(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107135190 B
(45)授权公告日 2021.01.15

(21)申请号 201610113560.7

(22)申请日 2016.02.29

(65)同一申请的已公布的文献号
申请公布号 CN 107135190 A

(43)申请公布日 2017.09.05

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 石磊

(74)专利代理机构 北京清源汇知识产权代理事务所(特殊普通合伙) 11644
代理人 冯德魁

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 104322001 A,2015.01.28
CN 101399721 A,2009.04.01
CN 101420336 A,2009.04.29
US 2013322626 A1,2013.12.05
US 9124629 B1,2015.09.01
US 2010325419 A1,2010.12.23

审查员 张俊锋

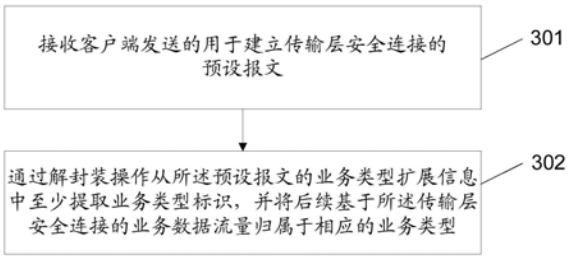
权利要求书6页 说明书20页 附图3页

(54)发明名称

基于传输层安全连接的数据流量归属识别方法及装置

(57)摘要

本申请公开了一种基于传输层安全连接的数据流量归属识别方法及装置,同时公开了一种基于传输层安全连接的业务类型提供方法及装置,以及一种基于传输层安全连接的数据流量归属识别系统。所述基于传输层安全连接的数据流量归属识别方法,包括:接收客户端发送的用于建立传输层安全连接的预设报文;通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识,并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。采用本申请提供的技术方案,可以简化数据业务提供方的操作,也为运营商的运维配置管理提供便利,而且还可以实现不同粒度的流量归属识别,与传统基于SNI的流量归属识别方法相比更为灵活。



CN 107135190 B

1.一种基于传输层安全连接的数据流量归属识别方法,其特征在于,所述方法在业务接入网关中实施,包括:

接收客户端发送的用于建立传输层安全连接的预设报文;

通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识和消息认证码,至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥,采用与所述客户端相同的预设散列算法计算本地消息认证码;判断所述本地消息认证码与所述提取的消息认证码是否一致;并在一致时,将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型;

其中,所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方,并预先指定给所述客户端;所述客户端存储的、与预先指定给其的业务类型标识相对应的密钥,与所述业务接入网关存储的相应信息保持同步。

2.根据权利要求1所述的基于传输层安全连接的数据流量归属识别方法,其特征在于,所述传输层安全连接包括:TLS连接。

3.根据权利要求1所述的基于传输层安全连接的数据流量归属识别方法,其特征在于,所述预设报文包括:client hello报文;

所述通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识,包括:通过解封装操作,从client hello报文的扩展数据块中提取业务类型扩展信息,并从所述业务类型扩展信息中至少提取所述业务类型标识。

4.根据权利要求1所述的基于传输层安全连接的数据流量归属识别方法,其特征在于,所述客户端存储的、与预先指定给其的业务类型标识相对应的密钥,与所述业务接入网关存储的相应信息保持同步,通过以下方式实现:

所述客户端从所述数据业务提供方的密钥中心获取、并且仅获取与预先指定给其的业务类型标识相对应的密钥,并存储于客户端;

所述业务接入网关从所述运营方的密钥中心获取与预先指定给所述客户端的业务类型标识相对应的密钥,并存储于业务接入网关;

所述数据业务提供方的密钥中心存储的业务类型标识及对应密钥,与所述运营方的密钥中心存储的相应信息保持同步。

5.根据权利要求1所述的基于传输层安全连接的数据流量归属识别方法,其特征在于,所述对应于所述业务类型标识的密钥数量为两个或者两个以上;

从所述预设报文的业务类型扩展信息中提取的信息还包括:密钥标识;

所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥,采用与所述客户端相同的预设散列算法计算本地消息认证码;包括:

根据提取的所述密钥标识,从本地存储的、对应于所述业务类型标识的各密钥中选取相应密钥;

至少根据所述业务类型标识和所选密钥,采用与所述客户端相同的预设散列算法计算本地消息认证码。

6.根据权利要求5所述的基于传输层安全连接的数据流量归属识别方法,其特征在于,从所述预设报文的业务类型扩展信息中提取的信息还包括:时间戳;

所述至少根据所述业务类型标识和所选密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码，包括：根据所述业务类型标识、所选密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

当所述判断所述本地消息认证码与所述提取的消息认证码是否一致的结果为一致时，包括：获取系统时间；通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

其中，所述系统时间与所述客户端的系统时间保持同步。

7.根据权利要求1所述的基于传输层安全连接的数据流量归属识别方法，其特征在于，从所述预设报文的业务类型扩展信息中提取的信息还包括：时间戳；

所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码，包括：根据所述业务类型标识、所述对应于所述业务类型标识的密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

当所述判断所述本地消息认证码与所述提取的消息认证码是否一致的结果为一致时，包括：获取系统时间；通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

其中，所述系统时间与所述客户端的系统时间保持同步。

8.根据权利要求1-7任一项所述的基于传输层安全连接的数据流量归属识别方法，其特征在于，所述客户端包括：OTT业务客户端。

9.一种基于传输层安全连接的数据流量归属识别装置，其特征在于，所述装置部署于业务接入网关，包括：

预设报文接收单元，用于接收客户端发送的用于建立传输层安全连接的预设报文；

业务类型标识提取单元，包括：信息提取子单元，用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识和消息认证码，本地消息认证码计算子单元，至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码；认证码比对子单元，判断所述本地消息认证码与所述提取的消息认证码是否一致；流量归属识别子单元，用于当所述认证码比对子单元的输出为是时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端；网关密钥同步单元，所述客户端存储的、与预先指定给其的业务类型标识相对应的密钥，与所述业务接入网关存储的相应信息保持同步。

10.根据权利要求9所述的基于传输层安全连接的数据流量归属识别装置，其特征在于，所述业务类型标识提取单元，具体用于通过解封装操作，从client hello报文的扩展数据块中提取业务类型扩展信息，从所述业务类型扩展信息中至少提取所述业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

11.根据权利要求9所述的基于传输层安全连接的数据流量归属识别装置，其特征在

于，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码和密钥标识；

所述本地消息认证码计算子单元，包括：

接入侧密钥选取子单元，用于根据提取的所述密钥标识，从本地存储的、对应于所述业务类型标识的各密钥中选取相应密钥；

接入侧计算执行子单元，用于至少根据所述业务类型标识和所选密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码。

12.根据权利要求11所述的基于传输层安全连接的数据流量归属识别装置，其特征在于，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码、密钥标识和时间戳；

所述接入侧计算执行子单元，具体用于根据所述业务类型标识、所选密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

所述业务类型标识提取单元还包括：

系统时间获取子单元，用于当所述认证码比对子单元的输出为是时，获取系统时间；

时间戳验证子单元，用于通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，触发所述流量归属识别子单元；

所述装置还包括：

网关时间同步单元，用于所述业务接入网关的系统时间与所述客户端的系统时间保持同步。

13.根据权利要求9所述的基于传输层安全连接的数据流量归属识别装置，其特征在于，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码和时间戳；

所述本地消息认证码计算子单元，具体用于根据所述业务类型标识、所述对应于所述业务类型标识的密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

所述业务类型标识提取单元还包括：

系统时间获取子单元，用于当所述认证码比对子单元的输出为是时，获取系统时间；

时间戳验证子单元，用于通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，触发所述流量归属识别子单元；

所述装置还包括：

网关时间同步单元，用于所述业务接入网关的系统时间与所述客户端的系统时间保持同步。

14.一种基于传输层安全连接的业务类型提供方法，其特征在于，所述方法在客户端实施，包括：

获取与待传输业务数据对应的业务类型标识，至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与业务接入网关相同的预设散列算法计算消息认证码；

在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息和所述消息认证码；

发送封装后的所述预设报文，以供业务接入网关根据所述业务类型标识进行业务数据流量归属的识别；

其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端，所述本地存储的、对应于所述业务类型标识的密钥与所述业务接入网关存储的相应信息保持同步。

15.根据权利要求14所述的基于传输层安全连接的业务类型提供方法，其特征在于，所述传输层安全连接包括：TLS连接。

16.根据权利要求14所述的基于传输层安全连接的业务类型提供方法，其特征在于，所述预设报文包括：client hello报文；

所述在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息，包括：在用于建立TLS连接的client hello报文的扩展数据块中，封装至少包含所述业务类型标识的业务类型扩展信息。

17.根据权利要求14所述的基于传输层安全连接的业务类型提供方法，其特征在于，所述本地存储的、对应于所述业务类型标识的密钥与所述业务接入网关存储的相应信息保持同步，通过以下方式实现：

所述客户端从所述数据业务提供方的密钥中心获取对应于所述业务类型标识的密钥，并存储于客户端；

所述业务接入网关从所述运营方的密钥中心获取对应于所述业务类型标识的密钥，并存储于业务接入网关；

所述数据业务提供方的密钥中心存储的业务类型标识及对应密钥，与所述运营方的密钥中心存储的相应信息保持同步。

18.根据权利要求14所述的基于传输层安全连接的业务类型提供方法，其特征在于，所述对应于所述业务类型标识的密钥数量为两个或者两个以上；

所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码，包括：按照预设策略从对应于所述业务类型标识的各密钥中选择一个密钥；至少根据所述业务类型标识和所选密钥，采用所述预设散列算法计算消息认证码；

