 的用户面，相应地，鉴权部分为核心网设备 70 的控制面，建立部分为核心网设备 70 的用户面。

在一种可能的实现方式中，所述第一接收部分 701，配置为在完成 TLS 握手后，所述核心网设备的控制面接收所述 UE 发送的非接入层会话管理 NAS-SM 消息；其中，所述 NAS-SM 消息的扩展字段中包括：第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征信息；其中，所述第一鉴权参数包括：随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

在上述实现方式中，所述鉴权部分 702，配置为根据所述第一鉴权参数中的随机数以及所述第二鉴权参数中的公共密钥按照设定的鉴权算法获得第二鉴权结果。

在上述实现方式中，所述建立部分 703，配置为：

当所述第二鉴权结果与所述第一鉴权结果比对一致时，根据所述 OTT 服务器的特征信息以及所述 UE 的特征信息生成所述数据包的特征信息，并建立所述生成的数据包的特征信息和所述应用标识之间的关联关系。具体来说，OTT 服务器的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址；UE 的特征信息包括：UE 的 IP 地址、端口和 MAC 地址。

可以理解地，在上述实现方式中，第一接收部分 701 和鉴权部分 702 可以为核心网设备 70 的控制面，相应地，建立部分 703 为核心网设备 70 的用户面。

在一种可能的实现方式中，参见图 7B，所述核心网设备 70 还包括第一发送部分 704，配置为将所述第二鉴权结果与所述第一鉴权结果的比对结果发送至所述 UE。需要说明的是，第一发送部分 704 为核心网设备 70 的控制面。

在上述方案中，所述第一接收部分 701，还配置为接收所述 UE 发送的有效时间信息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长。

在上述方案中，参见图 7C，所述核心网设备 70 还包括控制部分 705，配置为当所述有效时长计时完毕后，若加密数据流传输未完成，释放所述关联关系。

在上述方案中，所述第一接收部分 701，还配置为加密数据流传输完毕后，接收所述 UE 发送的释放指示消息；

所述控制部分 705，还配置为基于所述释放指示消息释放所述关联关系。

可以理解地，在本实施例中，“部分”可以是部分电路、部分处理器、部分程序或软件等等，当然也可以是单元，还可以是模块也可以是非模块化的。

另外，在本实施例中的各组成部分可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

所述集成的单元如果以软件功能模块的形式实现并非作为独立的产品进行销售或使用时，可以存储在一个计算机可读取存储介质中，基于这样的理解，本实施例的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或 processor（处理器）执行本实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM， Read Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

因此，本实施例提供了一种计算机可读介质，该计算机可读介质存储有加密数据流的识别程序，所述加密数据流的识别程序被至少一个处理器执行时实现上述实施例一所述的方法的步骤。

基于上述核心网设备 70 以及计算机可读介质，参见图 8，其示出了本发明实施例提供的核心网设备 70 的具体硬件结构，可以包括：第一网络接口 801、第一存储器 802 和第一处理器 803；各个组件通过总线系统 804 耦合在一起。可理解，总线系统 804 用于实现这些组件之间的连接通信。总线系统 804 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 8 中将各种总线都标为总线系统 804。其中，第一网络接口 801，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

第一存储器 802，用于存储能够在第一处理器 803 上运行的计算机程序；

第一处理器 803，用于在运行所述计算机程序时，执行：

接收用户设备 UE 发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识；

基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；

当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别。

可以理解，本发明实施例中的第一存储器 802 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-Only Memory，ROM)、可编程只读存储器 (Programmable ROM，PROM)、可擦除可编程只读存储器(Erasable PROM，EPROM)、电可擦除可编程只读存储器(Electrically EPROM，EEPROM)或闪存。易失性存储器可以是随机存取存储器(Random Access Memory，RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器(Static RAM，SRAM)、动态随机存取存储器 (Dynamic RAM，DRAM)、同步动态随机存取存储器(Synchronous DRAM，SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate SDRAM，DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM，ESDRAM)、同步连接动态随机存取存储器(Synchlink DRAM，SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM，DRRAM)。本文描述的系统和方法的第一存储器 802 旨在包括但不限于这些和任意其它适合类型的存储器。

而第一处理器 803 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过第一处理器 803 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的第一处理器 803 可以是通用处理器、数字信号处理器(Digital Signal Processor，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现成可编程门阵列(Field Programmable Gate Array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可

以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程 存储器、寄存器等本领域成熟的存储介质中。该存储介质位于第一存储器 802，第一处理器 803 读取第一存储器 802 中的信息，结合其硬件完成上述方法的步骤。

可以理解的是，本文描述的这些实施例可以用硬件、软件、固件、中间件、微码或其组合来实现。对于硬件实现，处理单元可以实现在一个或多个专用集成电路(Application Specific Integrated Circuits，ASIC)、数字信号处理器(Digital Signal Processing，DSP)、数字信号处理设备(DSP Device，DSPD)、可编程逻辑设备(Programmable Logic Device，PLD)、现场可编程门阵列(Field-Programmable Gate Array，FPGA)、通用处理器、控制器、微控制器、微处理器、用于执行本申请所述功能的其它电子单元或其组合中。

对于软件实现，可通过执行本文所述功能的模块(例如过程、函数等) 来实现本文所述的技术。软件代码可存储在存储器中并通过处理器执行。存储器可以在处理器中或在处理器外部实现。

具体来说，核心网设备 70 中的第一处理器 803 还配置为运行所述计算机程序时，执行前述实施例一中所述的方法步骤，这里不再进行赘述。

实施例五

基于前述实施例相同的发明构思，参见图 9，其示出了本发明实施例提供的一种用户设备 90 的组成，可以包括：第二发送部分 901，配置为发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识。

在上述方案中，所述第二发送部分 901，配置为：在应用层会话建立的 TLS 握手过程中，将所述鉴权数据承载于首次 TLS 握手请求中的明文字段；

将所述承载有所述鉴权数据的首次 TLS 握手请求通过核心网设备的用户面透传至所述核心网设备的控制面。

在上述方案中，所述第二发送部分 901，配置为：在完成 TLS 握手后，将所述鉴权数据承载于扩展的 PDCP 字段的鉴权请求发送至基站，并通过基站将 PDCP 扩展字段中的鉴权数据转换成 GTP-U 扩展字段后，将所述鉴权请求继续发送至所述核心网设备用户面。

在上述方案中，所述第二发送部分 901，配置为：在完成 TLS 握手后，向核心网设备的控制面发送非接入层会话管理 NAS-SM 消息；其中，所述 NAS-SM 消息的扩展字段中包括：第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征信息；其中，所述第一鉴权参数包括：随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

在上述方案中，参见图 10，所述 UE 90 还包括第二接收部分 902，配置为接收核心网设备的控制面回复的鉴权结果。

在上述方案中，所述第二发送部分 901，还配置为向所述核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长。

在上述方案中，所述第二发送部分 901，还配置为向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

此外，本实施例还提供了一种计算机可读介质，该计算机可读介质存储有加密数据流的识别程序，所述加密数据流的识别程序被至少一个处理器执行时实现上述实施例二所述的方法的步骤。针对计算机可读介质的具体阐述，参见实施例四中的说明，在此不再赘述。

基于上述 UE 90 的组成以及计算机可读介质，参见图 11，其示出了本发明实施例提供的 UE 90 的具体硬件结构，可以包括：第二网络接口 1101、第二存储器 1102 和第二处理器 1103；各个组件通过总线系统 1104 耦合在一起。可理解，总线系统 1104 用于实现这些组件之间的连接通信。总线系统 1104 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 11 中将各种总线都标为总线系统 1104。其中，所述第二网络接口 1101，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

第二存储器 1102，用于存储能够在第二处理器 1103 上运行的计算机程序；

第二处理器 1103，用于在运行所述计算机程序时，执行：

发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识。

可以理解地，本实施例中 UE 90 的具体硬件结构中的组成部分，与实施例四中的相应部分类似，在此不做赘述。

具体来说，UE 90 中的第二处理器 1103，还配置为运行所述计算机程序时，执行前述实施例二中所述的方法步骤，这里不再进行赘述。

实施例六

基于前述实施例相同的发明构思，参见图 12，其示出了本发明实施例提供的另一种核心网设备 120，包括：消息接收部分 1201、第一传输部分 1202 和控制部分 1203；其中，所述消息接收部分 1201，配置为在建立完成数据包的特征信息与应用标识之间的关联关系后，接收用户设备 UE 发送的有效时间消息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长；

