(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 110858834 B
(45)授权公告日 2022.02.08

(21)申请号 201810965714.4

(22)申请日 2018.08.23

(65)同一申请的已公布的文献号
申请公布号 CN 110858834 A

(43)申请公布日 2020.03.03

(73)专利权人 中国电信股份有限公司
地址 100033 北京市西城区金融大街31号

(72)发明人 李昆仑 张敏

(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 孙玉

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/02(2022.01)

(56)对比文件
CN 105577738 A,2016.05.11
CN 107306214 A,2017.10.31
CN 101534262 A,2009.09.16
CN 105577738 A,2016.05.11
WO 9802005 A1,1998.01.15
US 2010275248 A1,2010.10.28
CN 103442256 A,2013.12.11
王建军.《基于SSL的文件安全传输系统研究与设计》.《中国硕士学位论文全文数据库 信息技术辑》.2012,

审查员 王甜甜

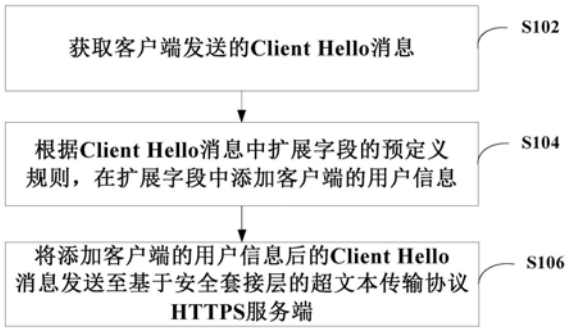
权利要求书3页 说明书10页 附图4页

(54)发明名称

用户信息传输方法、装置、系统和计算机可读存储介质

(57)摘要

本公开涉及一种用户信息传输方法、装置、系统和计算机可读存储介质，涉及通信技术领域。本公开的方法包括：获取客户端发送的Client Hello消息；根据Client Hello消息中扩展字段的预定义规则，在扩展字段中添加客户端的用户信息；将添加客户端的用户信息后的Client Hello消息发送至HTTPS服务端，以便HTTPS服务端获取客户端的用户信息。本公开针对HTTPS会话建立的特点，在HTTPS会话的建立初期的TLS/SSL握手阶段，携带用户信息进行头增强功能，解决了HTTPS报文不支持头增强的问题。



CN 110858834 B

1.一种用户信息传输方法,包括:

获取客户端发送的客户端问候Client Hello消息;

判断所述Client Hello消息中扩展字段中扩展字段的类型是否为预设类型,所述预设类型表示所述扩展字段用于传输用户信息,在所述扩展字段的类型为预设类型的情况下,将所述扩展字段中的已有信息删除,根据所述扩展字段的预定义规则,在所述扩展字段中添加所述客户端的用户信息;

将添加所述客户端的用户信息后的Client Hello消息发送至基于安全套接层的超文本传输协议HTTPS服务端,以便所述HTTPS服务端获取所述客户端的用户信息;

其中,所述在所述扩展字段中添加所述客户端的用户信息包括:

在扩展字段类型对应的位置添加预设类型值,所述预设类型值表示所述扩展字段用于传输用户信息;

在子扩展字段类型对应的位置添加所述用户信息的类型值,并在所述用户信息的类型值之后的字节中添加对应的用户信息值,不同类型的用户信息添加至不同子扩展字段中;

在各个子扩展字段长度和扩展字段总长度对应的位置分别添加各个子扩展字段的长度值和扩展字段的总长度值。

2.根据权利要求1所述的用户信息传输方法,其中,

所述在所述扩展字段中添加所述客户端的用户信息包括:

根据所述客户端与所述HTTPS服务端预先协商的加密方式,对添加所述客户端的用户信息后的扩展字段进行加密;

或者,根据所述客户端与所述HTTPS服务端预先协商的加密方式,对所述客户端的用户信息进行加密,将加密的所述用户信息添加至所述扩展字段中。

3.根据权利要求1所述的用户信息传输方法,其中,

在所述扩展字段中添加所述客户端的用户信息包括:

根据添加所述用户信息后的所述扩展字段的长度,修改所述Client Hello消息中安全套接层SSL、IP层的信息长度值和校验和值。

4.根据权利要求1所述的用户信息传输方法,其中,

所述在所述扩展字段中添加所述客户端的用户信息包括:

在所述Client Hello消息访问的HTTPS服务端的地址信息或类型信息在预设地址信息或类型信息的范围内的情况下,在所述扩展字段中添加所述客户端的用户信息。

5.根据权利要求1-4任一项所述的用户信息传输方法,其中,

所述用户信息包括用户号码;

所述方法还包括:

HTTPS服务端获取所述用户号码,根据所述用户号码对所述客户端进行认证。

6.根据权利要求1-4任一项所述的用户信息传输方法,其中,

所述用户信息包括用户私网IP地址和路径信息;

所述方法还包括:

HTTPS服务端获取所述用户私网IP地址和路径信息,向核心网设备发送服务质量调整请求,所述服务质量调整请求包括所述用户私网IP地址和路径信息,以便所述核心网设备根据所述用户私网IP地址和路径信息调整所述客户端的服务质量等级。

7.一种用户信息传输装置,包括:

信息获取模块,用于获取客户端发送的客户端问候Client Hello消息;

字段检测模块,用于判断所述Client Hello消息中扩展字段中扩展字段的类型是否为预设类型,所述预设类型表示所述扩展字段用于传输用户信息;在所述扩展字段的类型为预设类型的情况下,将所述扩展字段中的已有信息删除;

信息添加模块,用于根据所述扩展字段的预定义规则,在所述扩展字段中添加所述客户端的用户信息;

信息发送模块,用于将添加所述客户端的用户信息后的Client Hello消息发送至基于安全套接层的超文本传输协议HTTPS服务端,以便所述HTTPS服务端获取所述客户端的用户信息;

其中,所述信息添加模块用于在扩展字段类型对应的位置添加预设类型值,所述预设类型值表示所述扩展字段用于传输用户信息;在子扩展字段类型对应的位置添加所述用户信息的类型值,并在所述用户信息的类型值之后的字节中添加对应的用户信息值,不同类型的用户信息添加至不同子扩展字段中;在各个子扩展字段长度和扩展字段总长度对应的位置分别添加各个子扩展字段的长度值和扩展字段的总长度值。