在所述业务类型扩展信息中还包含：所选密钥的密钥标识。

19.根据权利要求18所述的基于传输层安全连接的业务类型提供方法，其特征在于，所述至少根据所述业务类型标识和所选密钥，采用所述预设散列算法计算消息认证码，包括：获取当前系统时间对应的时间戳；根据所述业务类型标识和所选密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

在所述业务类型扩展信息中还包含：所述时间戳；

其中，所述系统时间与所述业务接入网关的系统时间保持同步。

20.根据权利要求14所述的基于传输层安全连接的业务类型提供方法，其特征在于，所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码，包括：获取当前系统时间对应的时间戳；根据所述业务类型标识和所述对应于所述业务类型标识的密钥、以及所述时间戳，采

用所述预设散列算法计算消息认证码；

在所述业务类型扩展信息中还包含:所述时间戳；

其中,所述系统时间与所述业务接入网关的系统时间保持同步。

21.根据权利要求14所述的基于传输层安全连接的业务类型提供方法,其特征在于,包括：

根据预先获取的运营策略,判断是否执行封装业务类型标识的操作；

若是,则执行所述获取与待传输业务数据对应的业务类型标识的步骤。

22.一种基于传输层安全连接的业务类型提供装置,其特征在于,所述装置部署于客户端,包括：

业务类型标识获取单元,用于获取与待传输业务数据对应的业务类型标识;其中,所述业务类型标识由提供业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方,并预先指定给所述客户端；

消息认证码计算单元,用于在所述业务类型标识获取单元获取与待传输业务数据对应的业务类型标识后,至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥,采用与所述业务接入网关相同的预设散列算法计算消息认证码；

业务类型标识封装单元,用于在用于与服务端建立传输层安全连接的预设报文中,封装至少包含所述业务类型标识、及所述消息认证码的业务类型扩展信息；

预设报文发送单元,用于发送封装后的所述预设报文,以供业务接入网关根据所述业务类型标识进行业务数据流量归属的识别；

客户端密钥同步单元,用于本地存储的、对应于所述业务类型标识的密钥与所述业务接入网关存储的相应信息保持同步。

23.根据权利要求22所述的基于传输层安全连接的业务类型提供装置,其特征在于,所述业务类型标识封装单元,具体用于在用于建立TLS连接的client hello报文的扩展数据块中,封装至少包含所述业务类型标识的业务类型扩展信息。

24.根据权利要求22所述的基于传输层安全连接的业务类型提供装置,其特征在于,所述消息认证码计算单元,包括：

客户端密钥选取子单元,用于按照预设策略从对应于所述业务类型标识的各密钥中选择一个密钥；

客户端第一计算执行子单元,用于至少根据所述业务类型标识和所选密钥,采用与所述业务接入网关相同的预设散列算法计算消息认证码；

所述业务类型标识封装单元,具体用于在用于与服务端建立传输层安全连接的预设报文中,封装至少包含所述业务类型标识、所述消息认证码、以及所选密钥的密钥标识的业务类型扩展信息。

25.根据权利要求24所述的基于传输层安全连接的业务类型提供装置,其特征在于,所述客户端第一计算执行子单元,包括：

时间戳获取子单元,用于获取当前系统时间对应的时间戳；

客户端第二计算执行子单元,用于根据所述业务类型标识和所选密钥、以及所述时间戳,采用所述预设散列算法计算消息认证码；

所述业务类型标识封装单元,具体用于在用于与服务端建立传输层安全连接的预设报

文中，封装至少包含所述业务类型标识、所述消息认证码、以及所述时间戳的业务类型扩展信息；

所述装置还包括：

客户端时间同步单元，用于所述客户端的系统时间与业务接入网关的系统时间保持同步。

26.根据权利要求22所述的基于传输层安全连接的业务类型提供装置，其特征在于，所述消息认证码计算单元包括：

时间戳获取子单元，用于获取当前系统时间对应的时间戳；

客户端第三计算执行子单元，用于根据所述业务类型标识和所述对应于所述业务类型标识的密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、所述消息认证码、以及所述时间戳的业务类型扩展信息；

所述装置还包括：

客户端时间同步单元，用于所述客户端的系统时间与所述业务接入网关的系统时间保持同步。

27.根据权利要求22所述的基于传输层安全连接的业务类型提供装置，其特征在于，包括：

运营策略判断单元，用于根据预先获取的运营策略，判断是否执行封装业务类型标识的操作；并在是时，触发所述业务类型标识获取单元工作。

28.一种基于传输层安全连接的数据流量归属识别系统，其特征在于，包括：如上述权利要求9所述的基于传输层安全连接的数据流量归属识别装置、以及如上述权利要求22所述的基于传输层安全连接的业务类型提供装置。

基于传输层安全连接的数据流量归属识别方法及装置

技术领域

[0001] 本申请涉及数据处理技术领域，具体涉及一种基于传输层安全连接的数据流量归属识别方法及装置。本申请同时涉及一种基于传输层安全连接的业务类型提供方法及装置，以及一种基于传输层安全连接的数据流量归属识别系统。

背景技术

[0002] 电信运营商建设并拥有网络基础设施、并在此基础上提供通讯服务，数据业务提供方可以利用电信运营商的网络发展自己的数据业务，用户可以通过其提供的客户端(例如:App)访问相应的服务端，从而实现所需的功能。通常客户端发送的业务数据报文都会经过电信运营商提供的业务接入网关，业务接入网关可以对接收到的业务数据报文进行识别，统计并记录数据流量的归属信息、作为供计费网关进行计费的依据，并在处理完毕后将所述业务数据报文发送到公用数据网络中，所述业务数据报文最终经由路由器的转发到达相应的服务端，而服务端发送的业务数据报文也会经由所述业务接入网关返回给所述客户端。

[0003] 目前，大部分数据业务流量都采用加密传输的方式，普遍利用客户端与服务端建立的传输层安全连接(例如:TLS连接)实现业务数据的加密传输，所述传输层安全连接是为应用层提供的、位于TCP之上的安全传输通道，下面以TLS连接为例进行说明。客户端在TLS握手阶段向服务端发送client hello报文，随后双方可以验证证书并通过协商生成对称密钥，完成TLS连接(也称为TLS会话)的建立，此后双方就可以采用对称密钥基于所述TLS连接进行加密通信。

[0004] 在上述加密传输的基础上，业务接入网关通常采用基于SNI的流量归属识别方案，即:利用在TLS client hello报文的扩展字段中携带的SNI(Server Name Indication)进行识别。根据TLS协议的要求SNI中通常包含业务域名信息(例如:alipay.com或者baidu.com)，指明客户端想要访问的主机或者虚拟主机(多个虚拟主机可以位于同一个物理服务器上)的名称，业务接入网关根据此业务域名信息将后续基于TLS连接传输的数据业务流量归属到相应的数据业务。

[0005] 在具体应用中上述现有技术具有以下缺陷：

[0006] 1)因为运营商根据SNI携带的业务域名信息识别数据流量的归属，而业务域名存在变动的可能性，为了保证运营商能够正确地实施计费等功能，每当数据业务提供方增加、删除、或者更改业务域名信息，都需要通知运营商，由运营商进行相应的配置调整。由此可见，这种方式不仅增加了数据业务提供方的工作量，而且给运营商的运维配置管理带来不便。

[0007] 2)采用基于SNI的识别方式，只能根据业务域名识别数据流量的归属，粒度单一、不够灵活。

发明内容

[0008] 本申请实施例提供一种基于传输层安全连接的数据流量归属识别方法和装置，以解决采用现有技术导致的、数据业务提供方和运营商运作复杂以及识别粒度单一的问题。本申请实施例还提供一种基于传输层安全连接的业务类型提供方法和装置，以及一种基于传输层安全连接的数据流量归属识别系统。

[0009] 本申请提供一种基于传输层安全连接的数据流量归属识别方法，所述方法在业务接入网关中实施，包括：

[0010] 接收客户端发送的用于建立传输层安全连接的预设报文；

[0011] 通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

[0012] 其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端。

[0013] 可选的，所述传输层安全连接包括：TLS连接。

[0014] 可选的，所述预设报文包括：client hello报文；

[0015] 所述通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识，包括：通过解封装操作，从client hello报文的扩展数据块中提取业务类型扩展信息，并从所述业务类型扩展信息中至少提取所述业务类型标识。

[0016] 可选的，从所述预设报文的业务类型扩展信息中提取的信息还包括：消息认证码；

[0017] 通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识和所述消息认证码之后，包括：至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码；判断所述本地消息认证码与所述提取的消息认证码是否一致；并在一致时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