所述第一传输部分 1202，配置为在所述有效时长内，基于所述关联关系与所述 UE 进行加密数据流传输；

所述消息接收部分 1201，还配置为在所述加密数据流传输结束后，接收所述 UE 发送的释放指示消息；

所述控制部分 1203，配置为基于所述释放指示消息释放所述关联关系。

在上述方案中，所述控制部分 1203，还配置为在所述有效时长计时完毕后，释放所述关联关系；或者，

在所述有效时长计时完毕后，继续与所述 UE 进行加密数据流传输，直至所述加密数据流传输结束后所述第一接收部分接收所述释放指示消息，并基于所述释放指示消息释放所述关联关系。

此外，本实施例还提供了一种计算机可读介质，该计算机可读介质存储有加密数据流的传输程序，所述加密数据流的传输程序被至少一个处理器执行时实现上述实施例三中具体示例四所述的方法的步骤。针对计算机可读介质的具体阐述，参见实施例四中的说明，在此不再赘述。

基于上述核心网设备 120 的组成以及计算机可读介质，参见图 13，其示出了本发明实施例提供的核心网设备 120 的具体硬件结构，可以包括：第三网络接口 1301、第三存储器 1302 和第三处理器 1303；各个组件通过总线系统 1304 耦合在一起。可理解，总线系统 1304 用于实现这些组件之间的连接通信。总线系统 1304 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 13 中将各种总线都标为总线系统 1304。其中，所述第三网络接口 1301，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

第三存储器 1302，用于存储能够在第三处理器 1303 上运行的计算机程序；

第三处理器 1303，用于在运行所述计算机程序时，执行：

在建立完成数据包的特征信息与应用标识之间的关联关系后，接收用户设备 UE 发送的有效时间消息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长；

在所述有效时长内，基于所述关联关系与所述 UE 进行加密数据流传输；

在所述加密数据流传输结束后，接收所述 UE 发送的释放指示消息；

基于所述释放指示消息释放所述关联关系。

可以理解地，本实施例中核心网设备 120 的具体硬件结构中的组成部分，与实施例四中的相应部分类似，在此不做赘述。

具体来说，核心网设备 120 中的第三处理器 1303，还配置为运行所述计算机程序时，执行前述实施例三中具体示例四所述的方法步骤，这里不再进行赘述。

实施例七

基于前述实施例相同的发明构思，参见图 14，其示出了本发明实施例提供的另一种 UE140 的组成，包括：消息发送部分 1401 和第二传输部分 1402，其中，所述消息发送部分 1401，配置为向核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长；

所述第二传输部分 1402，配置为在所述有效时长内，基于所述关联关系与所述核心网设备进行加密数据流传输；

所述消息发送部分 1401，还配置为向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

此外，本实施例还提供了一种计算机可读介质，该计算机可读介质存储有加密数据流的传输程序，所述加密数据流的传输程序被至少一个处理器执行时实现上述实施例三中具体示例四所述的方法的步骤。针对计算机可读介质的具体阐述，参见实施例四中的说明，在此不再赘述。

基于上述 UE140 的组成以及计算机可读介质，参见图 15，其示出了本发明实施例提供的 UE 140 的具体硬件结构，可以包括：第四网络接口 1501、第四存储器 1502 和第四处理器 1503；各个组件通过总线系统 1504 耦合在一起。可理解，总线系统 1504 用于实现这些组件之间的连接通信。总线系统 1504 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 15 中将各种总线都标为总线系统 1304。其中，所述第四网络接口 1501，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

第四存储器 1502，用于存储能够在第四处理器 1503 上运行的计算机程序；

第四处理器 1503，用于在运行所述计算机程序时，执行：

向核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长；

在所述有效时长内，基于所述关联关系与所述核心网设备进行加密数据流传输；

向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

可以理解地，本实施例中 UE 140 的具体硬件结构中的组成部分，与实施例四中的相应部分类似，在此不做赘述。

实施例八

基于前述实施例相同的发明构思，参见图 16、其示出了本发明实施例提供的一种加密流量的识别系统 160 组成，包括核心网设备 70 以及用户设备 90，其中，

所述用户设备 90，配置为发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备 70 进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识；

所述核心网设备 70，配置为接收用户设备 UE90 发送的承载有鉴权数据的数据包；

基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；

当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 90 发送的与所述应用标识对应的加密数据流进行识别。

具体实现过程中，本实施例中的核心网设备 70 可以优选为前述任一实施例中所述的核心网设备 70；而用户设备 90 则可以优选为前述任一实施例中所述的用户设备 90。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

工业实用性

本实施例中，核心网设备在 UE 与 OTT 服务器进行 TLS 握手过程中或握手完成后与 UE 进行鉴权，从而建立用于对加密数据流进行识别的关联关系，以实现对加密数据流的检测和统计，无需依赖明文标识，更无需进行复杂的 IP 地址配置和维护，提高了安全性并减少了配置和维护所需的计算资源。

权利要求书

1、一种加密数据流的识别方法，所述方法应用于核心网设备，所述方法包括:

接收用户设备 UE 发送的承载有鉴权数据的数据包;其中,所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识;

基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数;

当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别；所述数据包的特征信息可以包括以下至少一项或多项：网络协议 IP 源地址、IP 源端口号、IP 目的地址、IP 目的端口号、MAC 源地址、IP 源端口号、媒体接入控制 MAC 目的地址、MAC 目的端口号、协议类型以及虚拟局域网 VLAN 标签。

2、根据权利要求 1 所述的方法，其中，所述接收用户设备 UE 发送的承载有鉴权数据的数据包，包括:

在应用层会话建立的 TLS 握手过程中，所述核心网设备的用户面接收所述 UE 发送的首次 TLS 握手请求；其中，所述鉴权数据承载于所述首次 TLS 握手请求中的明文字段。

3、根据权利要求 2 所述的方法，其中，在接收用户设备 UE 发送的承载有鉴权数据的数据包后，所述方法还包括:

所述核心网设备的用户面从所述首次 TLS 握手请求中的明文字段检测到所述鉴权数据后,将所述鉴权数据传输至所述核心网设备的控制面。

4、根据权利要求 1 所述的方法，其中，所述接收用户设备 UE 发送的承载有鉴权数据的数据包，包括:

在完成 TLS 握手后,所述核心网设备的用户面接收所述 UE 通过基站发送的鉴权请求;其中,所述鉴权数据承载于所述鉴权请求中的 GTP-U 扩展字段。

5、根据权利要求 4 所述的方法，其中，在接收用户设备 UE 发送的承载有鉴权数据的数据包后，所述方法还包括：所述核心网设备的用户面从鉴权请求中的 GTP-U 扩展字段检测到所述鉴权数据后，将所述鉴权数据传输至所述核心网设备的控制面。

6、根据权利要求 2 至 4 任一项所述的方法，其中，所述第一鉴权参数包括随机数；所述第二鉴权参数包括公共密钥 Ka。

7、根据权利要求 2 至 4 任一项所述的方法，其中，所述基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果，包括:

所述核心网设备的控制面基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果。

8、根据权利要求 2 至 4 任一项所述的方法，其中，当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系，包括:

当所述第二鉴权结果与所述第一鉴权结果比对一致时，所述核心网设备的控制面将比对结果传输至所述核心网用户面;

所述核心网设备的用户面建立所述数据包的特征信息与所述应用标识之间的关联关系。

9、根据权利要求 1 所述的方法，其中，所述接收用户设备 UE 发送的承载有鉴权数据的数据包，包括:

在完成 TLS 握手后，所述核心网设备的控制面接收所述 UE 发送的非接入层会话管理 NAS-SM 消息；其中，所述 NAS-SM 消息的扩展字段中包括：第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征信息；其中，所述第一鉴权参数包括：随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

10、根据权利要求 9 所述的方法，其中，所述基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果，包括:

所述核心网设备的控制面根据所述第一鉴权参数中的随机数以及所述第二鉴权参数中的公共密钥按照设定的鉴权算法获得第二鉴权结果。

11、根据权利要求 9 或 10 所述的方法，其中，当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系，包括:

当所述第二鉴权结果与所述第一鉴权结果比对一致时，所述核心网设备的控制面根据所述 OTT 服务器的特征信息以及所述 UE 的特征信息生成所述数据包的特征信息，并将生成的数据包的特征信息和所述应用标识传输至所述核心网设备的用户面；其中，所述 UE 的特征信息包括: UE 的 IP 地址、端口和 MAC 地址;

所述核心网设备的用户面建立所述生成的数据包的特征信息和所述应用标识之间的关联关系。

12、根据权利要求 1 所述的方法，其中，所述基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果后，所述方法还包括:

所述核心网设备的控制面通过所述核心网设备的用户面将所述第二鉴权结果与所述第一鉴权结果的比对结果发送至所述 UE。

13、根据权利要求 1 至 12 任一项所述的方法，其中，所述方法还包括:

接收所述 UE 发送的有效时间信息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长。

14、根据权利要求 13 所述的方法，其中，所述方法还包括:

当所述有效时长计时完毕后，若加密数据流传输未完成，释放所述关联关系。

15、根据权利要求 14 所述的方法，其中，所述方法还包括:

在所述有效时长内或所述有效时长结束，接收所述 UE 发送的释放指示消息;

基于所述释放指示消息释放所述关联关系。

16、一种加密数据流的传输方法，所述方法应用于核心网设备，所述方法包括:

在建立完成数据包的特征信息与应用标识之间的关联关系后，接收用户设备 UE 发送的有效时间消息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长;

在所述有效时长内，基于所述关联关系与所述 UE 进行加密数据流传输;

接收所述 UE 发送的释放指示消息;

基于所述释放指示消息释放所述关联关系。

17、根据权利要求 16 所述的方法，其中，所述方法还包括:

在所述有效时长计时完毕后，释放所述关联关系；或者，

在所述有效时长计时完毕后，继续与所述 UE 进行加密数据流传输，直至所述加密数据流传输结束后释放所述关联关系。

18、一种加密数据流的识别方法，所述方法应用于用户设备 UE，所述方法包括:

发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括: 第一鉴权参数、第一鉴权结果以及应用标识。

19、根据权利要求 18 所述的方法，其中，所述发送承载有鉴权数据的数据包，包括:

在应用层会话建立的 TLS 握手过程中，将所述鉴权数据承载于首次 TLS 握手请求中的明文字段;

将所述承载有所述鉴权数据的首次 TLS 握手请求通过核心网设备的用户面透传至所述核心网设备的控制面。

20、根据权利要求 18 所述的方法，其中，所述发送承载有鉴权数据的数据包，包括:

在完成 TLS 握手后，将所述鉴权数据承载于扩展的 PDCP 字段的鉴权请求发送至基站，并通过基站将 PDCP 扩展字段中的鉴权数据转换成 GTP-U 扩展字段后，将所述鉴权请求继续发送至所述核心网设备用户面。

21、根据权利要求 18 所述的方法，其中，所述发送承载有鉴权数据的数据包，包括:

在完成 TLS 握手后，向核心网设备的控制面发送非接入层会话管理 NAS-SM 消息；其中，所述 NAS-SM 消息的扩展字段中包括: 第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征信息；其中，所述第一鉴权参数包括: 随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

22、根据权利要求 18 所述的方法，其中，所述方法还包括:

接收核心网设备的控制面回复的鉴权结果。

23、根据权利要求 18 至 22 任一项所述的方法，其中，所述方法还包括:

向所述核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息

与应用标识之间的关联关系进行加密数据流识别的有效时长。

24、根据权利要求 18 至 22 任一项所述的方法，其中，所述方法还包括:

向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

25、一种加密数据流的传输方法，所述方法应用于用户设备 UE，所述方法包括:

向核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长;

在所述有效时长内，基于所述关联关系与所述核心网设备进行加密数据流传输;

向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

26、一种核心网设备，包括：第一接收部分、鉴权部分和建立部分；其中，

所述第一接收部分，配置为接收用户设备 UE 发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识;

所述鉴权部分，配置为基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数;

所述建立部分，配置为当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述 UE 发送的与所述应用标识对应的加密数据流进行识别；所述数据包的特征信息可以包括以下至少一项或多项：网络协议 IP 源地址、IP 源端口号、IP 目的地址、IP 目的端口号、MAC 源地址、IP 源端口号、媒体接入控制 MAC 目的地址、MAC 目的端口号、协议类型以及虚拟局域网 VLAN 标签。

27、根据权利要求 26 所述的核心网设备，其中，所述第一接收部分，配置为在应用层会话建立的 TLS 握手过程中，接收所述 UE 发送的首次 TLS 握手请求；其中，所述鉴权数据承载于所述首次 TLS 握手请求中的明文字段。

28、根据权利要求 26 所述的核心网设备，其中，所述第一接收部分，配置为：在完成 TLS 握手后，所述核心网设备的用户面接收所述 UE 通过基站发送的鉴权请求；其中，所述鉴权数据承载于所述鉴权请求中的 GTP-U 扩展字段。

29、根据权利要求 26 所述的核心网设备，其中，所述第一接收部分，配置为在完成 TLS 握手后，所述核心网设备的控制面接收所述 UE 发送的非接入层会话管理 NAS-SM 消息；其中，所述 NAS-SM 消息的扩展字段中包括：第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征信息；其中，所述第一鉴权参数包括：随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

30、根据权利要求 29 所述的核心网设备，其中，所述鉴权部分，配置为根据所述第一鉴权参数中的随机数以及所述第二鉴权参数中的公共密钥按照设定的鉴权算法获得第二鉴权结果。

31、根据权利要求 29 或 30 所述的核心网设备，其中，所述建立部分，配置为:

当所述第二鉴权结果与所述第一鉴权结果比对一致时，根据所述 OTT 服务器的特征信息以及所述 UE 的特征信息生成所述数据包的特征信息，并建立所述生成的数据包的特征信息和所述应用标识之间的关联关系；其中，UE 的特征信息包括：UE 的 IP 地址、端口和 MAC 地址。

32、根据权利要求 26 所述的核心网设备，其中，所述核心网设备还包括第一发送部分，配置为将所述第二鉴权结果与所述第一鉴权结果的比对结果发送至所述 UE。

33、根据权利要求 26 至 32 任一项所述的核心网设备，其中，所述第一接收部分，还配置为接收所述 UE 发送的有效时间信息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长。

34、根据权利要求 33 所述的核心网设备，其中，所述核心网设备还包括控制部分，配置为当所述有效时长计时完毕后，若加密数据流传输未完成，释放所述关联关系。

35、根据权利要求 34 所述的核心网设备，其中，所述第一接收部分，还配置为加密数据流传输完毕后，接收所述 UE 发送的释放指示消息;

所述控制部分，还配置为基于所述释放指示消息释放所述关联关系。

36、一种核心网设备，包括：消息接收部分、第一传输部分和控制部分；其中，所述消息接收部分，配置为在建立完成数据包的特征信息与应用标识之间的关联关系后，接收用户设备 UE 发送的有效时间消息；其中，所述有效时间信息用于指示所述关联关系进行加密数据流识别的有效时长;

所述第一传输部分，配置为在所述有效时长内，基于所述关联关系与所述 UE 进行加密数据流传输;

所述消息接收部分，还配置为接收所述 UE 发送的释放指示消息；

所述控制部分，配置为基于所述释放指示消息释放所述关联关系。

37、根据权利要求 36 所述的核心网设备，其中，所述控制部分，还配置为在所述有效时长计时完毕后，释放所述关联关系；或者，

在所述有效时长计时完毕后，继续与所述 UE 进行加密数据流传输，直至所述加密数据流传输结束后释放所述关联关系。

38、一种用户设备 UE，其中，所述 UE 包括：第二发送部分，配置为发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识。

39、根据权利要求 38 所述的 UE，其中，所述第二发送部分，配置为：在应用层会话建立的 TLS 握手过程中，将所述鉴权数据承载于首次 TLS 握手请求中的明文字段；

将所述承载有所述鉴权数据的首次 TLS 握手请求通过核心网设备的用户面透传至所述核心网设备的控制面。

40、根据权利要求 38 所述的 UE，其中，所述第二发送部分，配置为：在完成 TLS 握手后，将所述鉴权数据承载于扩展的 PDCP 字段的鉴权请求发送至基站，并通过基站将 PDCP 扩展字段中的鉴权数据转换成 GTP-U 扩展字段后，将所述鉴权请求继续发送至所述核心网设备用户面。