8.根据权利要求7所述的用户信息传输装置,其中,

所述信息添加模块用于根据所述客户端与所述HTTPS服务端预先协商的加密方式,对添加所述客户端的用户信息后的扩展字段进行加密;或者,根据所述客户端与所述HTTPS服务端预先协商的加密方式,对所述客户端的用户信息进行加密,将加密的所述用户信息添加至所述扩展字段中。

9.根据权利要求7所述的用户信息传输装置,其中,

所述信息添加模块用于根据添加所述用户信息后的所述扩展字段的长度,修改所述Client Hello消息中安全套接层SSL、IP层的信息长度值和校验和值。

10.根据权利要求7所述的用户信息传输装置,其中,

所述信息添加模块用于在所述Client Hello消息访问的HTTPS服务端的地址信息或类型信息在预设地址信息或类型信息的范围内的情况下,在所述扩展字段中添加所述客户端的用户信息。

11.一种用户信息传输装置,包括:

存储器;以及

耦接至所述存储器的处理器,所述处理器被配置为基于存储在所述存储器设备中的指令,执行如权利要求1-6任一项所述的用户信息传输方法。

12.一种计算机可读存储介质,其上存储有计算机程序,其中,该程序被处理器执行时实现权利要求1-6任一项所述方法的步骤。

13.一种用户信息传输系统,包括:权利要求7-11任一项所述的用户信息传输装置;以及

HTTPS服务端,用于解析所述Client Hello消息获取所述客户端的用户信息。

14.根据权利要求13所述的用户信息传输系统,其中,

所述用户信息包括用户号码;

所述HTTPS服务端用于获取所述用户号码,根据所述用户号码对所述客户端进行认证;

或者,所述用户信息包括用户私网IP地址和路径信息;

所述HTTPS服务端用于获取所述用户私网IP地址和路径信息,向核心网设备发送服务质量调整请求,所述服务质量调整请求包括所述用户私网IP地址和路径信息,以便所述核心网设备根据所述用户私网IP地址和路径信息调整所述客户端的服务质量等级。

用户信息传输方法、装置、系统和计算机可读存储介质

技术领域

[0001] 本公开涉及通信技术领域，特别涉及一种用户信息传输方法、装置、系统和计算机可读存储介质。

背景技术

[0002] HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer，基于安全套接层的超文本传输协议)主要用于安全的HTTP(Hyper Text Transfer Protocol，超文本传输协议)数据传输。因其对数据传输的安全性、完整性、正确性都优于HTTP协议，逐渐成为替代HTTP的主流应用层协议。目前主流业务应用均已向HTTPS协议转移。

[0003] 在现有HTTP报文传输过程中，可以根据业务应用侧需求对终端应用与服务器之间的报文头进行增强修改，以便携带用户相关信息到业务应用的服务端使用。

发明内容

[0004] 发明人发现：HTTP头增强是基于业务请求报文本身进行解析和插入，但HTTPS业务报文本身是加密传输，无法针对HTTPS的业务报文进行解析和插入，因此HTTP头增强方法无法适用于HTTPS协议。

[0005] 本公开所要解决的一个技术问题是：如何在HTTPS的报文中传输用户信息。

[0006] 根据本公开的一些实施例，提供的一种用户信息传输方法，包括：获取客户端发送的客户端问候Client Hello消息；根据Client Hello消息中扩展字段的预定义规则，在扩展字段中添加客户端的用户信息；将添加客户端的用户信息后的Client Hello消息发送至基于安全套接层的超文本传输协议HTTPS服务端，以便HTTPS服务端获取客户端的用户信息。

[0007] 在一些实施例中，在扩展字段中添加客户端的用户信息包括：在扩展字段类型对应的位置添加预设类型值，预设类型值表示扩展字段用于传输用户信息；在子扩展字段类型对应的位置添加用户信息的类型值，并在用户信息的类型值之后的字节中添加对应的用户信息值，不同类型的用户信息以及添加至不同子扩展字段中；在各个子扩展字段长度和扩展字段总长度对应的位置分别添加各个子扩展字段的长度值和扩展字段的总长度值。

[0008] 在一些实施例中，在扩展字段中添加客户端的用户信息之前还包括：判断扩展字段中扩展字段的类型是否为预设类型，预设类型表示扩展字段用于传输用户信息；在扩展字段的类型为预设类型的情况下，将扩展字段中的已有信息删除。

[0009] 在一些实施例中，在扩展字段中添加客户端的用户信息包括：根据客户端与HTTPS服务端预先协商的加密方式，对添加客户端的用户信息后的扩展字段进行加密；或者，根据客户端与HTTPS服务端预先协商的加密方式，对客户端的用户信息进行加密，将加密的用户信息添加至扩展字段中。

[0010] 在一些实施例中，在扩展字段中添加客户端的用户信息包括：根据添加用户信息后的扩展字段的长度，修改Client Hello消息中安全套接层SSL、IP层的信息长度值和校验

和值。

[0011] 在一些实施例中，在扩展字段中添加客户端的用户信息包括：在Client Hello消息访问的HTTPS服务端的地址信息或类型信息在预设地址信息或类型信息的范围内的情况下，在扩展字段中添加客户端的用户信息。

[0012] 在一些实施例中，用户信息包括用户号码；该方法还包括：HTTPS服务端获取用户号码，根据用户号码对客户端进行认证。

[0013] 在一些实施例中，用户信息包括用户私网IP地址和路径信息；该方法还包括：HTTPS服务端获取用户私网IP地址和路径信息，向核心网设备发送服务质量调整请求，服务质量调整请求包括用户私网IP地址和路径信息，以便核心网设备根据用户私网IP地址和路径信息调整客户端的服务质量等级。

[0014] 根据本公开的一些实施例，提供的一种用户信息传输装置，包括：信息获取模块，用于获取客户端发送的客户端问候Client Hello消息；信息添加模块，用于根据Client Hello消息中扩展字段的预定义规则，在扩展字段中添加客户端的用户信息；信息发送模块，用于将添加客户端的用户信息后的Client Hello消息发送至基于安全套接层的超文本传输协议HTTPS服务端，以便HTTPS服务端获取客户端的用户信息。