[0018] 其中，所述客户端存储的、与预先指定给其的业务类型标识相对应的密钥，与所述业务接入网关存储的相应信息保持同步。

[0019] 可选的，所述客户端存储的、与预先指定给其的业务类型标识相对应的密钥，与所述业务接入网关存储的相应信息保持同步，通过以下方式实现：

[0020] 所述客户端从所述数据业务提供方的密钥中心获取、并且仅获取与预先指定给其的业务类型标识相对应的密钥，并存储于客户端；

[0021] 所述业务接入网关从所述运营方的密钥中心获取与预先指定给所述客户端的业务类型标识相对应的密钥，并存储于业务接入网关；

[0022] 所述数据业务提供方的密钥中心存储的业务类型标识及对应密钥，与所述运营方的密钥中心存储的相应信息保持同步。

[0023] 可选的，所述对应于所述业务类型标识的密钥数量为两个或者两个以上；

[0024] 从所述预设报文的业务类型扩展信息中提取的信息还包括：密钥标识；

[0025] 所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码；包括：

[0026] 根据提取的所述密钥标识，从本地存储的、对应于所述业务类型标识的各密钥中选取相应密钥；

[0027] 至少根据所述业务类型标识和所选密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码。

[0028] 可选的，从所述预设报文的业务类型扩展信息中提取的信息还包括：时间戳；

[0029] 所述至少根据所述业务类型标识和所选密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码，包括：根据所述业务类型标识、所选密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0030] 当所述判断所述本地消息认证码与所述提取的消息认证码是否一致的结果为一致时，包括：获取系统时间；通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

[0031] 其中，所述系统时间与所述客户端的系统时间保持同步。

[0032] 可选的，从所述预设报文的业务类型扩展信息中提取的信息还包括：时间戳；

[0033] 所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码，包括：根据所述业务类型标识、所述对应于所述业务类型标识的密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0034] 当所述判断所述本地消息认证码与所述提取的消息认证码是否一致的结果为一致时，包括：获取系统时间；通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

[0035] 其中，所述系统时间与所述客户端的系统时间保持同步。

[0036] 可选的，所述客户端包括：OTT业务客户端。

[0037] 相应的，本申请还提供一种基于传输层安全连接的数据流量归属识别装置，所述装置部署于业务接入网关，包括：

[0038] 预设报文接收单元，用于接收客户端发送的用于建立传输层安全连接的预设报文；

[0039] 业务类型标识提取单元，用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端。

[0040] 可选的，所述业务类型标识提取单元，具体用于通过解封装操作，从client hello报文的扩展数据块中提取业务类型扩展信息，从所述业务类型扩展信息中至少提取所述业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

[0041] 可选的，所述业务类型标识提取单元包括：信息提取子单元、本地消息认证码计算子单元、认证码比对子单元、以及流量归属识别子单元；

[0042] 所述信息提取子单元，用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识和消息认证码；

[0043] 所述本地消息认证码计算子单元，用于至少根据所述业务类型标识和本地存储

的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0044] 所述认证码比对子单元，用于判断所述本地消息认证码与所述提取的消息认证码是否一致；

[0045] 所述流量归属识别子单元，用于当所述认证码比对子单元的输出为是时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

[0046] 所述装置还包括：

[0047] 网关密钥同步单元，用于所述客户端存储的、与预先指定给其的业务类型标识相对应的密钥，与所述业务接入网关存储的相应信息保持同步。

[0048] 可选的，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码和密钥标识；

[0049] 所述本地消息认证码计算子单元，包括：

[0050] 接入侧密钥选取子单元，用于根据提取的所述密钥标识，从本地存储的、对应于所述业务类型标识的各密钥中选取相应密钥；

[0051] 接入侧计算执行子单元，用于至少根据所述业务类型标识和所选密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码。

[0052] 可选的，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码、密钥标识和时间戳；

[0053] 所述接入侧计算执行子单元，具体用于根据所述业务类型标识、所选密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0054] 所述业务类型标识提取单元还包括：

[0055] 系统时间获取子单元，用于当所述认证码比对子单元的输出为是时，获取系统时间；

[0056] 时间戳验证子单元，用于通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，触发所述流量归属识别子单元；

[0057] 所述装置还包括：

[0058] 网关时间同步单元，用于所述业务接入网关的系统时间与所述客户端的系统时间保持同步。

[0059] 可选的，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码和时间戳；

[0060] 所述本地消息认证码计算子单元，具体用于根据所述业务类型标识、所述对应于所述业务类型标识的密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0061] 所述业务类型标识提取单元还包括：

[0062] 系统时间获取子单元，用于当所述认证码比对子单元的输出为是时，获取系统时间；

[0063] 时间戳验证子单元，用于通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，触发所述流量归属识别子

单元；

[0064] 所述装置还包括：

[0065] 网关时间同步单元，用于所述业务接入网关的系统时间与所述客户端的系统时间保持同步。

[0066] 此外，本申请还提供一种基于传输层安全连接的业务类型提供方法，所述方法在客户端实施，包括：

[0067] 获取与待传输业务数据对应的业务类型标识；

[0068] 在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息；

[0069] 发送封装后的所述预设报文，以供业务接入网关根据所述业务类型标识进行业务数据流量归属的识别；

[0070] 其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端。

[0071] 可选的，所述传输层安全连接包括：TLS连接。

[0072] 可选的，所述预设报文包括：client hello报文；

[0073] 所述在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息，包括：在用于建立TLS连接的client hello报文的扩展数据块中，封装至少包含所述业务类型标识的业务类型扩展信息。

[0074] 可选的，在所述获取与待传输业务数据对应的业务类型标识后，包括：至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码；

[0075] 在所述预设报文中封装的业务类型扩展信息中，不仅包含所述业务类型标识，还包含：所述消息认证码；

[0076] 其中，所述本地存储的、对应于所述业务类型标识的密钥与所述业务接入网关存储的相应信息保持同步。

[0077] 可选的，所述本地存储的、对应于所述业务类型标识的密钥与所述业务接入网关存储的相应信息保持同步，通过以下方式实现：

[0078] 所述客户端从所述数据业务提供方的密钥中心获取对应于所述业务类型标识的密钥，并存储于客户端；

[0079] 所述业务接入网关从所述运营方的密钥中心获取对应于所述业务类型标识的密钥，并存储于业务接入网关；

[0080] 所述数据业务提供方的密钥中心存储的业务类型标识及对应密钥，与所述运营方的密钥中心存储的相应信息保持同步。

[0081] 可选的，所述对应于所述业务类型标识的密钥数量为两个或者两个以上；

[0082] 所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码，包括：按照预设策略从对应于所述业务类型标识的各密钥中选择一个密钥；至少根据所述业务类型标识和所选密钥，采用所述预设散列算法计算消息认证码；

[0083] 在所述业务类型扩展信息中还包含：所选密钥的密钥标识。

[0084] 可选的，所述至少根据所述业务类型标识和所选密钥，采用所述预设散列算法计算消息认证码，包括：获取当前系统时间对应的时间戳；根据所述业务类型标识和所选密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

[0085] 在所述业务类型扩展信息中还包含：所述时间戳；

[0086] 其中，所述系统时间与所述业务接入网关的系统时间保持同步。

[0087] 可选的，所述至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码，包括：获取当前系统时间对应的时间戳；根据所述业务类型标识和所述对应于所述业务类型标识的密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

[0088] 在所述业务类型扩展信息中还包含：所述时间戳；

[0089] 其中，所述系统时间与所述业务接入网关的系统时间保持同步。

[0090] 可选的，所述方法包括：

[0091] 根据预先获取的运营策略，判断是否执行封装业务类型标识的操作；

[0092] 若是，则执行所述获取与待传输业务数据对应的业务类型标识的步骤。

[0093] 相应的，本申请还提供一种基于传输层安全连接的业务类型提供装置，所述装置部署于客户端，包括：

[0094] 业务类型标识获取单元，用于获取与待传输业务数据对应的业务类型标识；其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端；

[0095] 业务类型标识封装单元，用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息；

[0096] 预设报文发送单元，用于发送封装后的所述预设报文，以供业务接入网关根据所述业务类型标识进行业务数据流量归属的识别。

[0097] 可选的，所述业务类型标识封装单元，具体用于在用于建立TLS连接的client hello报文的扩展数据块中，封装至少包含所述业务类型标识的业务类型扩展信息。

[0098] 可选的，所述装置包括：

[0099] 消息认证码计算单元，用于在所述业务类型标识获取单元获取与待传输业务数据对应的业务类型标识后，至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码；

[0100] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、及所述消息认证码的业务类型扩展信息；

[0101] 所述装置还包括：

[0102] 客户端密钥同步单元，用于本地存储的、对应于所述业务类型标识的密钥与所述业务接入网关存储的相应信息保持同步。

[0103] 可选的，所述消息认证码计算单元，包括：

[0104] 客户端密钥选取子单元，用于按照预设策略从对应于所述业务类型标识的各密钥中选择一个密钥；

[0105] 客户端第一计算执行子单元，用于至少根据所述业务类型标识和所选密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码；

[0106] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、所述消息认证码、以及所选密钥的密钥标识的业务类型扩展信息。

[0107] 可选的，所述客户端第一计算执行子单元，包括：

[0108] 时间戳获取子单元，用于获取当前系统时间对应的时间戳；

[0109] 客户端第二计算执行子单元，用于根据所述业务类型标识和所选密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

[0110] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、所述消息认证码、以及所述时间戳的业务类型扩展信息；

[0111] 所述装置还包括：

[0112] 客户端时间同步单元，用于所述客户端的系统时间与所述业务接入网关的系统时间保持同步。

[0113] 可选的，所述消息认证码计算单元包括：

[0114] 时间戳获取子单元，用于获取当前系统时间对应的时间戳；

[0115] 客户端第三计算执行子单元，用于根据所述业务类型标识和所述对应于所述业务类型标识的密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

[0116] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、所述消息认证码、以及所述时间戳的业务类型扩展信息；