41、根据权利要求 38 所述的 UE，其中，所述第二发送部分，配置为：在完成 TLS 握手后，向核心网设备的控制面发送非接入层会话管理 NAS-SM 消息；其中，所述 NAS-SM 消息的扩展字段中包括：第一鉴权参数、第一鉴权结果、应用标识以及所述 NAS-SM 消息的特征消息；其中，所述第一鉴权参数包括：随机数和公共密钥 Ka；所述 NAS-SM 消息的特征信息包括 OTT 服务器的 IP 地址、端口号、协议类型和 OTT 服务器的 MAC 地址。

42、根据权利要求 38 所述的 UE，其中，所述 UE 还包括第二接收部分，配置为接收核心网设备的控制面回复的鉴权结果。

43、根据权利要求 38 至 42 任一项所述的 UE，其中，所述第二发送部分，还配置为向所述核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长。

44、根据权利要求 38 至 42 任一项所述的 UE，其中，所述第二发送部分，还配置为向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

45、一种 UE，所述 UE 包括：消息发送部分和第二传输部分，其中，所述消息发送部分，配置为向核心网设备发送有效时间消息；其中，所述有效时间信息用于指示数据包的特征信息与应用标识之间的关联关系进行加密数据流识别的有效时长；

所述第二传输部分，配置为在所述有效时长内，基于所述关联关系与所述核心网设备进行加密数据流传输；

所述消息发送部分，还配置为向所述核心网设备发送释放指示消息；其中，所述释放指示消息用于释放所述关联关系。

46、一种核心网设备，包括：第一网络接口，第一存储器和第一处理器；其中，

所述第一网络接口，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

所述第一存储器，用于存储能够在所述第一处理器上运行的计算机程序；

所述第一处理器，用于在运行所述计算机程序时，执行权利要求 1 至 15 任一项或者权利要求 16 至 17 任一项所述方法的步骤。

47、一种用户设备 UE，其中，所述 UE 包括：第二网络接口、第二存储器和第二处理器；

其中，所述第二网络接口，用于在与其他外部网元之间进行收发信息过程中，信号的接收和发送；

所述第二存储器，用于存储能够在第二处理器上运行的计算机程序；

所述第二处理器，用于在运行所述计算机程序时，执行权利要求 18 至 24 任一项或权利要求 25 所述方法的步骤。

48、一种计算机可读介质，所述计算机可读介质存储有加密数据流的识别程序，所述加密数据流的识别程序被至少一个处理器执行时实现权利要求 1 至 15 任一项或者权利要求 18 至 24 任一项所述的方法的步骤。

49、一种计算机可读介质，所述计算机可读介质存储有加密数据流的传输程序，所述加密数据流的传输程序被至少一个处理器执行时实现权利要求 16 至 17 任一项或者权利要求 25 所述的

方法的步骤。

50、一种加密流量的识别系统，包括核心网设备以及用户设备，其中，

所述用户设备，配置为发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识；

所述核心网设备，配置为接收用户设备UE发送的承载有鉴权数据的数据包；

基于所述第一鉴权参数和第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果；其中，所述第二鉴权参数为预存的所述应用标识对应的鉴权参数；

当所述第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的特征信息与所述应用标识之间的关联关系；其中，所述关联关系用于后续对所述UE发送的与所述应用标识对应的加密数据流进行识别。

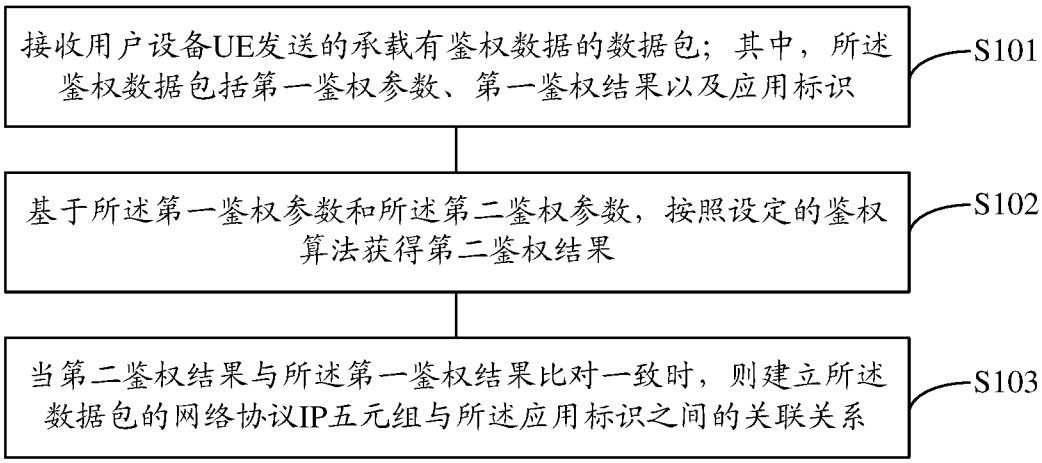
接收用户设备UE发送的承载有鉴权数据的数据包；其中，所述鉴权数据包括第一鉴权参数、第一鉴权结果以及应用标识
S101
基于所述第一鉴权参数和所述第二鉴权参数，按照设定的鉴权算法获得第二鉴权结果
S102
当第二鉴权结果与所述第一鉴权结果比对一致时，则建立所述数据包的网络协议IP五元组与所述应用标识之间的关联关系
S103

图 1

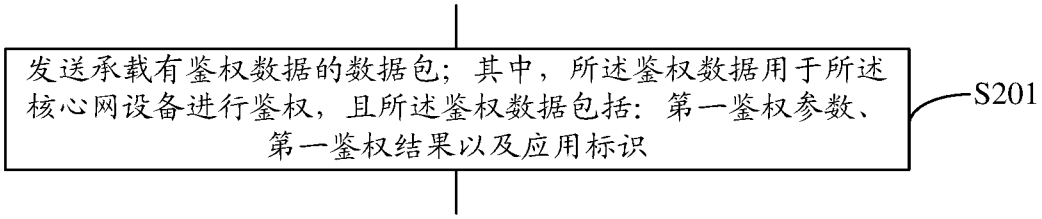
发送承载有鉴权数据的数据包；其中，所述鉴权数据用于所述核心网设备进行鉴权，且所述鉴权数据包括：第一鉴权参数、第一鉴权结果以及应用标识
S201