[0015] 在一些实施例中，信息添加模块用于在扩展字段类型对应的位置添加预设类型值，预设类型值表示扩展字段用于传输用户信息；在子扩展字段类型对应的位置添加用户信息的类型值，并在用户信息的类型值之后的字节中添加对应的用户信息值，不同类型的用户信息以及添加至不同子扩展字段中；在各个子扩展字段长度和扩展字段总长度对应的位置分别添加各个子扩展字段的长度值和扩展字段的总长度值。

[0016] 在一些实施例中，该装置还包括：字段检测模块，用于判断扩展字段中扩展字段的类型是否为预设类型，预设类型表示扩展字段用于传输用户信息；在扩展字段的类型为预设类型的情况下，将扩展字段中的已有信息删除。

[0017] 在一些实施例中，信息添加模块用于根据客户端与HTTPS服务端预先协商的加密方式，对添加客户端的用户信息后的扩展字段进行加密；或者，根据客户端与HTTPS服务端预先协商的加密方式，对客户端的用户信息进行加密，将加密的用户信息添加至扩展字段中。

[0018] 在一些实施例中，信息添加模块用于根据添加用户信息后的扩展字段的长度，修改Client Hello消息中安全套接层SSL、IP层的信息长度值和校验和值。

[0019] 在一些实施例中，信息添加模块用于在Client Hello消息访问的HTTPS服务端的地址信息或类型信息在预设地址信息或类型信息的范围内的情况下，在扩展字段中添加客户端的用户信息。

[0020] 根据本公开的一些实施例，提供的一种用户信息传输装置，包括：存储器；以及耦接至存储器的处理器，处理器被配置为基于存储在存储器设备中的指令，执行如前述任意实施例的用户信息传输方法。

[0021] 根据本公开的一些实施例，提供的一种计算机可读存储介质，其上存储有计算机程序，其中，该程序被处理器执行时实现前述任意实施例的用户信息传输方法。

[0022] 根据本公开的一些实施例，提供的一种用户信息传输系统，包括：前述任意实施例的用户信息传输装置，以及HTTPS服务端，用于解析Client Hello消息获取客户端的用户信

息。

[0023] 在一些实施例中,用户信息包括用户号码;HTTPS服务端用于获取用户号码,根据用户号码对客户端进行认证;或者,用户信息包括用户私网IP地址和路径信息;HTTPS服务端用于获取用户私网IP地址和路径信息,向核心网设备发送服务质量调整请求,服务质量调整请求包括用户私网IP地址和路径信息,以便核心网设备根据用户私网IP地址和路径信息调整客户端的服务质量等级。

[0024] 本公开中获取客户端发送的Client Hello消息,在Client Hello消息的扩展字段中添加客户端的用户信息,进而将携带用户信息的Client Hello消息发送至HTTPS服务端,以便HTTPS服务端获取所述客户端的用户信息并使用。本公开针对HTTPS会话建立的特点,在HTTPS会话的建立初期的TLS/SSL(Secure Sockets Layer/Transport Layer Security,安全套接层/传输层安全)握手阶段,携带用户信息进行头增强功能,解决了HTTPS报文不支持头增强的问题。

[0025] 通过以下参照附图对本公开的示例性实施例的详细描述,本公开的其它特征及其优点将会变得清楚。

附图说明

[0026] 为了更清楚地说明本公开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公开的一些实施例,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。

[0027] 图1示出本公开的一些实施例的用户信息传输方法的流程示意图。

[0028] 图2示出本公开的另一些实施例的用户信息传输方法的流程示意图。

[0029] 图3示出本公开的一些实施例的用户信息传输装置的结构示意图。

[0030] 图4示出本公开的另一些实施例的用户信息传输装置的结构示意图。

[0031] 图5示出本公开的又一些实施例的用户信息传输装置的结构示意图。

[0032] 图6示出本公开的一些实施例的用户信息传输系统的结构示意图。

具体实施方式

[0033] 下面将结合本公开实施例中的附图,对本公开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公开一部分实施例,而不是全部的实施例。以下对至少一个示例性实施例的描述实际上仅仅是说明性的,决不作为对本公开及其应用或使用的任何限制。基于本公开中的实施例,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,都属于本公开保护的范围。

[0034] 本公开提出一种用户信息传输方法,可用于HTTPS报文的头部增强,下面结合图1进行描述。

[0035] 图1为本公开用户信息传输方法一些实施例的流程图。如图1所示,该实施例的方法包括:步骤S102～步骤S106。

[0036] 在步骤S102中,获取客户端发送的Client Hello(客户端问候)消息。

[0037] Client Hello消息是HTTPS会话的建立初期的TLS/SSL握手阶段传递的消息。TLS/

SSL握手阶段主要用于客服端与服务端协商后续业务数据的密钥。TLS/SSL握手阶段包括Client Hello消息、Server Hello(服务器问候)消息、Client Key Exchange(客户端密钥交换)消息、Change Cipher Spec(更改密码规格)消息等。这些消息的交互过程属于现有技术,在此不再赘述。可以利用用户信息传输装置或者PGW(Packet Data Network GateWay,分组数据网关)获取Client Hello消息。

[0038] 在步骤S104中,根据Client Hello消息中扩展字段的预定义规则,在扩展字段中添加客户端的用户信息。

[0039] Client Hello消息可以携带扩展(Extension)字段。可以预先定义Client Hello消息中Extension字段的添加和解析规则并配置在相关设备中。例如,使PGW根据预定义规则对Extension字段进行解析和添加,并且使HTTPS服务端后续能够顺利对Extension字段进行解析。可以通过DPI(Deep Packet Inspection,深度报文检测)技术对Client Hello消息进行解析,解析出Extension字段。

[0040] 进一步,在一些实施例中,Extension字段例如包含扩展字段类型(Extension_Type)字段,扩展字段总长度(Total_Length)字段,后续为扩展头数据包括子扩展(Sub Extension)字段列表,每个Sub Extension字段包括Sub Extension的类型(Type),Sub Extension的长度(Length)和用户数据。

[0041] 在Extension_Type对应的位置添加预设类型值。预设类型值表示扩展字段用于传输用户信息,例如,预设类型值为1777,在占用2个字节的情况下可以转换为0x45 0x71。