[0117] 所述装置还包括：

[0118] 客户端时间同步单元，用于所述客户端的系统时间与所述业务接入网关的系统时间保持同步。

[0119] 可选的，所述装置包括：

[0120] 运营策略判断单元，用于根据预先获取的运营策略，判断是否执行封装业务类型标识的操作；并在是时，触发所述业务类型标识获取单元工作。

[0121] 此外，本申请还提供一种基于传输层安全连接的数据流量归属识别系统，包括：根据上述任意一项所述的基于传输层安全连接的数据流量归属识别装置，以及根据上述任意一项所述的基于传输层安全连接的业务类型提供装置。

[0122] 与现有技术相比，本申请具有以下优点：

[0123] 本申请提供的基于传输层安全连接的数据流量归属识别技术方案，由数据业务客户端和业务接入网关配合完成。其中，客户端获取与待传输业务数据对应的业务类型标识，在用于与服务端建立传输层安全连接的预设报文中封装至少包含所述业务类型标识的业务类型扩展信息，并发送封装后的所述预设报文；业务接入网关接收所述预设报文后，通过解封装操作从所述预设报文的业务类型扩展信息中至少提取所述业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方、通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端。

[0124] 本申请提出的上述技术方案，提供了一种识别数据业务流量归属的新思路，与传

统基于SNI的流量归属识别方法不同，本技术方案采用业务类型标识区分不同的业务类型，客户端在用于建立传输层安全连接的预设报文中封装与待传输业务数据对应的业务类型标识，业务接入网关则根据业务类型标识识别数据流量归属。由于业务类型标识是数据业务提供方与运营方预先协商分配的，对于运营方来说可以做到一次配置长期有效，而且由于与业务域名无关，当数据业务提供方需要变更业务域名信息时，无需通知运营商进行重新配置。从而既简化了数据业务提供方的操作，也为运营商的运维配置管理提供便利，而且还可以通过定义不同粒度的业务类型实现不同粒度的流量归属识别，与传统基于SNI的流量归属识别方法相比更为灵活，可以为流量统付等流量经营模式、以及用户行为监控等业务目标提供更好的支持。

附图说明

[0125] 图1是本申请的一种基于传输层安全连接的业务类型提供方法的实施例的流程图；

[0126] 图2是本申请的一种基于传输层安全连接的业务类型提供装置的实施例的示意图；

[0127] 图3是本申请的一种基于传输层安全连接的数据流量归属识别方法的实施例的流程图；

[0128] 图4是本申请的一种基于传输层安全连接的数据流量归属识别装置的实施例的示意图；

[0129] 图5是本申请的一种基于传输层安全连接的数据流量归属识别系统的实施例的示意图；

[0130] 图6是本申请实施例提供的流量归属识别的基本流程示意图。

具体实施方式

[0131] 在下面的描述中阐述了很多具体细节以便于充分理解本申请。但是，本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似推广，因此，本申请不受下面公开的具体实施的限制。

[0132] 在本申请中，分别提供了一种基于传输层安全连接的数据流量归属识别方法及装置，一种基于传输层安全连接的业务类型提供方法及装置，以及一种基于传输层安全连接的数据流量归属识别系统。在下面的实施例中逐一进行详细说明。

[0133] 为了便于理解，在描述具体的实施例之前，先对本申请的技术方案进行简要说明。本申请提供了一种识别数据业务流量归属的新技术方案，其核心在于：提出了业务类型标识的概念，用业务类型标识区分不同的业务类型，客户端在用于建立传输层安全连接的预设报文中封装与待传输业务数据对应的业务类型标识，业务接入网关则根据业务类型标识识别数据流量归属。由于业务类型标识是数据业务提供方与运营方预先协商分配的，而且与业务域名无关，因此可以简化数据业务提供方的操作，也为运营商的运维配置管理提供便利。

[0134] 所述数据业务包括基于有线宽带接入方式或者无线接入方式、利用运营方的网络设施向用户提供的各种应用服务，其中包括OTT业务。所述数据业务提供方则是指提供数据

业务的一方，例如：阿里巴巴、腾讯等。所述客户端是指数据业务提供方提供的、用于访问数据业务服务的应用程序，例如：来往客户端、QQ客户端等。所述运营方是指建设并拥有网络基础设施的一方，可以是通常所述的运营商，例如：中国电信等。数据业务客户端发送的报文通常都会经过运营方提供的业务接入网关，业务接入网关采集数据流量的归属信息，为其他网关或者服务器执行基于数据流量归属的相关业务处理提供依据，例如：为计费网关进行计费提供依据。

[0135] 所述业务类型标识是由提供业务接入网关的运营方与数据业务提供方、通过预先协商分配给所述数据业务提供方的。例如：可以由数据业务提供方向运营方发出申请，由运营方为其分配一个或者多个业务类型标识；也可以由数据业务提供方向运营商上报一个或者多个业务类型标识，经由运营商审批后、相应业务类型标识被分配给所述数据业务提供方。

[0136] 所述业务类型则可以采用不同的粒度加以定义，例如：可以将数据业务提供方开展的多种数据业务指定为一种业务类型，那么通过协商为数据业务提供方分配一个业务类型标识(下面以serviceID表示)即可；为了实现更为细致的流量归属识别、为运营商进行流量经营提供便利，也可以将数据业务提供方的不同数据业务分别定义为不同的业务类型，并用不同的serviceID加以区分，例如：阿里巴巴可以将支付宝和淘宝设定为不同的业务类型，用serviceID＝1标识支付宝业务类型，用serviceID＝2标识淘宝业务类型，进一步地，也可以将一种数据业务根据预设策略细化为不同的业务类型，例如对于淘宝数据业务，可以将对店铺A的访问和对店铺B的访问分别设定为不同的业务类型，用不同的serviceID加以标识。

[0137] 由此可见，在具体实施中，本技术方案引入的业务类型标识，可以定义不同粒度的业务类型，因此为实现不同粒度的流量归属识别提供了可能性，比基于SNI的流量归属识别方法更为灵活。具体实施时，定义好业务类型与serviceID的对应关系后，数据业务提供方可以将serviceID指定给相应的客户端，即：建立业务类型标识与客户端的对应关系。

[0138] 所述传输层安全连接是指为应用层提供的、位于TCP之上的安全传输通道。客户端与服务端建立传输层安全连接的过程通常包括：两者之间先建立TCP数据连接，然后双方采用预设流程协商对称密钥(在此过程中还可以进行身份验证等安全性检查)，完成对称密钥的协商后，可以认为传输层安全连接建立完毕，此后双方就可以采用对称密钥基于所述传输层安全连接进行加密通信。

[0139] 本技术方案可以应用于基于传输层安全连接进行数据传输的应用场景中，客户端获取与待传输业务数据对应的业务类型标识，在用于与服务端建立传输层安全连接的预设报文中封装至少包含所述业务类型标识的业务类型扩展信息，并发送封装后的所述预设报文；业务接入网关接收所述预设报文后，通过解封装操作从所述预设报文的业务类型扩展信息中提取所述业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

[0140] 作为一种优选实施方式，可以采用基于TLS协议(Transport Layer Security Protocol—安全传输层协议)的TLS连接(也称为TLS会话)作为所述传输层安全连接，从而便于目前各种基于TLS协议的数据业务客户端、以及业务接入网关实施本技术方案。在建立TLS连接的过程中，客户端向服务端发送client hello报文、密钥交换报文等多个报文，实

施本技术方案的客户端可以在上述报文的扩展数据块或者预留字段、或者其它不影响TLS连接建立过程的字段中封装至少包含业务类型标识的业务类型扩展信息。考虑到client hello报文是TLS连接建立过程中通常需要发送的报文、而且其报文格式支持扩展数据块，因此，在本文下面的实施例中以在TLS连接的client hello报文中，封装至少包含业务类型标识的业务类型扩展信息为例，对本技术方案的实施方式进行描述。

[0141] 但是本技术方案并不局限于采用TLS连接的应用场景，也可以应用于其他基于传输层安全连接的应用场景中，只要客户端与业务接入网关预先协商好所述预设报文的封装格式，客户端按照所述格式的要求封装业务类型标识，业务接入网关接收预设报文后按照所述格式执行解封装操作，提取业务类型标识，就同样可以实现本申请的技术方案。

[0142] 下面对本申请提供的实施例逐一进行说明。为了便于理解，首先描述本申请提供的一种基于传输层安全连接的业务类型提供方法的实施例，所述方法在客户端实施。

[0143] 参考图1，其为本申请的一种基于传输层安全连接的业务类型提供方法的实施例的流程图，所述方法包括如下步骤：

[0144] 步骤101、获取与待传输业务数据对应的业务类型标识。

[0145] 通常，客户端可以预先接收服务端下发的运营策略，所述运营策略规定客户端在报文中封装业务类型标识的条件，因此在执行本步骤之前，可以先根据所述营运策略，判断是否需要执行封装业务类型标识的操作，若是，则执行本步骤，获取与待传输业务数据对应的业务类型标识。所述运营策略可以包含时间、地域、或者系统配置等多个维度的条件，例如：可以规定在每天8:00—10:00之间封装业务类型标识，如果当前时间为9:00，则满足运营策略规定的条件，可以执行本步骤。采用这种方式，可以根据运营需求、灵活地触发本方法的实施。

[0146] 本步骤获取与待传输业务数据对应的业务类型标识，为步骤102执行封装操作做好准备。在具体实施时，预先指定给所述客户端的业务类型标识可以预置在所述客户端中(例如写在配置文件中)，也可以由客户端在启动时向服务端动态获取。如果指定给所述客户端的业务类型标识只有一个，那么本步骤直接获取所述业务类型标识即可，如果根据对业务类型的划分，为所述客户端预先指定了两个或者两个以上的业务类型标识，那么本步骤则可以根据配置文件中对每种业务类型的描述、以及待传输业务数据的属性或特征判断其所属的业务类型、并选择相应的业务类型标识。

