(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 109155779 B
(45)授权公告日 2021.06.11

(21)申请号 201780010718.0
(22)申请日 2017.02.11
(65)同一申请的已公布的文献号
申请公布号 CN 109155779 A
(43)申请公布日 2019.01.04
(30)优先权数据
62/294,482 2016.02.12 US
15/098,899 2016.04.14 US
(85)PCT国际申请进入国家阶段日
2018.08.09
(86)PCT国际申请的申请数据
PCT/IB2017/050772 2017.02.11
(87)PCT国际申请的公布数据
WO2017/137959 EN 2017.08.17
(73)专利权人 杰皮优艾欧有限公司
地址 以色列佩塔提科瓦
(72)发明人 乔纳森·施瓦茨 弗兰克·马尔卡
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王萍 杨林森
(51)Int.Cl.
H04W 12/03(2021.01)
H04L 29/06(2006.01)
G06F 21/60(2013.01)
H04W 12/106(2021.01)
H04W 12/06(2021.01)
H04W 12/088(2021.01)
H04W 12/10(2021.01)

(56)对比文件
CN 103297437 A,2013.09.11
CN 103916239 A,2014.07.09
US 2013219168 A1,2013.08.22
CN 102164148 A,2011.08.24
CN 200976598 Y,2007.11.14
CN 103916456 A,2014.07.09
CN 102685165 A,2012.09.19
CN 103327020 A,2013.09.25
CN 102037708 A,2011.04.27
CN 101517986 A,2009.08.26

审查员 陈馨

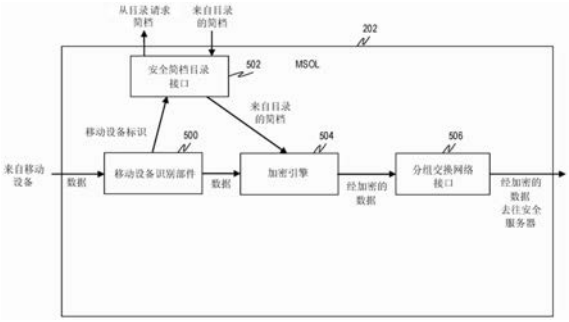
权利要求书2页 说明书19页 附图14页

(54)发明名称

移动安全卸载器

(57)摘要

在示例实施方式中,提供了移动安全卸载器(MSOL)。在MSOL内,使用移动设备识别部件在移动无线电网络中从移动设备接收未加密数据并且根据未加密数据来确定移动设备的移动设备标识。然后,安全简档目录接口使用移动设备标识从安全简档目录检索与移动设备标识对应的安全简档,该安全简档标识了用于对来自与移动设备标识对应的移动设备的数据进行加密的安全协议。使用加密引擎来使用在安全简档中标识的安全协议对未加密数据进行加密。然后使用分组交换网络接口经由分组交换网络将经加密的数据路由到在数据中标识的安全服务器。



CN 109155779 B

1.一种用于将安全方法和处理从移动设备卸载的移动安全卸载器MSOL(202),包括:

移动设备识别部件(500),被配置成在移动无线电网络中从移动设备(300)接收未加密数据并且根据所述未加密数据来确定所述移动设备的移动设备标识,所述移动设备标识包括所述移动设备的唯一标识,并且所述未加密数据是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的;

安全简档目录接口(502),被配置成使用所述移动设备标识从安全简档目录(204)检索与所述移动设备标识对应的安全简档,所述安全简档标识了用于对来自与所述移动设备标识对应的所述移动设备的数据进行加密的安全协议;

加密引擎(504),能够由一个或更多个处理器执行并且被配置成使用在所述安全简档中标识的所述安全协议对所述未加密数据进行加密;以及

分组交换网络接口(506),被配置成经由分组交换网络将经加密的数据路由到在所述数据中标识的安全服务器(118)。

2.根据权利要求1所述的MSOL,其中,所述分组交换网络接口(506)还被配置成从所述安全服务器(118)接收经加密的响应数据,并且其中,所述加密引擎(504)还被配置成基于所述安全简档对所述经加密的响应数据进行解密。