图 2

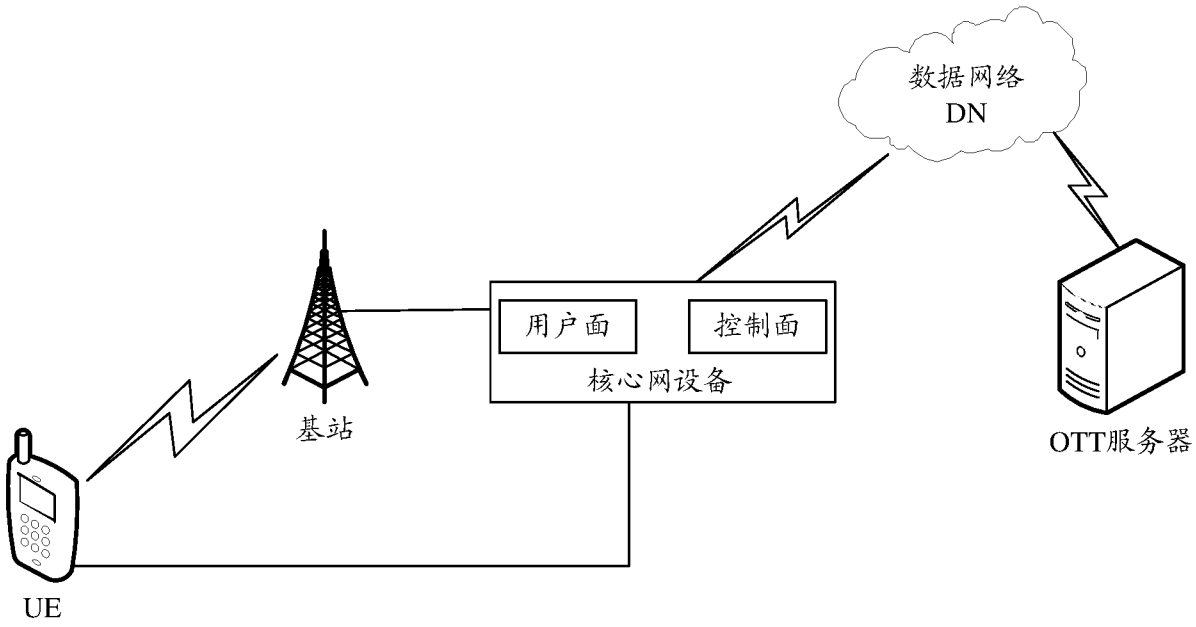
数据网络
DN
用户面
控制面
核心网设备
基站
UE
OTT服务器

图 3

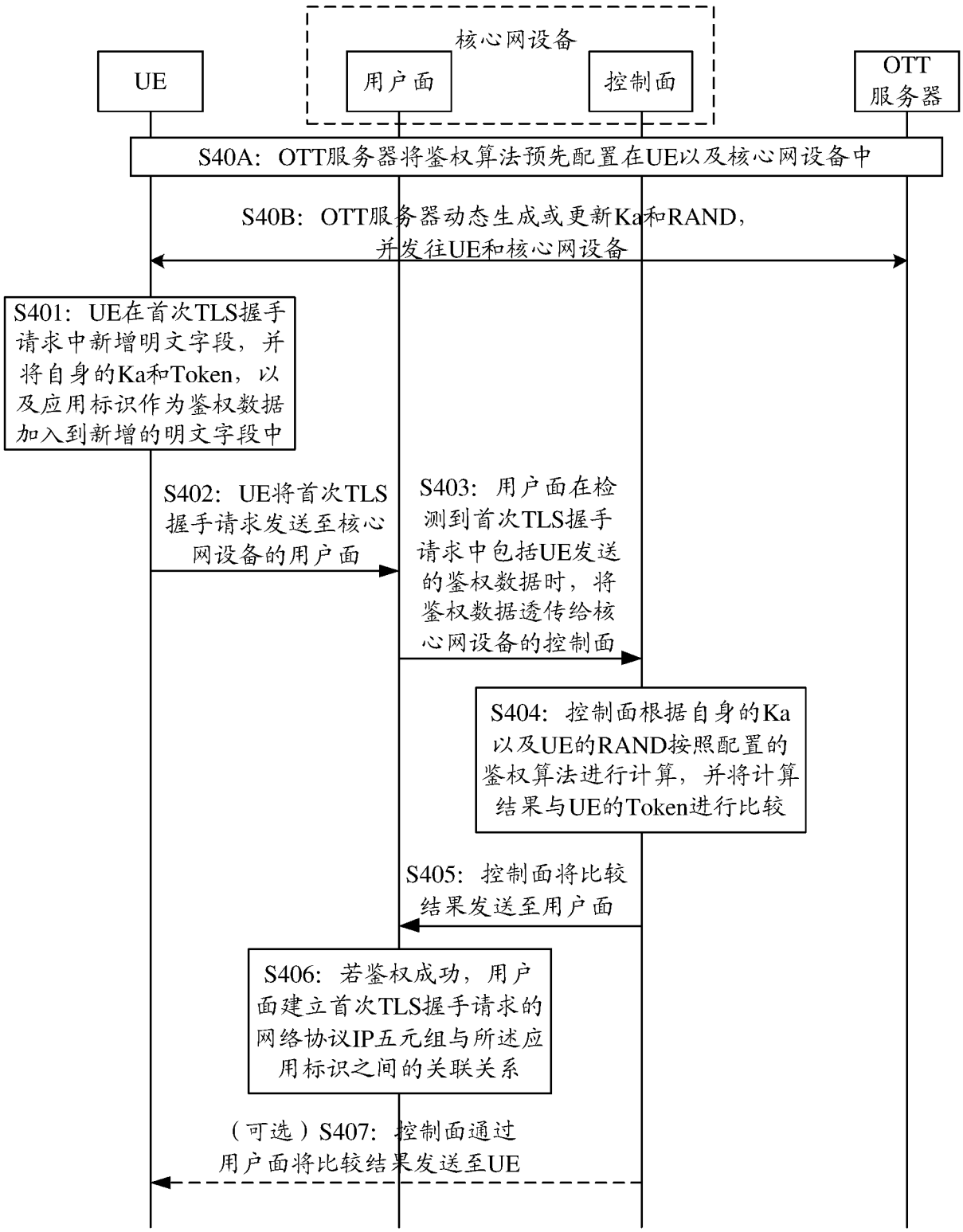
核心网设备
UE
用户面
控制面
OTT
服务器
S40A：OTT服务器将鉴权算法预先配置在UE以及核心网设备中
S40B：OTT服务器动态生成或更新Ka和RAND，
并发往UE和核心网设备
S401：UE在首次TLS握手请求中新增明文字段，并将自身的Ka和Token，以及应用标识作为鉴权数据加入到新增的明文字段中
S402：UE将首次TLS握手请求发送至核心网设备的用户面
S403：用户面在检测到首次TLS握手请求中包括UE发送的鉴权数据时，将鉴权数据透传给核心网设备的控制面
S404：控制面根据自身的Ka以及UE的RAND按照配置的鉴权算法进行计算，并将计算结果与UE的Token进行比较
S405：控制面将比较结果发送至用户面
S406：若鉴权成功，用户面建立首次TLS握手请求的网络协议IP五元组与所述应用标识之间的关联关系
（可选）S407：控制面通过用户面将比较结果发送至UE

图 4

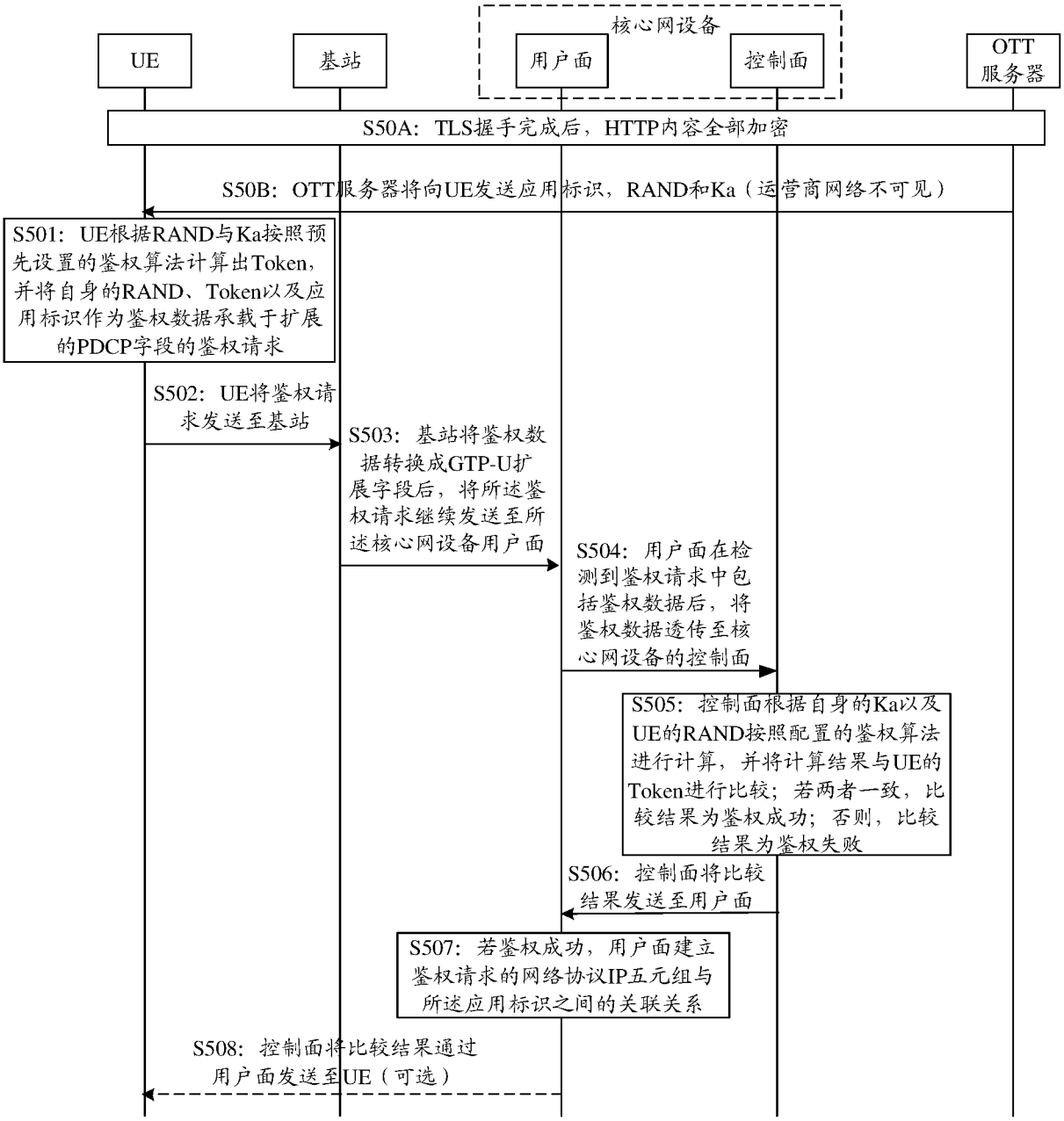
核心网设备
UE
基站
用户面
控制面
OTT
服务器
S50A：TLS握手完成后，HTTP内容全部加密
S50B：OTT服务器将向UE发送应用标识，RAND和Ka（运营商网络不可见）
S501：UE根据RAND与Ka按照预先设置的鉴权算法计算出Token，并将自身的RAND、Token以及应用标识作为鉴权数据承载于扩展的PDCP字段的鉴权请求
S502：UE将鉴权请求发送至基站
S503：基站将鉴权数据转换成GTP-U扩展字段后，将所述鉴权请求继续发送至所述核心网设备用户面
S504：用户面在检测到鉴权请求中包括鉴权数据后，将鉴权数据透传至核心网设备的控制面
S505：控制面根据自身的Ka以及UE的RAND按照配置的鉴权算法进行计算，并将计算结果与UE的Token进行比较；若两者一致，比较结果为鉴权成功；否则，比较结果为鉴权失败
S506：控制面将比较结果发送至用户面
S507：若鉴权成功，用户面建立鉴权请求的网络协议IP五元组与所述应用标识之间的关联关系
S508：控制面将比较结果通过用户面发送至UE（可选）