[0147] 步骤102、在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息。

[0148] 客户端与服务端之间建立起TCP连接之后，可以启动传输层安全连接的建立过程，在本实施例中所述传输层安全连接是指TLS连接，所述预设报文是client hello报文，因此本步骤在用于建立TLS连接的client hello报文中封装包含所述业务类型标识的业务类型扩展信息。

[0149] 在client hello报文封装所述业务类型扩展信息，是为了让业务接入网关根据其中包含的业务类型标识，进行数据流量归属的识别。在最为简单易行的实施方式中，所述业务类型扩展信息中可以仅包含业务类型标识。

[0150] 优选地，为了便于业务接入网关验证接收到的业务类型标识的完整性、以及甄别业务类型标识是否被冒用，本实施例提供根据步骤101获取的业务类型标识及对应密钥计

算消息认证码、并在所述业务类型扩展信息中包含所述消息认证码的优选实施方式。另外，在此基础上还分别提供了从多个密钥中选取密钥、以及在所述业务类型扩展信息中包含时间戳的另外两种优选实施方式。下面分别进行说明。

[0151] (一)根据所述业务类型标识及对应密钥计算消息认证码

[0152] 为了采用这种优选实施方式，所述客户端通常存储对应于所述业务类型标识的密钥，并且与所述业务接入网关存储的相应信息保持同步。例如：所述业务类型标识为serviceID1，对应密钥为key1，客户端存储该信息，业务接入网关也同样存储了该信息。

[0153] 具体实施时，所述客户端可以预置指定给它的各业务类型标识的对应密钥，业务接入网关也可以预置指定给所述客户端的各业务类型标识的对应密钥，并且与所述客户端相同。

[0154] 此外，也可以采用动态获取的方式，客户端可以在启动过程中、或者定期从数据业务提供方的密钥中心获取(可以通过请求获取、也可以被动接收下发的密钥信息)指定给它的各业务类型标识的对应密钥，并将获取的信息在本地存储；类似的，业务接入网关也可以定期从运营方的密钥中心获取指定给所述客户端的各业务类型标识的对应密钥，并存储在本地；并且，所述数据业务提供方的密钥中心存储的业务类型标识及对应密钥、与运营方的密钥中心存储的相应信息保持同步，例如：所述数据业务提供方的密钥中心可以定期将其维护的业务类型标识及对应密钥发送给运营方的密钥中心。需要说明的是，所述客户端不能从数据业务提供方的密钥中心获取未指定给它的其他业务类型标识的对应密钥。

[0155] 通过上述同步机制，在所述客户端一侧存储的、预先指定给所述客户端的各业务类型标识的对应密钥，与所述业务接入网关存储的相应信息保持同步；自然，对于通过步骤101获取的与待传输业务数据对应的所述业务类型标识，双方也存储了相同的密钥。

[0156] 在执行本步骤之前，可以获取本地存储的、与所述业务类型标识对应的密钥，然后根据所述业务类型标识和所述密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码，例如：可以将所述业务类型标识和所述密钥直接连接成字符串，然后采用预设散列算法计算消息认证码。本步骤在client hello报文的扩展数据块中，封装不仅包含所述业务类型标识，还包含所述消息认证码的业务类型扩展信息。

[0157] (二)从对应于所述业务类型标识的多个密钥中选取密钥

[0158] 为了进一步加强安全性，与所述业务类型标识对应的密钥数量可以为两个或者两个以上，每个密钥都有各自的标识信息。在这种情况下，在执行本步骤之前，可以按照预设策略从对应于所述业务类型标识的各密钥中选择一个密钥，然后根据所述业务类型标识和所选密钥，采用与业务接入网关相同的预设散列算法计算消息认证码。本步骤在client hello报文的扩展数据块中，封装不仅包含所述业务类型标识和所述消息认证码、还包含所选密钥的密钥标识的业务类型扩展信息。

[0159] (三)在所述业务类型扩展信息中包含时间戳

[0160] 为了便于业务接入网关验证其接收到的client hello报文中的业务类型标识的新鲜性，识别可能存在的回放(也称为重放)行为，本实施例还提供在所述业务类型扩展信息中包含时间戳的优选实施方式。采用这种优选实施方式，要求客户端的系统时间与业务接入网关的系统时间保持同步，保持系统时间同步可以有多种实施方式，此处列举一种：客户端与数据业务提供方的密钥中心通过时间同步协议(例如：简单网络时间协议)保持彼此

的系统时间同步;业务接入网关与运营方密钥中心通过时间同步协议保持彼此的系统时间同步;上述两个密钥中心则可以通过从原子钟获取时间的方式保持双方系统时间的同步。在具体实施时,可以根据需要设置系统时间同步的精度,例如:可以设置为小时或者分钟。

[0161] 在客户端的系统时间与业务接入网关的系统时间保持同步的基础上,在执行本步骤之前,可以获取当前系统时间对应的时间戳,根据步骤101获取的业务类型标识和对应于所述业务类型标识的密钥、以及所述时间戳,采用与业务接入网关相同的预设散列算法计算消息认证码。本步骤在client hello报文的扩展数据块中,封装不仅包含所述业务类型标识和所述消息认证码,还包含所述时间戳的业务类型扩展信息。

[0162] 以上,在利用密钥生成消息认证码的优选实施方式的基础上,还分别给出了从多个密钥中选取密钥、以及携带时间戳的优选实施方式,在具体实施时,这些优选实施方式也可以结合使用。例如,可以将(二)和(三)结合起来实施,在执行本步骤之前,首先从对应于所述业务类型标识的多个密钥中选取一个,获取当前系统时间对应的时间戳,然后根据所述业务类型标识、所选密钥、以及所述时间戳,采用与业务接入网关相同的预设散列算法计算消息认证码,那么本步骤在client hello报文的扩展数据块中封装的业务类型扩展信息中,不仅包括所述业务类型标识、所述消息认证码,还包括所选密钥的密钥标识、以及所述时间戳。

[0163] 在client hello报文的扩展数据块中封装至少包含业务类型标识的业务类型扩展信息时,通常需要根据TLS协议的规定进行封装,例如添加类型信息、长度信息等。下面给出一个在client hello报文的扩展数据块中封装业务类型扩展信息的具体例子,在本例子中,所述业务类型扩展信息中包含业务类型标识、时间戳、密钥标识、以及消息认证码:

[0164] Type:0x698 说明:扩展数据块类型

[0165] Length:xx 说明:扩展数据块长度

[0166] ServiceID:xxxx 说明:业务类型标识

[0167] ServiceTimeStamp:12345678 说明:时间戳

[0168] KeyID:1 说明:密钥标识

[0169] MAC:1233456789abcdefg 说明:消息认证码

[0170] 上面描述了本实施例提供的多种优选实施方式,主要是为了便于业务接入网关验证业务类型标识的完整性、甄别是否被冒用、以及是否存在重放行为等,这些对于实施本技术方案都不是必需的。本技术方案的核心在于,客户端在用于与服务端建立传输层安全连接的预设报文中封装至少包含所述业务类型标识的业务类型扩展信息,以供业务接入网关根据所述业务类型标识进行数据流量归属的识别,因此只要在所述预设报文中封装了所述业务类型标识信息,就都在本申请的保护范围内。

[0171] 步骤103、发送封装后的所述预设报文,以供业务接入网关根据所述业务类型标识进行数据流量归属的识别。

[0172] 步骤102完成预设报文的封装后,就可以向服务端发送所述预设报文。所述预设报文在传输过程中,会经过所述业务接入网关,业务接入网关识别所述预设报文后,可以根据其中封装的业务类型标识进行数据流量归属的识别。

[0173] 综上所述,本实施例提供的一种基于传输层安全连接的业务类型提供方法,由客户端在用于建立传输层安全连接的预设报文中封装至少包含业务类型标识的业务类型扩

展信息，为业务接入网关根据业务类型标识进行数据流量归属的识别提供了必要前提；而且客户端封装的业务类型标识可以对应于不同粒度的业务类型，因此可以在业务接入网关一侧实现不同粒度的数据流量归属识别。

[0174] 在上述的实施例中，提供了一种基于传输层安全连接的业务类型提供方法，与之相对应的，本申请还提供一种基于传输层安全连接的业务类型提供装置。请参看图2，其为本申请的一种基于传输层安全连接的业务类型提供装置的实施例示意图。由于装置实施例基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。下述描述的装置实施例仅仅是示意性的。

[0175] 本实施例的一种基于传输层安全连接的业务类型提供装置，所述装置部署于客户端，包括：业务类型标识获取单元201，用于获取与待传输业务数据对应的业务类型标识；其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端；业务类型标识封装单元202，用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息；预设报文发送单元203，用于发送封装后的所述预设报文，以供业务接入网关根据所述业务类型标识进行业务数据流量归属的识别。

[0176] 可选的，所述业务类型标识封装单元，具体用于在用于建立TLS连接的client hello报文的扩展数据块中，封装至少包含所述业务类型标识的业务类型扩展信息。

[0177] 可选的，所述装置包括：

[0178] 消息认证码计算单元，用于在所述业务类型标识获取单元获取与待传输业务数据对应的业务类型标识后，至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码；