3.根据权利要求2所述的MSOL,其中,所述安全简档目录接口(502)还被配置成将所述安全简档存储在所述MSOL上的高速缓冲存储器中。

4.根据权利要求1所述的MSOL,其中,所述移动无线电网络是4G网络,并且所述未加密数据是经由服务网关SGW来接收的,或者

其中,所述安全简档在多个移动设备标识之间共享并且包含标识所述多个移动设备标识的字段。

5.根据权利要求1所述的MSOL,其中,所述安全简档目录(204)包含另外的安全简档,所述另外的安全简档标识了用于对来自相应移动设备的数据进行加密的不同安全协议。

6.一种安全方法,包括:

在用于将安全方法和处理从移动设备卸载的移动安全卸载器MSOL处,在移动无线电网络中从移动设备接收未加密数据,所述未加密数据是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的;

根据所述未加密数据来确定所述移动设备的移动设备标识,所述移动设备标识包括所述移动设备的唯一标识;

使用所述移动设备标识从安全简档目录检索与所述移动设备标识对应的安全简档,所述安全简档标识了用于对来自与所述移动设备标识对应的所述移动设备的数据进行加密的安全协议;

使用在所述安全简档中标识的所述安全协议对所述未加密数据进行加密;以及

经由分组交换网络将经加密的数据路由到在所述数据中标识的安全服务器。

7.根据权利要求6所述的安全方法,还包括:

从所述安全服务器接收经加密的响应数据;以及

基于所述安全简档对所述经加密的响应数据进行解密。

8.根据权利要求7所述的安全方法,还包括:

将所述安全简档存储在所述MSOL上的高速缓冲存储器中。

9.根据权利要求6所述的安全方法,其中,所述安全简档在多个移动设备标识之间共享并且包含标识所述多个移动设备标识的字段。

10.根据权利要求6所述的安全方法,其中,所述安全简档目录包含另外的安全简档,所述另外的安全简档标识了用于对来自相应移动设备的数据进行加密的不同安全协议。

11.根据权利要求6所述的安全方法,其中,所述移动设备的唯一标识是以下中之一:国际移动订户标识IMSI、移动台国际订户目录号码MSISDN、或电话号码。

12.一种用于将安全方法和处理从移动设备卸载的移动安全卸载器MSOL(1200),包括:

移动设备识别部件(1202),被配置成经由移动无线电网络从移动设备(300)接收在安全服务器上开始登录过程的请求并且根据所述请求来确定所述移动设备的移动设备标识,所述移动设备标识包括所述移动设备的唯一标识,并且所述请求是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的;

安全简档目录接口(1204),被配置成使用所述移动设备标识通过安全简档目录(204)认证所述移动设备并且响应于所述认证从所述安全简档目录(204)接收认证凭证;

认证凭证注入部件(1206),能够由一个或更多个处理器执行并且被配置成将所述认证凭证注入到所述开始登录过程的请求中;以及

分组交换网络接口(1208),被配置成经由分组交换网络将所述开始登录过程的请求路由到安全服务器。

13.根据权利要求12所述的MSOL,其中,所述分组交换网络接口(1208)还被配置成从所述安全服务器接收登录成功消息并且经由所述移动无线电网络将所述登录成功消息转发到所述移动设备。

14.一种安全方法,包括:

在用于将安全方法和处理从移动设备卸载的移动安全卸载器MSOL处,经由移动无线电网络从移动设备接收在安全服务器上开始登录过程的请求,所述请求是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的;

根据所述请求来确定所述移动设备的移动设备标识,所述移动设备标识包括所述移动设备的唯一标识,并且;

使用所述移动设备标识从安全简档目录(204)获取与所述移动设备标识对应的认证凭证;