[0042] 在Sub Extension字段类型(Type)对应的位置添加用户信息的类型值,并在用户信息的类型值之后的字节中添加对应的用户信息值,不同类型的用户信息以及添加至不同子扩展字段中。例如,用户信息可以包括:手机号、私网IP地址、IMSI(International Mobile Subscriber Identification Number,国际移动用户识别码)、IMEI(International Mobile Equipment Identity,国际移动设备识别码)、ECGI(E-UTRAN Cell Global Identifier,E-UTRAN小区全局标识符)、SGW(Serving GateWay,服务网关)IP、PGW IP、时间戳中至少一项,具体携带哪些用于信息可以根据业务需求进行灵活选取,头增强携带的信息也可以根据网络运营需要灵活使用。

[0043] 例如,Sub Extension的Type可以占用1个字节,定义如下:1表示该Sub Extension携带手机号码,2表示该Sub Extension携带私网IP地址,3表示该Sub Extension携带IMSI,4表示该Sub Extension携带IMEI,5表示该Sub Extension携带ECGI,6表示该Sub Extensionn携带SGW IP,7表示Sub Extension携带PGW IP,8表示Sub Extension携带时间戳。

[0044] 在各个Sub Extension的Length和Total_Length对应的位置分别添加各个Sub Extension的长度值和Extension的总长度值。例如,Sub Extension的Length占2个字节,Total_Length占2个字节。

[0045] 下面以手机号码8613312345678,私网IP地址221.32.1.64,IMSI为460001999090001,IMEI为560001999030000,ECGI为46002238008832,SGW IP为1.1.1.1,PGW IP为2.2.2.2为例,描述Extension字段的添加。

[0046] 1.Extension_Type值为17777,转为2字节为0x45 0x71。

[0047] 2.Total_Length长度值为80,转为2字节为0x00 0x50,不足2字节前面补0。

[0048] 3.用于承载手机号的Sub Extension：

[0049] (3-1)Type值为1,转为1字节表示为0x01；

[0050] (3-2)Length值为8,转为2字节为0x00 0x08,不足2字节前面补0；

[0051] (3-3)Value值为手机号8613312345678,转为8字节为0x00 0x000x07 0xd5 0x71 0x6c 0x36 0x4e,不足8字节前面补0。

[0052] 4.用于承载私网IP的Sub Extension：

[0053] (4-1)Type值为2,转为1字节为0x02；

[0054] (4-2)Length值为4,转为2字节为0x00 0x04,不足2字节前面补0；

[0055] (4-3)Value值为用户私网IP 224.32.1.64,转为4字节为0xe00x20 0x01 0x40。

[0056] 5.用于承载IMSI的Sub Extension：

[0057] (5-1)Type值为3,转为1字节为0x03；

[0058] (5-2)Length值为8,转为2字节为0x00 0x08,不足2字节前面补0；

[0059] (5-3)Value值为460001999090001,转为8字节为0x00 0x010xA2 0x5E 0x8F 0xC0 0x71 0x51;不足8字节前面补0。

[0060] 6.用于承载源IMEI的Sub Extension：

[0061] (6-1)Type值为4,转为用1字节为0x04；

[0062] (6-2)Length值为8,转为2字节为0x00 0x08,不足2字节前面补0；

[0063] (6-3)Value值为560001999030000,转为8字节为0x00 0x010xFD 0x51 0xA0 0x39 0xC6 0xF0,不足8字节前面补0。

[0064] 7.用于承载源ECGI的Sub Extension：

[0065] (7-1)Type值为5,转为1字节为0x05；

[0066] (7-2)Length值为8,转为2字节为0x00 0x08,不足2字节前面补0；

[0067] (7-3)Value值为46002238008832,转为8字节为0x00 0x00 0x290xD6 0xBB 0x0E 0x2E 0x00;不足8字节前面补0。

[0068] 8.用于承载源SGW IP的Sub Extension：

[0069] (8-1)Type值为6,转为1字节为0x06；

[0070] (8-2)Length值为4,转为2字节为0x00 0x04,不足2字节前面补0；

[0071] (8-3)Value值为1.1.1.1,转为4字节为0x01 0x01 0x01 0x01。

[0072] 9.用于承载源PGW IP的Sub Extension：

[0073] (9-1)Type值为7,转为1字节为0x07；

[0074] (9-2)Length值为4,转为2字节为0x00 0x04,不足2字节前面补0；

[0075] (9-3)Value值为2.2.2.2,转为4字节为0x02 0x02 0x02 0x02。

[0076] 10.用于标识时间戳的Sub Extension：

[0077] (10-1)Type值为8,转为1字节为0x08；

[0078] (10-2)Length值为8,转为2字节为0x00 0x08,不足8字节前面补0；

[0079] (10-3)时间戳值为1503368319,代表2017-08-22 10:18:39,Value值为1503368319,转为8字节为0x00 0x00 0x00 0x00 0x59 0x9B 0x940x7F。

[0080] 因此,自动添加的Extension为：

[0081] 0x45 0x71 0x00 0x50

[0082] 0x01 0x00 0x08 0x00 0x00 0x07 0xd5 0x71 0x6c 0x36 0x4e

[0083] 0x02 0x00 0x04 0xe0 0x20 0x01 0x40

[0084] 0x03 0x00 0x08 0x00 0x01 0xA2 0x5E 0x8F 0xC0 0x71 0x51

[0085] 0x04 0x00 0x08 0x00 0x01 0xFD 0x51 0xA0 0x39 0xC6 0xF0

[0086] 0x05 0x00 0x08 0x00 0x00 0x29 0xD6 0xBB 0x0E 0x2E 0x00

[0087] 0x06 0x00 0x04 0x01 0x01 0x01 0x01

[0088] 0x07 0x00 0x04 0x02 0x02 0x02 0x02

[0089] 0x08 0x00 0x08 0x00 0x00 0x00 0x00 0x59 0x9B 0x94 0x7F

[0090] 添加扩展字段后,需要对Client Hello消息中其他对应的信息进行修改,以保证信息的准确性。在一些实施例中,根据添加用户信息后的扩展字段的长度,修改报文中Client Hello消息的长度值,Client Hello消息中安全套接层SSL、IP层的信息长度值和校验和值(checksum)。