[0179] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、及所述消息认证码的业务类型扩展信息；

[0180] 所述装置还包括：

[0181] 客户端密钥同步单元，用于本地存储的、对应于所述业务类型标识的密钥与所述业务接入网关存储的相应信息保持同步。

[0182] 可选的，所述消息认证码计算单元，包括：

[0183] 客户端密钥选取子单元，用于按照预设策略从对应于所述业务类型标识的各密钥中选择一个密钥；

[0184] 客户端第一计算执行子单元，用于至少根据所述业务类型标识和所选密钥，采用与所述业务接入网关相同的预设散列算法计算消息认证码；

[0185] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、所述消息认证码、以及所选密钥的密钥标识的业务类型扩展信息。

[0186] 可选的，所述客户端第一计算执行子单元，包括：

[0187] 时间戳获取子单元，用于获取当前系统时间对应的时间戳；

[0188] 客户端第二计算执行子单元，用于根据所述业务类型标识和所选密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

[0189] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预

设报文中，封装至少包含所述业务类型标识、所述消息认证码、以及所述时间戳的业务类型扩展信息；

[0190] 所述装置还包括：

[0191] 客户端时间同步单元，用于所述客户端的系统时间与所述业务接入网关的系统时间保持同步。

[0192] 可选的，所述消息认证码计算单元包括：

[0193] 时间戳获取子单元，用于获取当前系统时间对应的时间戳；

[0194] 客户端第三计算执行子单元，用于根据所述业务类型标识和所述对应于所述业务类型标识的密钥、以及所述时间戳，采用所述预设散列算法计算消息认证码；

[0195] 所述业务类型标识封装单元，具体用于在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识、所述消息认证码、以及所述时间戳的业务类型扩展信息；

[0196] 所述装置还包括：

[0197] 客户端时间同步单元，用于所述客户端的系统时间与所述业务接入网关的系统时间保持同步。

[0198] 可选的，所述装置包括：

[0199] 运营策略判断单元，用于根据预先获取的运营策略，判断是否执行封装业务类型标识的操作；并在是时，触发所述业务类型标识获取单元工作。

[0200] 此外，本申请还提供一种基于传输层安全连接的数据流量归属识别方法，所述方法通常业务接入网关中实施。

[0201] 请参考图3，其为本申请提供的一种基于传输层安全连接的数据流量归属识别方法的实施例的流程图，本实施例与上述方法实施例步骤相同的部分不再赘述，下面重点描述不同之处。本实施例的一种基于传输层安全连接的数据流量归属识别方法，包括如下步骤：

[0202] 步骤301、接收客户端发送的用于建立传输层安全连接的预设报文。

[0203] 客户端发送的数据报文在传输到达服务端之前，通常都会经过业务接入网关，业务接入网关接收客户端发送的数据报文后，根据报文封装的协议类型、端口等相关信息识别是否为所述预设报文，如果是则可以执行后续步骤302。

[0204] 在本实施例中，所述传输层安全连接是TLS连接，在TLS连接上承载的是Https应用，所述预设报文是client hello报文，那么如果业务接入网关通过对接收报文的解析，发现该报文是443端口的，并且是TLS握手阶段(ContentType＝22)的消息类型为1的报文，就可以识别出该报文为client hello报文，随后就可以执行步骤302。

[0205] 步骤302、通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

[0206] 本步骤可以根据与客户端约定好的格式，从所述预设报文的业务类型扩展信息中提取业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。本实施例中，可以从client hello报文扩展数据块中提取业务类型扩展信息，并从中提取所述业务类型标识。

[0207] 为了便于业务接入网关能够对报文信息的完整性进行验证，以及甄别冒用业务类

型标识等现象，所述客户端还可以在预设报文的业务类型扩展信息中包含消息验证码、密钥标识、时间戳等信息，业务接入网关和所述客户端可以预先约定好在预设报文中封装哪些信息，那么本步骤可以根据从所述业务类型扩展信息中提取的信息执行相应的验证操作，下面描述几种优选实施方式。

[0208] (一)提取的信息包括：业务类型标识和基于密钥计算得到的消息认证码。

[0209] 采用基于密钥计算消息认证码的优选实施方式，要求所述客户端存储的密钥信息与业务接入网关同步，即：对于预先指定给所述客户端的各业务类型标识，客户端所存储的相应密钥，与业务接入网关存储的相应信息保持同步。此外，业务接入网关通常为多种客户端(包括本实施例中的所述客户端)提供接入服务，因此也可以存储指定给其他客户端的业务类型标识的对应密钥，这些密钥可以是预置的、也可以是从运营方的密钥中心获取的。

[0210] 本步骤可以通过以下方式验证业务类型标识的完整性、以及所述客户端是否存在冒用业务类型标识的行为。

[0211] 具体实现可以为：根据从预设报文中提取的业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码；判断所述本地消息认证码与所述提取的消息认证码是否一致。

[0212] 若一致，一方面验证了业务类型标识的信息完整性，另一方面说明所述客户端在计算消息认证码时使用的是指定给其的业务类型标识以及相对应的正确密钥，所述客户端没有冒用其他客户端的业务类型标识，在这种情况下，可以根据所述业务类型标识，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

[0213] 若不一致，可能是因为在所述预设报文中封装的业务类型标识的完整性在传输过程中被破坏，或者是客户端冒用了未指定给它的业务类型标识，而客户端没有相对应的正确密钥，因此导致其在预设报文中封装的消息认证码与业务接入网关计算得到的不同。在这两种情况下，都不能够根据所述业务类型标识，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

[0214] 传统基于SNI的数据流量识别方案不具备对SNI正确性的验证机制，因此无法识别可能存在的流量欺诈现象，例如：访问某一数据业务的报文、却携带了其他数据业务的SNI，从而导致业务接入网关做出错误的流量归属判定。而本实施例提供的上述优选实施方式，通过对消息认证码的比对，可以识别出客户端的冒充行为，从而避免作出错误的流量归属判定。

[0215] (二)提取的信息包括：业务类型标识、消息认证码和密钥标识。

[0216] 为了进一步提高安全性，与所述业务类型标识对应的密钥数量可以为两个或者两个以上，所述客户端选用了其中一个参与消息认证码的计算，业务接入网关也需要使用同样的密钥进行验证。在这种情况下，本步骤从所述预设报文的业务类型扩展信息中提取的信息不仅包括业务类型标识、消息认证码，还包括密钥标识，计算本地消息认证码的方式也相应地调整为：

[0217] 根据提取的所述密钥标识，从本地存储的对应于所述业务类型标识的各密钥中选取相应密钥；至少根据所述业务类型标识和所选密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码。

[0218] 在通过上述方式计算得到消息认证码后，可以采用在(一)中描述的相同方式进行

验证，从而不仅可以甄别是否存在冒用业务类型标识的现象，而且由于采用了多密钥，因此可以进一步增强安全性。

[0219] (三)提取的信息包括：业务类型标识、消息认证码和时间戳信息。

[0220] 为了识别是否存在报文重放(也称回放)现象，客户端可以在发送的报文中封装时间戳，业务接入网关则根据系统时间和所述时间戳判断接收到的报文是否为重放报文。采用这种优选实施方案，要求客户端的系统时间与业务接入网关的系统时间保持同步，具体实施方式，请参见上一方法实施例中的相关描述，此处不再赘述。

[0221] 本步骤从所述预设报文的业务类型扩展信息中提取的信息不仅包括业务类型标识、消息认证码，还包括时间戳，计算本地消息认证码的方式也相应地调整为：根据所述业务类型标识、对应于所述业务类型标识的密钥、以及所述时间戳信息，采用与所述客户端相同的预设散列算法计算本地消息认证码。

[0222] 在通过上述方式计算得到本地消息认证码后，可以采用在(一)中描述的相同方式进行验证，当判断出本地消息认证码与从预设报文中提取的消息认证码一致时，可以执行如下操作：获取系统时间；通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

[0223] 为了便于理解，此处举例说明。预先设置有效范围为：业务接入网关接收并处理所述预设报文之前的10分钟，那么如果业务接入网关在本步骤获取的系统时间为9:10，从预设报文中提取的时间戳所对应的时间为9:08，由于9:08处于9:10之前的10分钟之内，因此可以认为不是重放报文，但是如果时间戳所对应的时间为8:30，则可以认为接收到的预设报文是经过拦截、复制处理后的重放报文，在这种情况下，则不能利用从所述预设报文中提取的业务类型标识进行后续流量的归属判定。采用这种实施方式可以抵御网络中可能存在的重放攻击。

[0224] 以上给出了与客户端相配合的几种优选实施方式，在具体实施时，可以根据需要选取相应的实施方式，例如：也可以将上述第二种与第三种优选实施方式结合起来，在这种情况下，客户端在预设报文中封装的业务类型扩展信息中包含：业务类型标识、消息认证码、密钥标识、以及时间戳，本步骤可以在提取上述信息后，先根据提取的所述密钥标识，从本地存储的、对应于所述业务类型标识的各密钥中选取相应密钥，然后根据提取的业务类型标识、所选密钥、以及提取的时间戳计算本地消息认证码，最后判断所述本地消息认证码与提取的消息认证码是否一致，并在一致的情况下判断时间戳是否在有效范围内。

[0225] 需要说明的是，本技术方案的核心在于：业务接入网关从预设报文中提取业务类型标识，并根据所述标识确定后续流量归属。上述提供的多种优选实施方式，主要是为了识别冒用业务类型标识、以及重放行为等异常操作行为，是对本技术方案的进一步的优化。