将所述认证凭证注入到所述开始登录过程的请求中;以及

经由分组交换网络将所述开始登录过程的请求路由到安全服务器。

15.根据权利要求14所述的安全方法,其中,所述移动设备的唯一标识是以下中之一:国际移动订户标识IMSI、移动台国际订户目录号码MSISDN、或电话号码。

16.根据权利要求14所述的安全方法,还包括:

从所述安全服务器接收登录成功消息并且经由所述移动无线电网络将所述登录成功消息转发到所述移动设备。

移动安全卸载器

[0001] 优先权

[0002] 本申请要求于2016年2月12日提交的美国临时申请No.62/294,482的权益。本申请还要求于2016年4月14日提交的美国专利申请No.15/098,899的优先权。

技术领域

[0003] 本公开内容总体上涉及移动无线电联网。更具体地,本公开内容描述了卸载移动安全性。

背景技术

[0004] 作为由国际标准组织定义的网络内提供的基本服务的一部分,移动网络使得设备能够连接到外部分组交换网络(例如因特网)。这样的国际标准组织的示例包括用于全球移动通信系统(GSM)/通用移动电信系统(UMTS)/长期演进(LTE)域的第三代合作伙伴计划(3GPP)、时分多址(TDMA)/码分多址(CDMA)/CDMA2000网络以及较新的低功率广域网(LPWAN)计划,如LoRa和SIGFOX。

[0005] 在这样的系统中,去往移动设备的以及来自移动设备的分组数据经由无线电网络被发送到诸如2G网络中的基站收发信台(BTS)、3G网络中的NodeB或4G网络中的eNodeB的元件。之后,使用隧道向2G/3G网络中的服务通用分组无线业务(GPRS)支持节点(SGSN)或4G网络中的服务网关(SGW)或其他移动网络解决方案中的类似设备发送分组数据。

[0006] 来自所有移动设备的GPRS隧道协议(GTP)隧道被朝向2G/3G网络中的网关GPRS支持节点(GGSN)或4G网络中的PDN网关(PGW)或其他移动网络解决方案中的类似设备聚合。然后,这些设备将在每个连接中包含多个隧道的许多以太网连接合并。

[0007] 然后,GGSN或PGW负责将聚合的GTP隧道的业务分散到多个数据流中,并且将每个单个的流路由到由移动设备初始指定的外部分组交换网络上的指定目的地。

[0008] 随着物联网(IoT)领域的激增,与以往任何时候相比越来越多不同类型的移动设备正在被使用,而这种趋势仅趋于随着越来越多类型的设备例如汽车、智能城市传感器、集装箱、婴儿车等采用移动通信部件而增长。

[0009] 随着不同类型的移动设备的过多,对通信和数据安全性的威胁增加。虽然移动电话设计者当然可能是通信安全专家,但是婴儿车设计者可能不是。这使得嵌入这些完全不同的产品的移动通信部件不太可能解决常见的安全问题。

[0010] 此外,IoT设备通常被设计成廉价且节省电池的。在IoT设备上运行安全特征需要较复杂的CPU设计和较多功耗,因此可能与这些目标不一致。

[0011] 虽然大多数移动网络本身都是安全的,但是因特网是不太安全的媒介,因此当通信离开移动网络并且进入因特网时,对安全的威胁增加。

发明内容

[0012] 根据本发明的一方面,提供了一种用于将安全方法和处理从移动设备卸载的移动

安全卸载器MSOL，包括：移动设备识别部件，被配置成在移动无线电网络中从移动设备接收未加密数据并且根据所述未加密数据来确定所述移动设备的移动设备标识，所述移动设备标识包括所述移动设备的唯一标识，并且所述未加密数据是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的；安全简档目录接口，被配置成使用所述移动设备标识从安全简档目录检索与所述移动设备标识对应的安全简档，所述安全简档标识了用于对来自与所述移动设备标识对应的所述移动设备的数据进行加密的安全协议；加密引擎，能够由一个或更多个处理器执行并且被配置成使用在所述安全简档中标识的所述安全协议对所述未加密数据进行加密；以及分组交换网络接口，被配置成经由分组交换网络将经加密的数据路由到在所述数据中标识的安全服务器。