[0091] 在添加扩展字段的情况下,还可以根据MTU(Maximum Transmission Unit,最大传输单元)对进行Client Hello消息的数据包长度检测。在Client Hello消息的数据包长度超过MTU的情况下,对扩展字段的进行删减,将扩展字段超出的部分内容删除。

[0092] 为了进一步增加信息传递的安全性。在一些实施例中,根据客户端与HTTPS服务端预先协商的加密方式,对添加客户端的用户信息后的扩展字段进行加密;或者,根据客户端与HTTPS服务端预先协商的加密方式,对客户端的用户信息进行加密,将加密的用户信息添加至扩展字段中。例如,可以采用RC4(Rivest Cipher 4)对用户信息或者扩展字段。加密和解密方式可以在PGW或服务端进行预配置,或者,客户端与服务端预先通过协商确定。

[0093] 为了进一步增加Client Hello消息的安全性,避免出现头增强欺诈,在添加扩展字段之前,可以对Client Hello消息进行检验。在扩展字段的类型为预设类型的情况下,将扩展字段中的已有信息删除。即如果扩展字段已经被添加,并且解析出扩展字段的类型为预设类型,例如1777,则将已有的信息删除,重新按照上述方法添加扩展字段。

[0094] 为了适应不同的HTTPS服务端的需求,可以针对访问不同的服务端的Client Hello消息进行识别,并确定是否添加扩展字段以及扩展字段的内容等。在一些实施例中,在Client Hello消息访问的HTTPS服务端的地址信息(例如IP地址、域名等)或类型信息在预设地址信息或类型信息的范围内的情况下,在扩展字段中添加客户端的用户信息。进一步,根据Client Hello消息访问的HTTPS服务端的地址信息或类型信息,确定在扩展字段中添加客户端的用户信息的类型。例如,针对发往某些服务端的Client Hello消息在扩展字段中添加客户端的手机号码,而针对发往另一些服务端的Client Hello消息在扩展字段中添加客户端的私网IP地址等。可以根据服务端的请求,在扩展字段添加装置中设置不同服务端对应的扩展字段添加方式和添加的用户信息的类型。

[0095] 在步骤S106中,将添加客户端的用户信息后的Client Hello消息发送至基于安全套接层的超文本传输协议HTTPS服务端,以便HTTPS服务端获取客户端的用户信息。

[0096] 上述实施例的方法中获取客户端发送的Client Hello消息,在Client Hello消息的扩展字段中添加客户端的用户信息,进而将携带用户信息的Client Hello消息发送至HTTPS服务端,以便HTTPS服务端获取客户端的用户信息并使用。上述实施例的方法针对HTTPS会话建立的特点,在HTTPS会话的建立初期的TLS/SSL(Secure Sockets Layer/

Transport Layer Security,安全套接层/传输层安全)握手阶段,携带用户信息进行头增强功能,解决了HTTPS报文不支持头增强的问题。

[0097] 本公开的HTTPS头增强方案,可以携带用户的信息到达服务端,服务端获取用户信息可以对用户进行识别、认证和其他处理。下面结合图2描述本公开中用户信息应用的一些实施例。

[0098] 图2为本公开用户信息传输方法一些实施例的流程图。如图2所示,该实施例的方法包括:步骤S202～步骤S222。

[0099] 步骤S202,客户端向服务端发起认证请求。

[0100] 认证请求的应用层协议为HTTPS。

[0101] 步骤S204,HTTPS会话建立过程中,客户端发送Client Hello消息。

[0102] 步骤S206,用户信息传输装置获取客户端发送的Client Hello消息。

[0103] 用户信息传输装置例如设置于PGW中,或者利用PGW实现用户信息传输装置的功能。用户信息传输装置可以通过DPI功能检测Client Hello消息。

[0104] 步骤S208,用户信息传输装置根据头增强预配置规则,判断是否对Client Hello消息进行扩展字段的修改。如果是,则执行步骤S210,否则执行步骤S211。

[0105] 头增强预配置规则例如包括:HTTPS服务端的地址信息或类型信息,以及对应的是否添加扩展字段和扩展字段中添加的用户信息的类型。用户信息传输装置根据Client Hello消息中的HTTPS服务端的地址信息或类型信息与头增强预配置规则进行匹配,确定是否对Client Hello消息进行扩展字段的修改。

[0106] 步骤S210,用户信息传输装置检测Client Hello消息中扩展字段的类型是否为预设类型。如果为预设类型,则执行步骤S212,否则执行步骤S214。

[0107] 步骤S212,用户信息传输装置将扩展字段中的已有信息删除。

[0108] 步骤S214,用户信息传输装置根据Client Hello消息中扩展字段的预定义规则,在扩展字段中添加客户端的用户信息。

[0109] 用户信息包括用户的手机号码。可以对用户信息进行加密后添加到扩展字段中。

[0110] 步骤S216,用户信息传输装置修改Client Hello消息中的长度字段,并修改SSL层、IP层的长度值,重新计算并替换原报文中的checksum值,根据MTU检测头增强后的报文为合法报文。

[0111] 步骤S218,用户信息传输装置将Client Hello消息发送至服务端。

[0112] 步骤S220,服务端解析Client Hello消息,获取用户信息。

[0113] 步骤S222,服务端根据用户号码对客户端进行认证。

[0114] 若认证成功,由服务端通知对应的业务应用服务器完成登录;若认证失败,由服务端通知业务应用服务器网络认证失败,可进行后续其他登录方式。

[0115] 目前用户进行登录认证的过程中,一般由服务器发送短信验证码,由用户输入验证码,验证登录信息是由用户的手机号发出的。而利用上述实施例的方法,由用户信息传输装置直接在Client Hello消息,以使服务端认证该消息发送的手机号。整个认证过程用户不需要短信验证码、不需要中断现有业务,不需要额外操作,完全实现无感认证,提升用户体验。并且由用户信息传输装置添加用户手机号码,进一步还可以对用户手机号码进行加密传输,提高了传输过程的安全性,提高了认证的安全性和准确性。