图 5

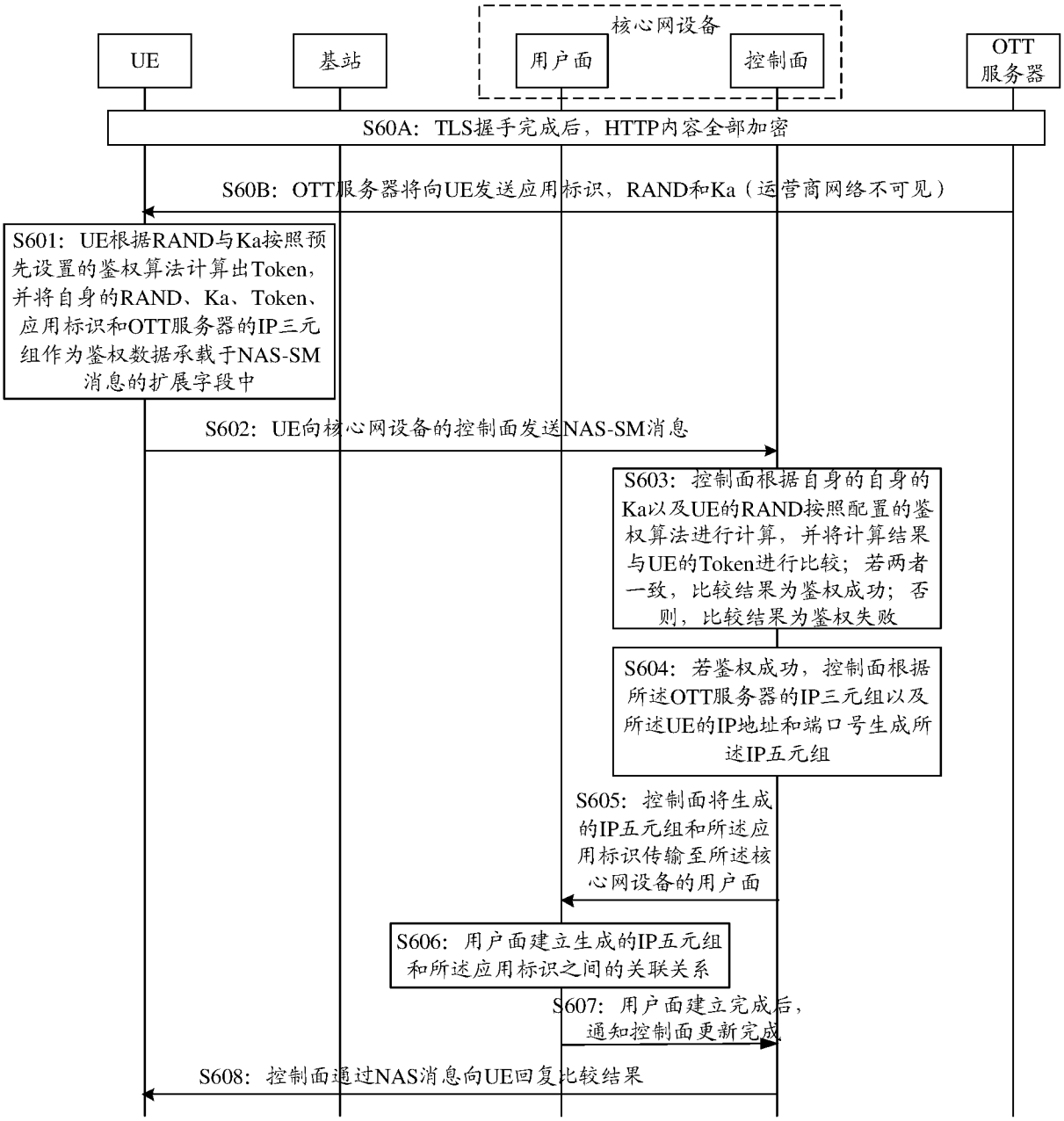
核心网设备
UE
基站
用户面
控制面
OTT
服务器
S60A：TLS握手完成后，HTTP内容全部加密
S60B：OTT服务器将向UE发送应用标识，RAND和Ka（运营商网络不可见）
S601：UE根据RAND与Ka按照预先设置的鉴权算法计算出Token，并将自身的RAND、Ka、Token、应用标识和OTT服务器的IP三元组作为鉴权数据承载于NAS-SM消息的扩展字段中
S602：UE向核心网设备的控制面发送NAS-SM消息
S603：控制面根据自身的自身的Ka以及UE的RAND按照配置的鉴权算法进行计算，并将计算结果与UE的Token进行比较；若两者一致，比较结果为鉴权成功；否则，比较结果为鉴权失败
S604：若鉴权成功，控制面根据所述OTT服务器的IP三元组以及所述UE的IP地址和端口号生成所述IP五元组
S605：控制面将生成的IP五元组和所述应用标识传输至所述核心网设备的用户面
S606：用户面建立生成的IP五元组和所述应用标识之间的关联关系
S607：用户面建立完成后，通知控制面更新完成
S608：控制面通过NAS消息向UE回复比较结果