[0013] 根据本发明的一方面，提供了一种安全方法，包括：在用于将安全方法和处理从移动设备卸载的移动安全卸载器MSOL处，在移动无线电网络中从移动设备接收未加密数据，所述未加密数据是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的；根据所述未加密数据来确定所述移动设备的移动设备标识，所述移动设备标识包括所述移动设备的唯一标识；使用所述移动设备标识从安全简档目录检索与所述移动设备标识对应的安全简档，所述安全简档标识了用于对来自与所述移动设备标识对应的所述移动设备的数据进行加密的安全协议；使用在所述安全简档中标识的所述安全协议对所述未加密数据进行加密；以及经由分组交换网络将经加密的数据路由到在所述数据中标识的安全服务器。

[0014] 根据本发明的一方面，提供了一种用于将安全方法和处理从移动设备卸载的移动安全卸载器MSOL，包括：移动设备识别部件，被配置成经由移动无线电网络从移动设备接收在安全服务器上开始登录过程的请求并且根据所述请求来确定所述移动设备的移动设备标识，所述移动设备标识包括所述移动设备的唯一标识，并且所述请求是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的；安全简档目录接口，被配置成使用所述移动设备标识通过安全简档目录认证所述移动设备并且响应于所述认证从所述安全简档目录接收认证凭证；认证凭证注入部件，能够由一个或更多个处理器执行并且被配置成将所述认证凭证注入到所述开始登录过程的请求中；以及分组交换网络接口，被配置成经由分组交换网络将所述开始登录过程的请求路由到安全服务器。

[0015] 根据本发明的一方面，提供了一种安全方法，包括：在用于将安全方法和处理从移动设备卸载的移动安全卸载器MSOL处，经由移动无线电网络从移动设备接收在安全服务器上开始登录过程的请求，所述请求是经由码分多址CDMA、全球移动通信系统GSM或通用移动电信系统UMTS从所述移动设备发送的；根据所述请求来确定所述移动设备的移动设备标识，所述移动设备标识包括所述移动设备的唯一标识，并且；使用所述移动设备标识从安全简档目录获取与所述移动设备标识对应的认证凭证；将所述认证凭证注入到所述开始登录过程的请求中；以及经由分组交换网络将所述开始登录过程的请求路由到安全服务器。