[0116] 下面描述用户信息的应用的另一些实施例。

[0117] 在一些实施例中，用户信息包括用户私网IP地址。HTTPS服务端获取用户私网IP地址向核心网设备发送服务质量调整请求，服务质量调整请求包括用户私网IP地址，以便核心网设备根据用户私网IP地址调整客户端的服务质量等级。

[0118] 针对不同等级的用户，服务端可以为其提供不同等级的服务质量。例如，优先级高的用户可以享受速率更高的服务。服务端通过监测不同等级的客户端的服务质量，可以实时向核心网请求调整用户的服务质量(QoS)。服务端可以通过Client Hello消息获取客户端的用户私网IP地址，向核心网发送服务质量调整请求携带用户私网IP地址，从而使核心网根据用户私网IP地址找到用户对应的承载，调整用户的服务质量。

[0119] 进一步，在用户私网IP地址可能重复的情况下，Client Hello消息可以携带用户的路径信息，例如，SGW的IP地址和PGW的IP地址中至少一项。HTTPS服务端获取用户私网IP地址和路径信息，向核心网设备发送服务质量调整请求，服务质量调整请求包括用户私网IP地址和路径信息，以便核心网设备根据用户私网IP地址和路径信息调整客户端的服务质量等级。

[0120] 上述实施例的方法，服务端能够自动根据用户的实时服务质量，对不同用户的服务进行调整，满足不同用户的需求，提升用户体验。

[0121] 在一些实施例中，用户信息包括：用户的位置信息，例如，ECGI信息。HTTPS服务端获取用户的位置信息，根据用户的位置为用户推送相关的应用信息。通过该实施例的方法，服务端可以获取用户的位置信息，根据用户的位置推送相关的服务，提升用户体验。

[0122] 在一些实施例中，用户信息包括：时间戳。HTTPS服务端根据时间戳确认Client Hello消息是否在有效时间内，对于已过有效时间的Client Hello消息不进行处理。通过该实施例的方法，可以提高消息传输的安全性，减少服务端的无效工作和工作负担。

[0123] 本公开还提供一种用户信息传输装置，下面结合图3进行描述。用户信息传输装置可以设置于PGW中，或者利用PGW实现用户信息传输装置的功能。

[0124] 图3为本公开用户信息传输装置的一些实施例的结构图。如图3所示，该实施例的装置30包括：信息获取模块302，信息添加模块304，信息发送模块306。

[0125] 信息获取模块302，用于获取客户端发送的客户端问候Client Hello消息。

[0126] 信息添加模块304，用于根据Client Hello消息中扩展字段的预定义规则，在扩展字段中添加客户端的用户信息。

[0127] 在一些实施例中，信息添加模块304用于在扩展字段类型对应的位置添加预设类型值，预设类型值表示扩展字段用于传输用户信息；在子扩展字段类型对应的位置添加用户信息的类型值，并在用户信息的类型值之后的字节中添加对应的用户信息值，不同类型的用户信息以及添加至不同子扩展字段中；在各个子扩展字段长度和扩展字段总长度对应的位置分别添加各个子扩展字段的长度值和扩展字段的总长度值。

[0128] 在一些实施例中，信息添加模块304用于根据客户端与HTTPS服务端预先协商的加密方式，对添加客户端的用户信息后的扩展字段进行加密；或者，根据客户端与HTTPS服务端预先协商的加密方式，对客户端的用户信息进行加密，将加密的用户信息添加至扩展字段中。

[0129] 在一些实施例中，信息添加模块304用于根据添加用户信息后的扩展字段的长度，

修改Client Hello消息中安全套接层SSL、IP层的信息长度值和校验和值。

[0130] 在一些实施例中，信息添加模块304用于在Client Hello消息访问的HTTPS服务端的地址信息或类型信息在预设地址信息或类型信息的范围内的情况下，在扩展字段中添加客户端的用户信息。

[0131] 信息发送模块306，用于将添加客户端的用户信息后的Client Hello消息发送至基于安全套接层的超文本传输协议HTTPS服务端，以便HTTPS服务端获取客户端的用户信息。

[0132] 在一些实施例中，用户信息传输装置30还可以包括：字段检测模块303，用于判断扩展字段中扩展字段的类型是否为预设类型，预设类型表示扩展字段用于传输用户信息；在扩展字段的类型为预设类型的情况下，将扩展字段中的已有信息删除。

[0133] 本公开的实施例中的用户信息传输装置可各由各种计算设备或计算机系统来实现，下面结合图4以及图5进行描述。

[0134] 图4为本公开用户信息传输装置的一些实施例的结构图。如图4所示，该实施例的装置40包括：存储器410以及耦接至该存储器410的处理器420，处理器420被配置为基于存储在存储器410中的指令，执行本公开中任意一些实施例中的用户信息传输方法。

[0135] 其中，存储器410例如可以包括系统存储器、固定非易失性存储介质等。系统存储器例如存储有操作系统、应用程序、引导装载程序(Boot Loader)、数据库以及其他程序等。

[0136] 图5为本公开用户信息传输装置的另一些实施例的结构图。如图5所示，该实施例的装置50包括：存储器510以及处理器520，分别与存储器410以及处理器420类似。还可以包括输入输出接口530、网络接口540、存储接口550等。这些接口530，540，550以及存储器510和处理器520之间例如可以通过总线560连接。其中，输入输出接口530为显示器、鼠标、键盘、触摸屏等输入输出设备提供连接接口。网络接口540为各种联网设备提供连接接口，例如可以连接到数据库服务器或者云端存储服务器等。存储接口550为SD卡、U盘等外置存储设备提供连接接口。

[0137] 本公开还提供一种用户信息传输系统，下面结合图6进行描述。

[0138] 图6为本公开用户信息传输系统的一些实施例的结构图。如图6所示，该实施例的系统6包括：前述任意实施例的用户信息传输装置30/40/50；以及HTTPS服务端62，用于解析Client Hello消息获取客户端的用户信息。

[0139] 在一些实施例中，用户信息包括用户号码；HTTPS服务端62用于获取用户号码，根据用户号码对客户端进行认证

[0140] 在一些实施例中，用户信息包括用户私网IP地址和路径信息；HTTPS服务端62用于获取用户私网IP地址和路径信息，向核心网设备发送服务质量调整请求，服务质量调整请求包括用户私网IP地址和路径信息，以便核心网设备根据用户私网IP地址和路径信息调整客户端的服务质量等级。