[0226] 在本实施例中，在从用于建立TLS连接的client hello报文中提取业务类型标识后，可以将后续基于所述TLS连接的业务数据流量归属于相应的业务类型。在具体实施时，可以在解封装操作过程中，记录所述TLS连接的五元组信息，包括：源IP地址，源端口，目的IP地址，目的端口和协议号，并建立起五元组与所述业务类型标识的对应关系，那么当客户端与服务端利用建立好的TLS连接传输应用层数据时，业务接入网关可以将与所述五元组对应的业务数据流量都归属于所述业务类型标识所对应的业务类型。

[0227] 需要说明的是，基于TLS连接传输的应用层数据，并不局限于遵循HTTP协议的应用层数据，也可以是基于其他协议的应用层数据，例如：FTP、SMTP、POP、Telnet等，都是可以的。

[0228] 在具体实施时，业务接入网关通过实施本实施例描述的方法，在根据业务类型标识识别数据流量归属的基础上，可以定期生成流量清单，记录与每个业务类型标识对应的数据流量。例如，为了简化描述用serviceID代表业务类型标识，可以生成如下形式的流量清单：serviceID1—xxxx字节，serviceID2—xxxx字节，.....。并可以将生成的流量清单提供给进行计费的计费网关，由于serviceID是由运营方与数据业务提供方协商分配的，计费网关通常预先配置了serviceID与数据业务提供方之间的对应关系，因此可以将属于同一数据业务提供方的流量统一进行计费，也可以采用预先设定的差异化计费方式，根据不同的serviceID采用不同的计费方式，并最终汇总到相应的数据业务提供方。

[0229] 此外，业务接入网关生成的流量清单不仅可以用于计费，还可以提供给其他的服务端进行进一步的数据挖掘，例如：可以基于不同时段、不同业务类型的数据流量，分析用户上网行为、实施用户行为监控等其他业务目标。

[0230] 综上所述，本申请提供的基于传输层安全连接的数据流量归属识别方法，可以在运营方原有设备的基础上增加通过业务类型标识识别数据流量归属的功能，即：客户端可以在用于建立传输层安全连接的预设报文中封装业务类型标识，而业务接入网关根据该标识识别后续业务数据的流量归属。采用该技术方案，可以在保证业务数据安全传输的基础上实现数据流量的有效识别，不仅可以简化数据业务提供方和运营方的操作复杂度，实现不同粒度的流量归属识别，而且可以为流量统付等流量经营模式、以及用户行为监控等业务目标提供更好的支持。

[0231] 在上述的实施例中，提供了一种基于传输层安全连接的数据流量归属识别方法，与之相对应的，本申请还提供一种基于传输层安全连接的数据流量归属识别装置。请参看图4，其为本申请的一种基于传输层安全连接的数据流量归属识别装置的实施例示意图。由于装置实施例基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。下述描述的装置实施例仅仅是示意性的。

[0232] 本实施例的一种基于传输层安全连接的数据流量归属识别装置，所述装置部署于业务接入网关，包括：预设报文接收单元401，用于接收客户端发送的用于建立传输层安全连接的预设报文；业务类型标识提取单元402，用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；其中，所述业务类型标识由提供所述业务接入网关的运营方与提供所述客户端的数据业务提供方通过预先协商分配给所述数据业务提供方，并预先指定给所述客户端。

[0233] 可选的，所述业务类型标识提取单元，具体用于通过解封装操作，从client hello报文的扩展数据块中提取业务类型扩展信息，从所述业务类型扩展信息中至少提取所述业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型。

[0234] 可选的，所述业务类型标识提取单元包括：信息提取子单元、本地消息认证码计算子单元、认证码比对子单元、以及流量归属识别子单元；

[0235] 所述信息提取子单元，用于通过解封装操作从所述预设报文的业务类型扩展信息

中至少提取业务类型标识和消息认证码；

[0236] 所述本地消息认证码计算子单元，用于至少根据所述业务类型标识和本地存储的、对应于所述业务类型标识的密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0237] 所述认证码比对子单元，用于判断所述本地消息认证码与所述提取的消息认证码是否一致；

[0238] 所述流量归属识别子单元，用于当所述认证码比对子单元的输出为是时，将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型；

[0239] 所述装置还包括：

[0240] 网关密钥同步单元，用于所述客户端存储的、与预先指定给其的业务类型标识相对应的密钥，与所述业务接入网关存储的相应信息保持同步。

[0241] 可选的，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码和密钥标识；

[0242] 所述本地消息认证码计算子单元，包括：

[0243] 接入侧密钥选取子单元，用于根据提取的所述密钥标识，从本地存储的、对应于所述业务类型标识的各密钥中选取相应密钥；

[0244] 接入侧计算执行子单元，用于至少根据所述业务类型标识和所选密钥，采用与所述客户端相同的预设散列算法计算本地消息认证码。

[0245] 可选的，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码、密钥标识和时间戳；

[0246] 所述接入侧计算执行子单元，具体用于根据所述业务类型标识、所选密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0247] 所述业务类型标识提取单元还包括：

[0248] 系统时间获取子单元，用于当所述认证码比对子单元的输出为是时，获取系统时间；

[0249] 时间戳验证子单元，用于通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，触发所述流量归属识别子单元；

[0250] 所述装置还包括：

[0251] 网关时间同步单元，用于所述业务接入网关的系统时间与所述客户端的系统时间保持同步。

[0252] 可选的，所述信息提取子单元，具体用于通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识、消息认证码和时间戳；

[0253] 所述本地消息认证码计算子单元，具体用于根据所述业务类型标识、所述对应于所述业务类型标识的密钥、以及所述时间戳，采用与所述客户端相同的预设散列算法计算本地消息认证码；

[0254] 所述业务类型标识提取单元还包括：

[0255] 系统时间获取子单元，用于当所述认证码比对子单元的输出为是时，获取系统时间；

[0256] 时间戳验证子单元，用于通过与所述系统时间进行比较，判断所述时间戳所对应的时间是否处于预设有效范围内；并在处于所述有效范围内时，触发所述流量归属识别子单元；

[0257] 所述装置还包括：

[0258] 网关时间同步单元，用于所述业务接入网关的系统时间与所述客户端的系统时间保持同步。

[0259] 此外，本申请实施例还提供了一种基于传输层安全连接的数据流量归属识别系统，如图5所示，该系统包括：基于传输层安全连接的数据流量归属识别装置501，以及基于传输层安全连接的业务类型提供装置502。

[0260] 其中，所述基于传输层安全连接的业务类型提供装置(以下简称业务类型提供装置)可以部署于移动终端或者计算机等客户端设备，所述基于传输层安全连接的数据流量归属识别装置(以下简称数据流量归属识别装置)可以部署于运营方的业务接入网关服务器上。在具体实施时，所述系统中通常还包括：数据业务服务器，下面结合图6，对流量归属识别的基本流程作简要说明。

[0261] 部署于移动终端设备的业务类型提供装置在需要发送应用层数据时，在与数据业务服务器建立TCP连接的基础上，启动TLS连接的建立过程，在client hello报文中封装业务类型标识，部署于业务接入网关服务器的数据流量归属识别装置识别该报文后，从中提取业务类型标识，与TLS连接建立关联，并将client hello报文继续传输给数据业务服务器；TLS连接建立完毕，移动终端设备与数据业务服务器之间利用TLS连接传输应用层数据，数据流量归属识别装置根据已提取的业务类型标识，将这些数据流量归属于相应的业务类型。

[0262] 在具体实施时，本系统中还可以有数据业务提供方的密钥中心、以及运营方的密钥中心，分别为业务类型提供装置和数据流量归属识别装置提供与业务类型标识对应的密钥，从而数据流量归属识别装置从client hello报文中提取业务类型标识后，还可以实现对业务类型标识的完整性、是否被冒用进行验证；在业务类型提供装置和数据流量归属识别装置保持系统时间同步的情况下，数据流量归属识别装置还可以对重放进行识别。具体的实施方式此处不再赘述，请参见前面实施例中的相应描述。

[0263] 本申请虽然以较佳实施例公开如上，但其并不是用来限定本申请，任何本领域技术人员在不脱离本申请的精神和范围内，都可以做出可能的变动和修改，因此本申请的保护范围应当以本申请权利要求所界定的范围为准。

[0264] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0265] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0266] 1、计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器

(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0267] 2、本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请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、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