附图说明

[0016] 在附图的各个图中通过示例并不作为限制示出了一些实施方式，在附图中：

[0017] 图1是示出根据示例实施方式的用于在GSM(2G)和/或UMTS(3G)移动网络中对网络通信进行路由的系统的框图。

[0018] 图2是示出根据示例实施方式的用于在GSM(2G)和/或UMTS(3G)移动网络中对网络通信进行路由的系统的框图。

[0019] 图3是示出根据示例实施方式的用于GPRS子网络服务的协议栈的框图。

[0020] 图4是示出包括SGSN/SGW和GGSN/PDN网关(PGW)的系统的框图。

[0021] 图5是更详细地示出根据示例实施方式的MSOL的框图。

[0022] 图6是示出根据示例实施方式的对移动设备分组执行超文本传输协议安全(HTTPS)加密的方法的交互图。

[0023] 图7是示出根据示例实施方式的对移动设备分组执行TLS加密的方法的交互图。

[0024] 图8是示出根据示例实施方式的对移动设备分组执行VPN加密的方法的交互图。

[0025] 图9是示出根据示例实施方式的对短消息发送服务(SMS)分组执行TLS加密的方法的交互图。

[0026] 图10是示出根据示例实施方式的对语音呼叫执行基于TLS的会话发起协议(SIPS)/安全实时协议(SRTP)加密的方法的交互图。

[0027] 图11是示出根据示例实施方式的MSOL将网络凭证添加到登录过程的交互图。

[0028] 图12是示出根据示例实施方式的能够将网络凭证添加到登录过程的MSOL的框图。

[0029] 图13是示出可以与本文描述的各种硬件架构结合使用的代表性软件架构的框图。

[0030] 图14是示出根据一些示例实施方式的能够从机器可读介质(例如,机器可读存储介质)读取指令并执行本文所讨论的任一种或更多种方法的机器的部件的框图。

具体实施方式

[0031] 以下描述包括体现说明性实施方式的说明性系统、方法、技术、指令序列和计算机器程序产品。在以下描述中,出于解释的目的,阐述了许多具体细节以便提供对本发明主题的各种实施方式的理解。然而,对于本领域技术人员而言显然的是,可以在没有这些具体细节的情况下实践本发明主题的实施方式。通常,未详细地示出公知的指令实例、协议、结构和技术。

[0032] 在示例实施方式中,安全方法和处理从移动设备被卸载到如下移动安全卸载器部件:该移动安全卸载器部件被设计成在经由无线电网络从移动设备发送的通信被发送到分组交换网络例如因特网时执行所有安全方法和加密以保护所述通信。

[0033] 图1是示出根据示例实施方式的用于在GSM(2G)和/或UMTS(3G)移动网络中对网络通信进行路由的系统100的框图。系统100包括一个或更多个移动设备102A-102D。每个移动设备102A-102D可以是通常称为单元收发器(cell transceiver)的具有无线电通信器的任何类型的设备。移动设备102A-102D包括例如智能电话、平板计算机、联网的汽车、传感器、警报系统等。

[0034] 每个移动设备102A-102D经由无线电通信连接到移动网络。在图1中,描绘了两个不同示例类型的移动网络。第一个是基于GSM的移动网络。在基于GSM的移动网络中,移动设备102A、102B经由无线电通信与基站收发信台(BTS)104A、104B连接。BTS 104A、104B是无线电接口的终端节点。每个BTS 104A、104B包括一个或更多个收发器并且负责无线电接口的加密。

[0035] 然后,每个BTS 104与基站控制器(BSC)106通信。通常,BSC 106具有在其控制下的

数百个BTS 104A、104B。BSC 106用于向移动设备102A、102B分配无线电资源，管理频率以及控制BTS 104之间的切换。BSC 106还可以用作集中器，使得到BSC 106的许多低容量连接变得减少到较少数量的连接。

[0036] 这里描绘的第二类型的移动网络是基于通用移动电信系统UMTS的移动网络。基于UMTS的移动网络使用宽带码分多址(W-CDMA)无线电接入技术。这里，移动设备102C-102D通过无线电通信与NodeB 108A、108B连接。NodeB 108A、108B是无线电接口的终端节点。每个NodeB108A、108B包括一个或更多个收发器并且负责无线电接口的加密。每个NodeB 108A-108B被配置成应用代码来描述基于CDMA的UMTS网络中的信道。通常，每个NodeB 108A-108B针对UMTS网络来执行与BTS104A-104B针对GSM网络执行的功能类似的功能。

[0037] 然后，每个NodeB 108A-108B与无线电网络控制器(RNC)110通信。通常，RNC 110具有在其控制下的数百个NodeB 108A、108B。RNC 110用于向移动设备102C、102D分配无线电资源，管理频率以及控制NodeB108A-108B之间的切换。RNC 110还可以用作集中器，使得到RNC 110的许多低容量连接变得减少到较少数量的连接。

[0038] 应当注意，虽然这里描绘了两种不同的移动网络类型，但是本公开内容中描述的构思将在除了在图1中描绘的网络类型或代替在图1中描绘的网络类型的仅具有单一网络类型的系统中以及在具有多种网络类型的系统中工作。

[0039] BTS 104A、104B和/或NodeB 108A、108B连接到处理网络内的所有分组交换数据的服务GPRS支持节点(SGSN)112。在典型系统100中实际上存在两种形式的GPRS支持节点(GSN)。这里相关的是第一类型：SSGN，其通常负责向在其地理服务区域内的BTS 104A、104B和NodeB108A、108B以及从所述BTS 104A、104B和NodeB 108A、108B传送数据分组。其他任务可以包括分组路由和传输、移动性管理(附接/分拆和移动性管理)、逻辑链路管理和计费功能。