[0141] 本领域内的技术人员应当明白，本公开的实施例可提供为方法、系统、或计算机程序产品。因此，本公开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，本公开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非瞬时性存储介质(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。

[0142] 本公开是参照根据本公开实施例的方法、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。应理解为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。

[0143] 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。

[0144] 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。

[0145] 以上所述仅为本公开的较佳实施例,并不用以限制本公开,凡在本公开的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本公开的保护范围之内。

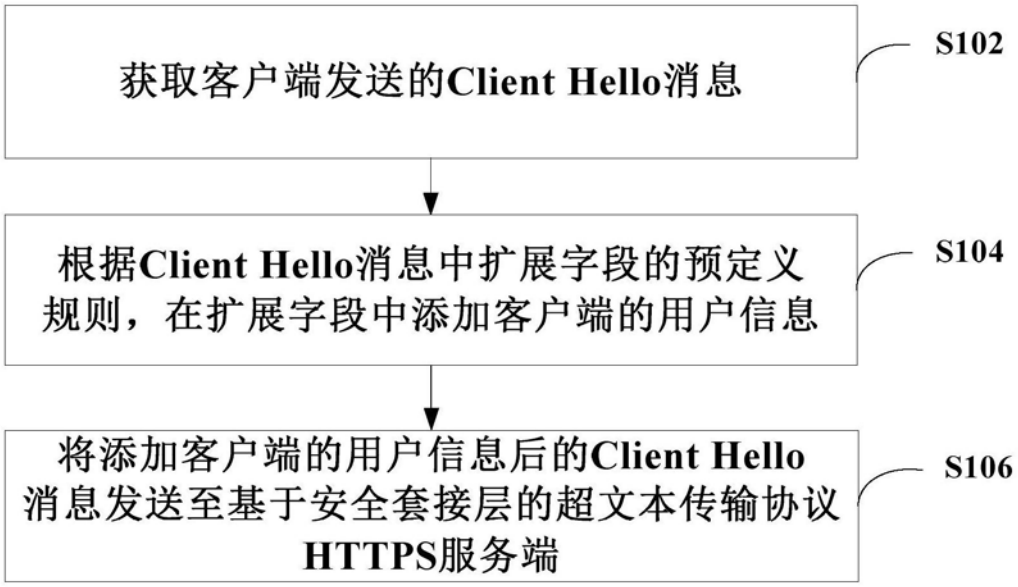

获取客户端发送的Client Hello消息
S102
根据Client Hello消息中扩展字段的预定义规则，在扩展字段中添加客户端的用户信息
S104
将添加客户端的用户信息后的Client Hello消息发送至基于安全套接层的超文本传输协议HTTPS服务端
S106