图 6A

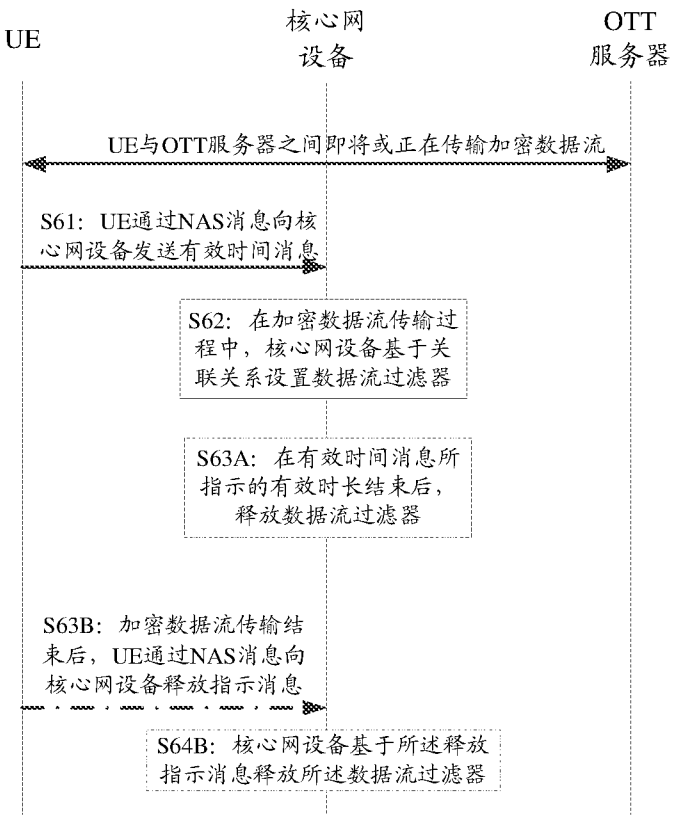
UE
核心网
设备
OTT
服务器
UE与OTT服务器之间即将或正在传输加密数据流
S61：UE通过NAS消息向核心网设备发送有效时间消息
S62：在加密数据流传输过程中，核心网设备基于关联关系设置数据流过滤器
S63A：在有效时间消息所指示的有效时长结束后，释放数据流过滤器
S63B：加密数据流传输结束后，UE通过NAS消息向核心网设备释放指示消息
S64B：核心网设备基于所述释放指示消息释放所述数据流过滤器

图 6B

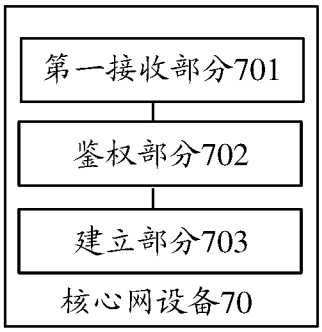
第一接收部分701
鉴权部分702
建立部分703
核心网设备70

图 7A

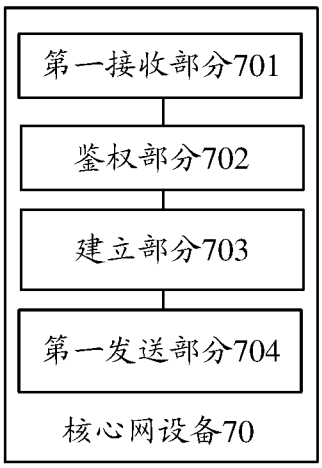
第一接收部分701
鉴权部分702
建立部分703
第一发送部分704
核心网设备70

图 7B

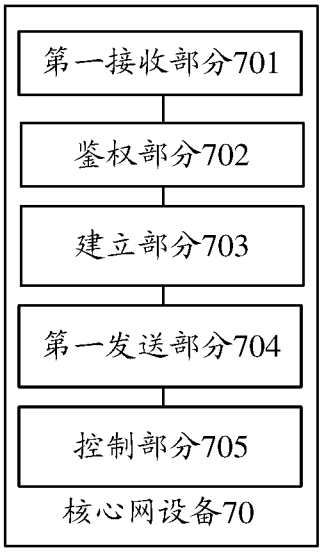
第一接收部分701
鉴权部分702
建立部分703
第一发送部分704
控制部分705
核心网设备70

图 7C

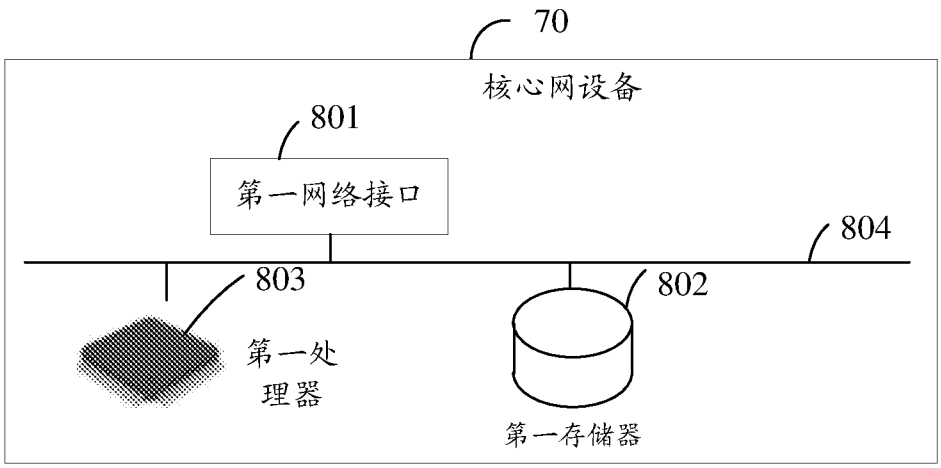
70
核心网设备
801
第一网络接口
804
803
802
第一处理器
第一存储器