[0040] 在一些示例实施方式中，以上关于SGSN 112描述的功能由服务网关(SGW)执行，为了简单起见未在这里描绘SGW。在一些其他示例实施方式中，一些其他类型的设备可以执行以上关于SGSN 112描述的功能。包括SGSN 112和SGW的所有这些类型的设备可以统称为“聚合器”或“分组聚合器”。

[0041] 数据分组从移动设备102A-102D向上游发送到外部分组交换数据网络，诸如因特网114。SGSN 112将来自移动设备102A-102D的数据分组聚合，并且将它们发送到作为第二类型的GSN的网关GPRS支持节点(GGSN)116。GGSN 116负责GPRS网络与诸如因特网114的外部分组交换网络之间的互连。从外部网络的角度来看，GGSN 116是到子网络的路由器，因为GGSN 116对外部网络隐藏了GPRS基础结构。当GGSN 116接收到寻址到特定用户的数据时，其检查该用户是否是活动的。如果是，则GGSN 116将数据转发到为该移动用户服务的SGSN 112。如果移动用户是不活动的，则丢弃该数据。GGSN 116是实现GPRS网络中的用户终端的移动性的锚点。

[0042] 为了保护数据通过该系统100发送，移动设备102A-102D可以使用诸如安全套接层(SSL)、传输层安全性(TLS)、虚拟专用网络(VPN)等的方法来加密数据。然后，该加密被保持通过包括BTS 104A、104B或NodeB 108A、108B、BSC 106或RNC 110、SGSN 112、GGSN 116的网络中的所有部件，并且最终通过因特网114到达安全服务器118。然而，这增加了移动设备102A-102D的成本和功率利用，因为移动设备102A-102D必须用加密机制来编程/设计。另

外,需要保持内部防火墙以便保护移动设备102A-102D免受因特网114上的恶意设备的影响。

[0043] 图2是示出根据示例实施方式的用于在GSM(2G)和/或UMTS(3G)移动网络中对网络通信进行路由的系统200的框图。除了添加了移动安全卸载器(MSOL,mobile security offloader)202和相应的安全简档目录204之外,图2中的各种部件类似于图1的部件。在图2中,不对移动设备102A-102D本身执行安全加密,而是移动设备102A-102D通过移动网络向MSOL 202发送未加密业务,依赖于移动网络提供商的安全协议来保护该业务。然后,MSOL 202从安全简档目录204中检索与发送移动设备102A-102D对应的安全简档。可以基于订户标识模块(SIM)或通用集成电路卡(UICC)卡标识符诸如国际移动订户标识(International Mobile Subscriber Identity,IMSI)或移动台国际订户目录号码(Mobile Station International Subscriber Directory Number,MSISDN)来识别发送移动设备102A-102D。基于相应的安全简档,MSOL 202知道如何加密业务并以加密形式将其传递给安全服务器118。可以使用诸如SSL、TLS、VPN等的方法在MSOL 202上执行加密,而不需要在移动设备102A-102D本身上处理安全性和加密。在一些示例实施方式中,MSOL 202还可以基于存储的安全简档向移动设备102A-102D提供外部防火墙。

[0044] 图3是示出根据示例实施方式的用于GPRS子网络服务的协议栈的框图。这里描绘的是移动设备(MS)300、基站(BS)302、SGSN 304和GGSN 306。GTP 308是使用Gn接口在SGSN 304与GGSN 306之间使用的协议。这是第3层隧道协议。发生的处理看起来像是网络内外的用户的正常IP子网络。应用310通过IP 312进行通信,IP 312通过GPRS网络携载并通过GGSN 306被传送出去。在GGSN 306与SGSN 304之间移动的分组使用GTP 308。这样,位于GPRS外部的IP地址不必处理内部主干。在SGSN 304上,UDP 314和IP 312由GTP 308运行。