图1

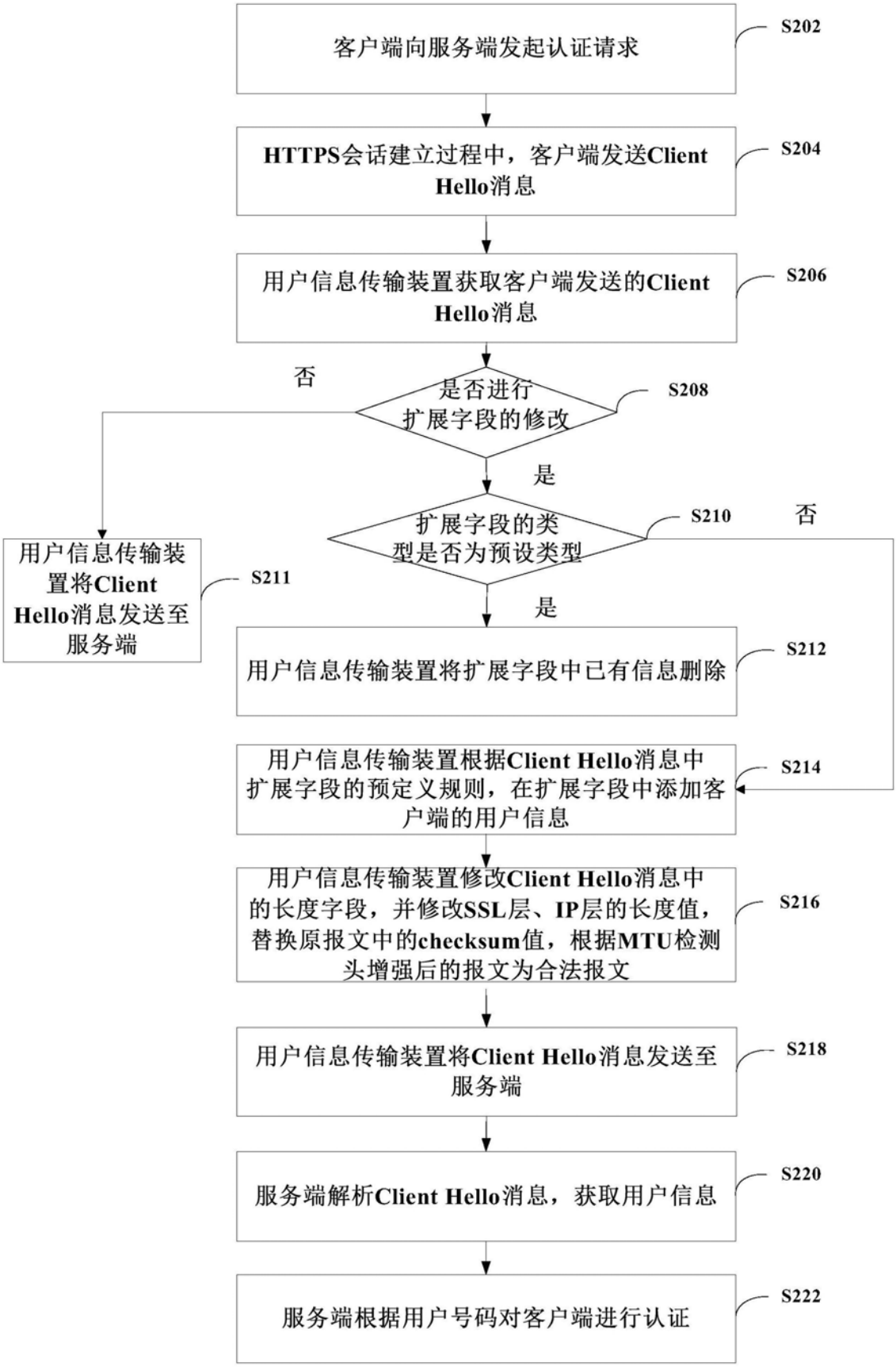

客户端向服务端发起认证请求
S202
HTTPS会话建立过程中，客户端发送Client Hello消息
S204
用户信息传输装置获取客户端发送的Client Hello消息
S206
否
是否进行扩展字段的修改
S208
是
扩展字段的类型是否为预设类型
S210
否
用户信息传输装置将Client Hello消息发送至服务端
S211
是
用户信息传输装置将扩展字段中已有信息删除
S212
用户信息传输装置根据Client Hello消息中扩展字段的预定义规则，在扩展字段中添加客户端的用户信息
S214
用户信息传输装置修改Client Hello消息中的长度字段，并修改SSL层、IP层的长度值，替换原报文中的checksum值，根据MTU检测头增强后的报文为合法报文
S216
用户信息传输装置将Client Hello消息发送至服务端
S218
服务端解析Client Hello消息，获取用户信息
S220
服务端根据用户号码对客户端进行认证
S222

图2


30
信息获取模块
302
字段检测模块
303
信息添加模块
304
信息发送模块
306

图3

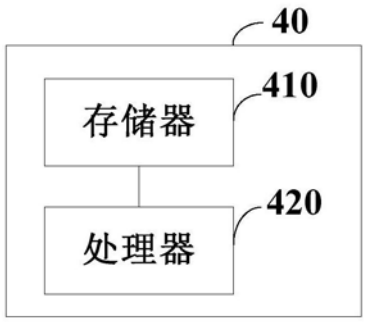

40
存储器
410
处理器
420

图4

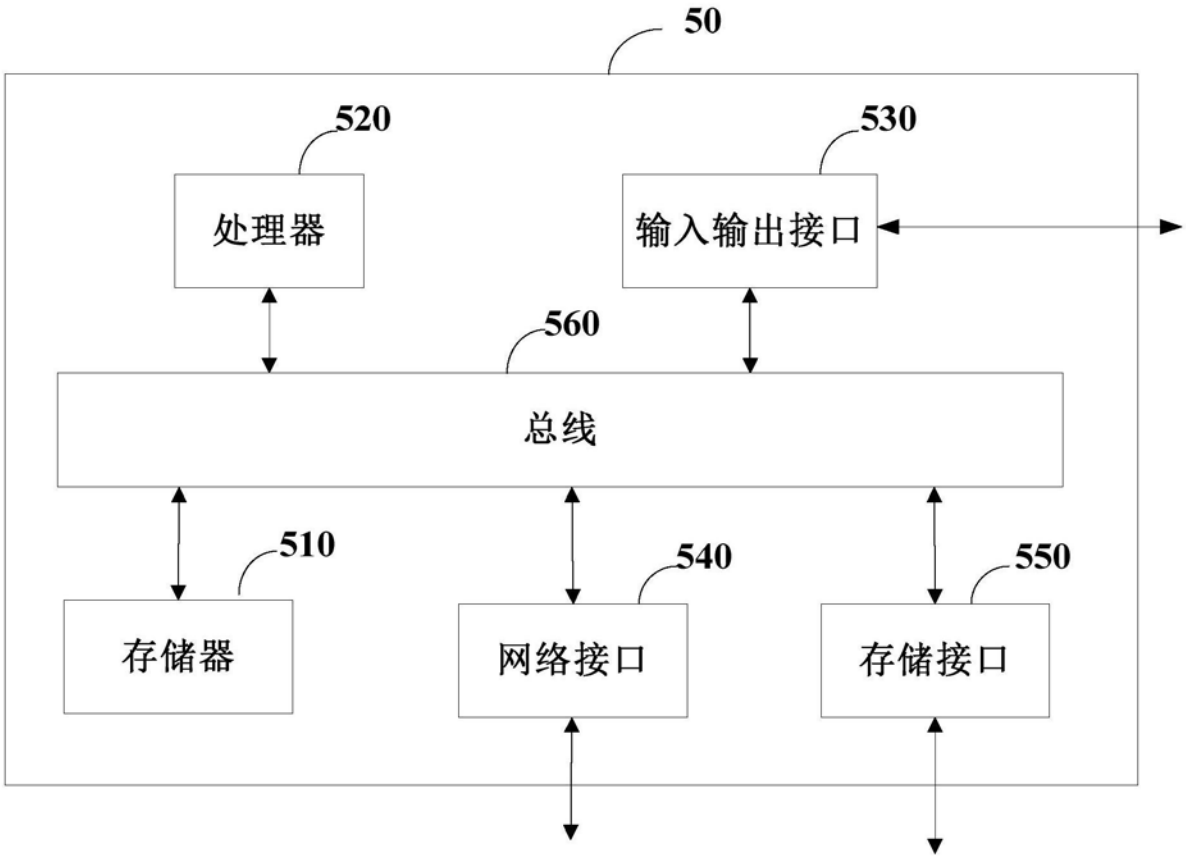

50
520
处理器
530
输入输出接口
560
总线
510
存储器
540
网络接口
550
存储接口

图5

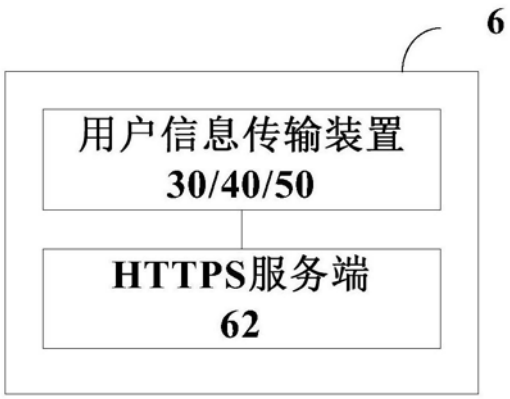

6
用户信息传输装置
30/40/50
HTTPS服务端
62

图6