图 8

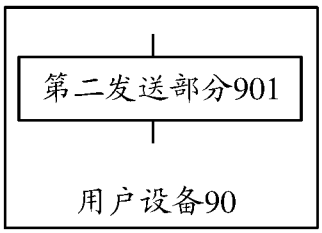
第二发送部分901
用户设备90

图 9

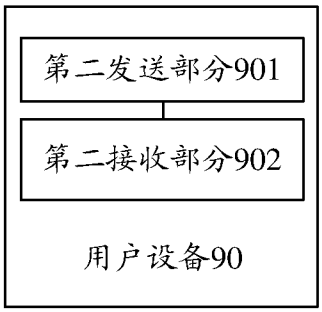
第二发送部分901
第二接收部分902
用户设备90

图 10

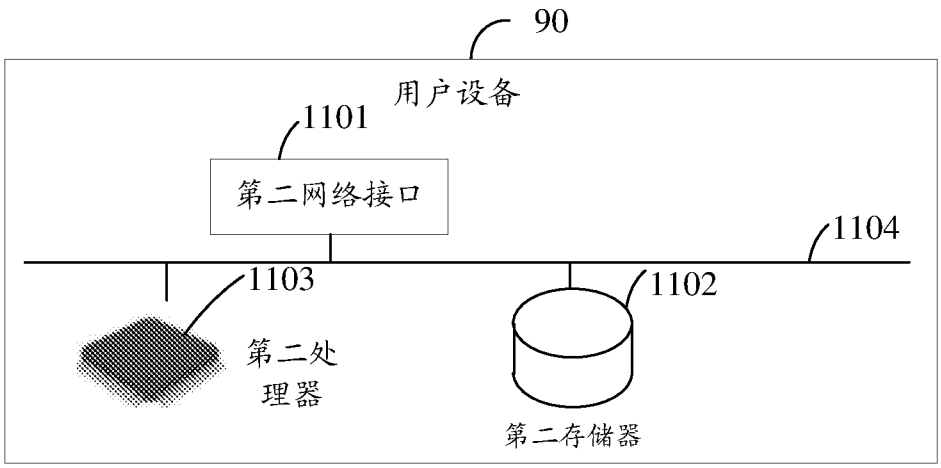

图 11

图 12

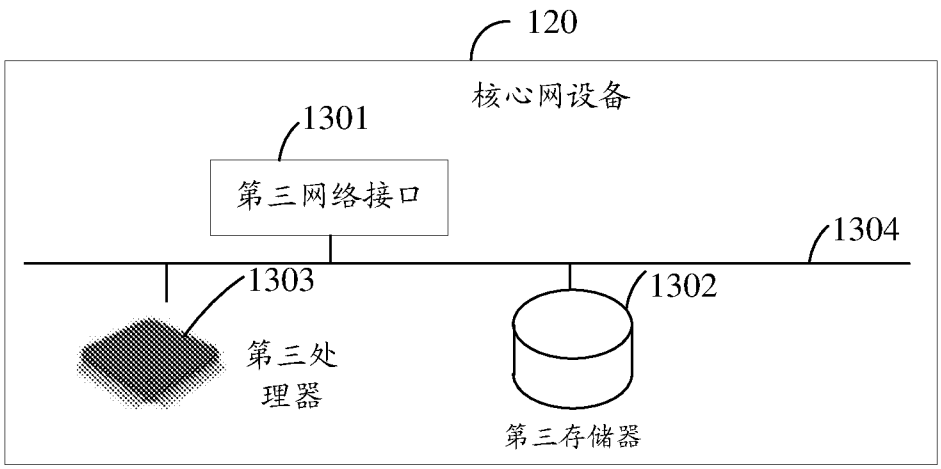

图 13

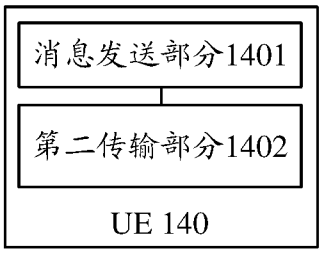

图 14

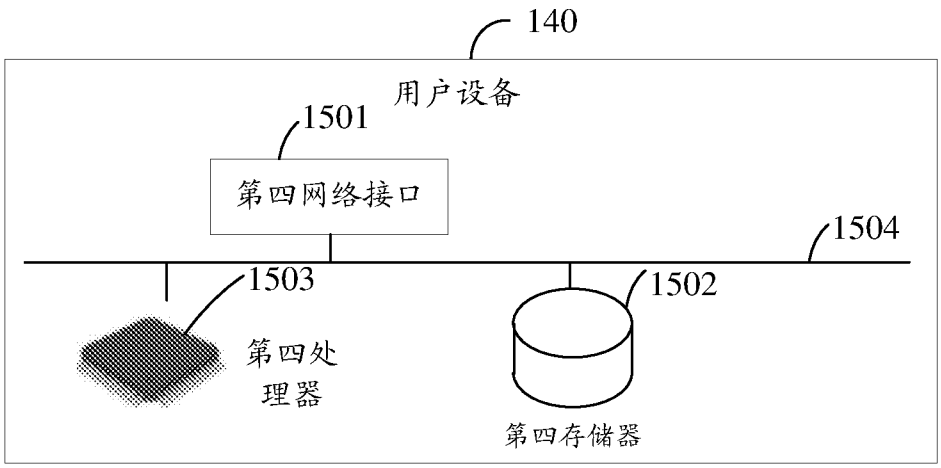
140
用户设备
1501
第四网络接口
1504
1503
1502
第四处理器
第四存储器

图 15

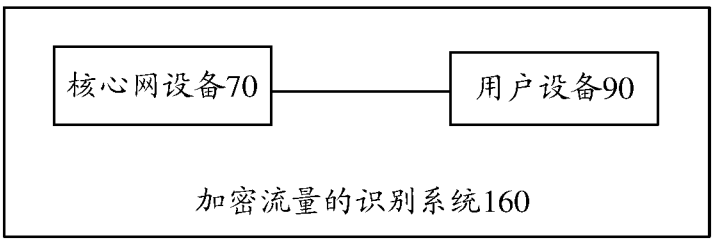
核心网设备70
用户设备90
加密流量的识别系统160

图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/081774

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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)

H04L, H04W, H04Q

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)

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 加密, 数据流, 识别, 票据, 核心网, 核心层, 应用, 标识, APP ID, 应用ID, 关联, 绑定, 对应, 关系, 建立, 生成, 生存时间, 有效时间, 有效时长, 生存期, 释放, 注销, 特征, 控制层, 匹配, 验证, 预设, 客户端, UE, token, TLS, OTT, application, ID, recogni +, traffic, flow, data packet, identification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 101714952 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 26 May 2010 (26.05.2010), description, paragraphs [0071] and [0072]	1-15, 26-35, 46, 50
Y	US 2016262021 A1 (QUALCOMM INC.) 08 September 2016 (08.09.2016), description, paragraphs [0029] and [0078]-[0095]	1-15, 23, 24, 26-35, 43, 44, 46, 50
Y	CN 103428643 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) 04 December 2013 (04.12.2013), description, paragraphs [0059] and [0078]-[0080]	13-15, 23, 24, 33-35, 43, 44
X	US 2016262021 A1 (QUALCOMM INC.) 08 September 2016 (08.09.2016), description, paragraphs [0029] and [0078]-[0095]	18-22, 38-42, 47, 48
X	CN 103428643 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) 04 December 2013 (04.12.2013), description, paragraphs [0059] and [0078]-[0080]	16, 17, 25, 36, 37, 45-47, 49

☒ 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
31 May 2018	25 June 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 TAN, Meiling Telephone No. (86-20) 28950742

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/081774

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 105915396 A (CHINA UNICOM GROUP CO., LTD.) 31 August 2016 (31.08.2016), entire document	1-50
A	US 2008307518 A1 (NOKIA CORPORATION) 11 December 2008 (11.12.2008), entire document	1-50

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/081774

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101714952 A	26 May 2010	CN 101714952 B	07 March 2012
US 2016262021 A1	08 September 2016	AU 2016229439 A1	10 August 2017
		EP 3266180 A1	10 January 2018
		US 9717003 B2	25 July 2017
		US 2017230829 A1	10 August 2017
		KR 101819878 B1	28 February 2018
		KR 20170106490 A	20 September 2017
		TW 201644250 A	16 December 2016
		WO 2016144516 A1	15 September 2016
		KR 20180004310 A	10 January 2018
		US 9769665 B2	19 September 2017
		CN 107431701 A	01 December 2017
		IN 201727024949 A	08 September 2017
		TW 616084 B1	21 February 2018
CN 103428643 A	04 December 2013	None	
CN 105915396 A	31 August 2016	None	
US 2008307518 A1	11 December 2008	WO 2008152201 A1	18 December 2008
		US 8875236 B2	28 October 2014

国际检索报告

国际申请号
PCT/CN2018/081774

A. 主题的分类

H04L 29/06(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)

H04L,H04W,H04Q

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））

CNABS;CNTXT;CNKI;VEN;USTXT;EPTXT;WOTXT:加密，数据流，识别，票据，核心网，核心层，应用，标识，APP ID，应用ID，关联，绑定，对应，关系，建立，生成，生存时间，有效时间，有效时长，生存期，释放，注销，特征，控制层，匹配，验证，预设，客户端，UE，token，TLS，OTT，application，ID，recogni+，traffic，flow，data packet，identification

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
Y	CN 101714952 A (北京邮电大学) 2010年 5月 26日 (2010-05-26) 说明书[0071]-[0072]段	1-15、26-35、46、50
Y	US 2016262021 A1 (QUALCOMM INC) 2016年 9月 8日 (2016-09-08) 说明书第[0029]、[0078]-[0095]段	1-15、23-24、26-35、43-44、46、50
Y	CN 103428643 A (大唐移动通信设备有限公司) 2013年 12月 4日 (2013-12-04) 说明书第[0059]、[0078]-[0080]段	13-15、23-24、33-35、43-44
X	US 2016262021 A1 (QUALCOMM INC) 2016年 9月 8日 (2016-09-08) 说明书第[0029]、[0078]-[0095]段	18-22、38-42、47-48
X	CN 103428643 A (大唐移动通信设备有限公司) 2013年 12月 4日 (2013-12-04) 说明书第[0059]、[0078]-[0080]段	16-17、25、36-37、45-47、49
A	CN 105915396 A (中国联合网络通信集团有限公司) 2016年 8月 31日 (2016-08-31) 全文	1-50
A	US 2008307518 A1 (NOKIA CORP) 2008年 12月 11日 (2008-12-11) 全文	1-50

☐ 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
2018年 5月 31日	2018年 6月 25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 谭美玲 电话号码 86-(20)-28950742

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/081774

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	101714952	A	2010年 5月 26日	CN	101714952	B	2012年 3月 7日
US	2016262021	A1	2016年 9月 8日	AU	2016229439	A1	2017年 8月 10日
				EP	3266180	A1	2018年 1月 10日
				US	9717003	B2	2017年 7月 25日
				US	2017230829	A1	2017年 8月 10日
				KR	101819878	B1	2018年 2月 28日
				KR	20170106490	A	2017年 9月 20日
				TW	201644250	A	2016年 12月 16日
				WO	2016144516	A1	2016年 9月 15日
				KR	20180004310	A	2018年 1月 10日
				US	9769665	B2	2017年 9月 19日
				CN	107431701	A	2017年 12月 1日
				IN	201727024949	A	2017年 9月 8日
				TW	616084	B1	2018年 2月 21日
CN	103428643	A	2013年 12月 4日		无		
CN	105915396	A	2016年 8月 31日		无		
US	2008307518	A1	2008年 12月 11日	WO	2008152201	A1	2008年 12月 18日
				US	8875236	B2	2014年 10月 28日