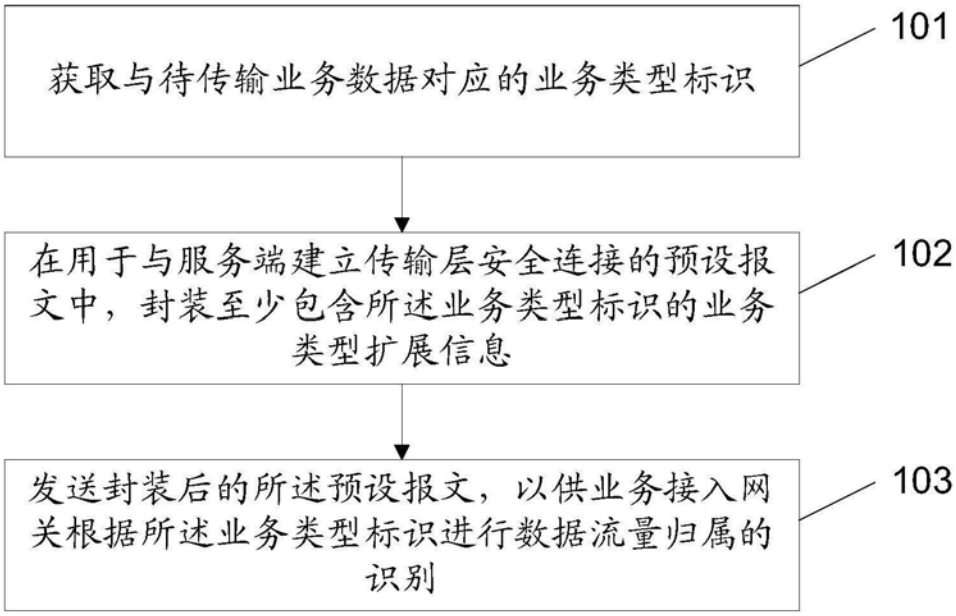

获取与待传输业务数据对应的业务类型标识
101
在用于与服务端建立传输层安全连接的预设报文中，封装至少包含所述业务类型标识的业务类型扩展信息
102
发送封装后的所述预设报文，以供业务接入网关根据所述业务类型标识进行数据流量归属的识别
103

图1

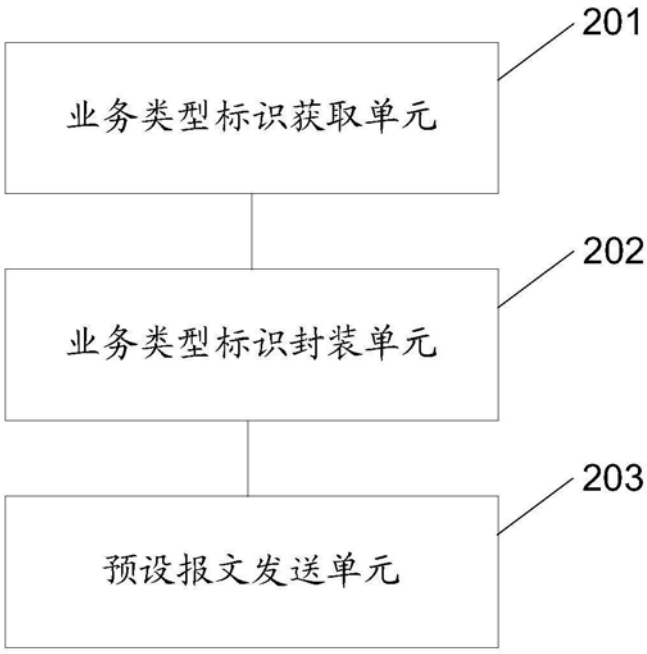

业务类型标识获取单元
201
业务类型标识封装单元
202
预设报文发送单元
203

图2

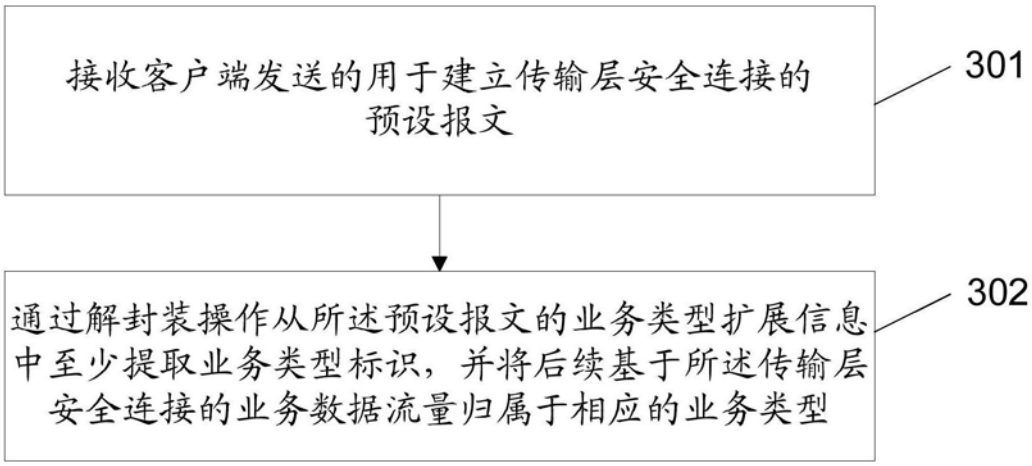

接收客户端发送的用于建立传输层安全连接的预设报文
301
通过解封装操作从所述预设报文的业务类型扩展信息中至少提取业务类型标识，并将后续基于所述传输层安全连接的业务数据流量归属于相应的业务类型
302

图3

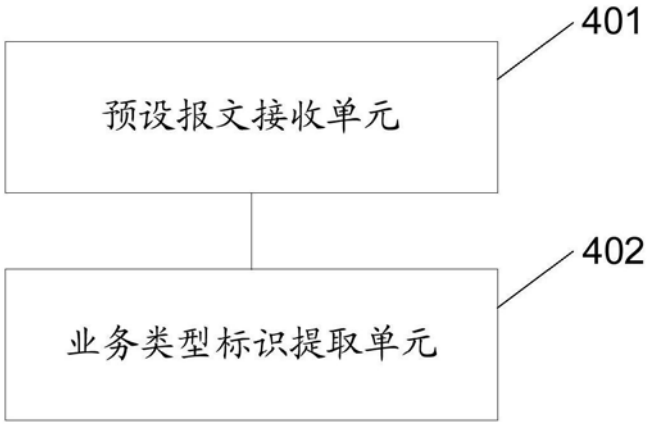

预设报文接收单元
401
业务类型标识提取单元
402

图4

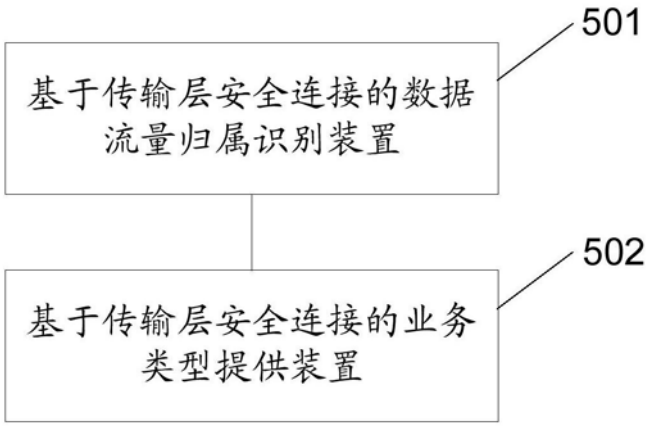

基于传输层安全连接的数据流量归属识别装置
501
基于传输层安全连接的业务类型提供装置
502

图5

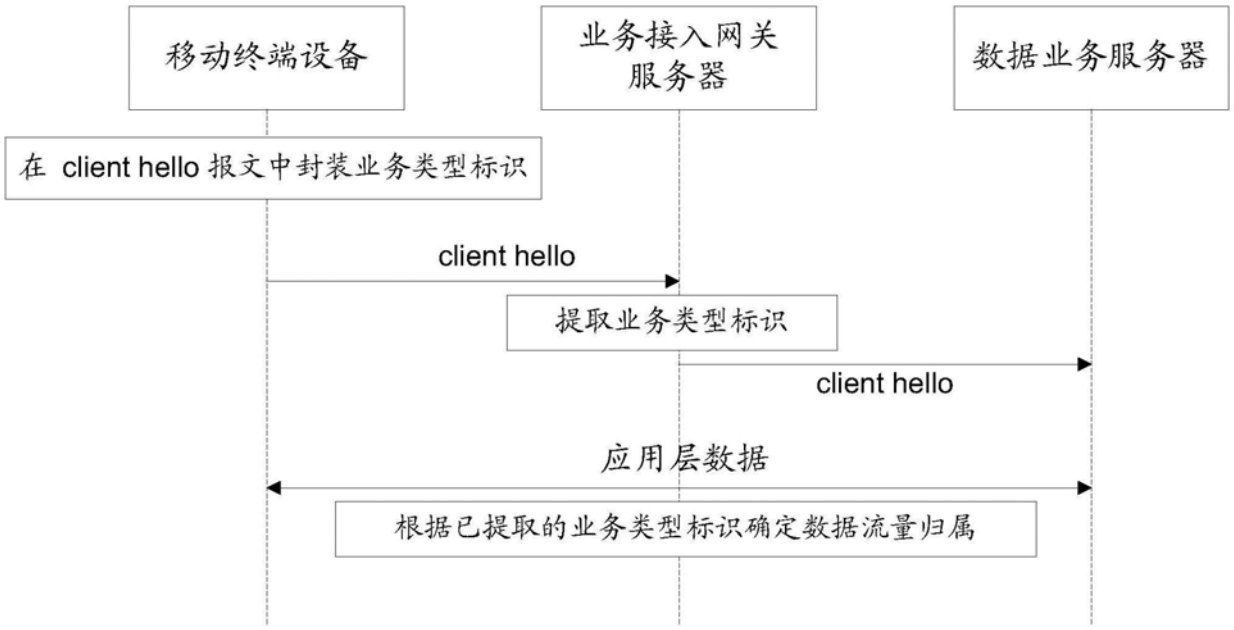

移动终端设备
业务接入网关服务器
数据业务服务器
在 client hello 报文中封装业务类型标识
client hello
提取业务类型标识
client hello
应用层数据
根据已提取的业务类型标识确定数据流量归属

图6