[0045] 子网络相关会聚协议(SNDCP)316和逻辑链路控制(LLC)318在SGSN 304与MS 300之间组合使用。SNDCP 316是用户平面GPRS协议栈的最顶层。SNDCP 316使数据平坦化以减少无线电信道上的负荷。SNDCP 316的主要目的是缓冲并且分段网络协议数据单元(PDU),向每个段添加报头,然后将该段提供给LLC 318以进行传输。通过对分组进行加密所创建的安全逻辑链路由LLC 318提供,并且只要移动设备在单个SGSN 304下,则使用相同的LLC 318链路。SNDCP 316还执行压缩和解压缩。意图是减少需要通过空中发送的数据量。因此,SNDCP 316通常知道关于用于压缩相关功能的分组数据网络(PDN)协议的某些细节。SNDCP316还可以知道PDP上下文和诸如PDP类型、QoS等的相应信息。该信息在PDP上下文激活过程期间给出。

[0046] LLC 318的功能是管理和确保数据传输的完整性。LLC 318提供到网络层协议的服务的数据链路层链路。这通过驻留在网络计算机上的针对所述服务的LLC服务接入点来实现。此外,存在用于传递请求或服务的LLC控制字段。LLC 318还可以执行对分组的加密和解密。

[0047] 图4是示出包括SGSN/SGW 402和GGSN/PDN网关(PGW)404的系统400的框图。在示例实施方式中,SGSN/SGW 402可以是图1的SGSN112,并且GGSN/PGW 404可以是图1的GGSN 116。SGSN/SGW 402经由Gn接口端口将数据从移动无线电网络传送到GGSN/PGW 404。Gn包括GPRS隧道协议(GTP)隧道。GTP 308被分成控制隧道的GTP-C和作为实际用户业务数据的GTP-U。

[0048] 在线计费系统(OCS)406经由Gy参考点连接到GGSN/PGW 404。OCS 406是向GGSN/PGW 404告知某个隧道是否具有带宽配额并且还基于每用户的实际服务计划和帐户余额来允许或不允许隧道的计费系统。在线计费具有两个子功能:评级(rating)和单位确定(unit determination)。它们二者都可以实现为集中式或分散式。

[0049] 评级是指由单位确定功能计算的非货币单位的计算。单位确定是指在开始提供服务之前应当分配的非货币单位(服务单位、数据量、时间和事件)的数量的计算。

[0050] 可以区分在线计费的三种情况:即时事件计费(IEC)、具有单位预约的事件计费(ECUR)以及具有单位预约的会话计费(SCUR)。

[0051] IEC涉及直接借记操作,在该直接借记操作中,立即从金融账户中借记适当的费用。在ECUR中,在服务提供之前保留金融单位,并且在服务提供结束之后执行金融账户借记操作。在SCUR中,在会话监督之前保留金融单位,并且在会话终止结束之后执行金融账户借记操作。

[0052] 离线计费系统(OFCS)408经由Gz参考点连接到GGSN/PGW 404。OFCS 408是用于后支付呼叫详细记录(CDR)处理的计费系统。离线计费是与网络资源使用同时地收集该网络资源使用的计费信息的处理。然后,计费信息被传递通过一系列逻辑计费功能。在该处理结束时,由网络生成CDR文件,CDR文件然后被传送到网络运营商的计费域,以用于订户计费和/或互操作者计费(或诸如统计的另外的功能)。计费域通常包括后处理系统,诸如运营商的计费系统或计费中介设备。

[0053] 离线计费功能的示例包括计费触发功能(CTF)、计费数据功能(CDF)和计费网关功能(CGF)。CTF基于对网络资源使用的观察来生成计费事件。CTF是用于收集与网络元件内的可计费事件有关的信息、将该信息组合成匹配计费事件并且将这些计费事件朝向CDF发送的集中点。CTF由两个功能块组成:帐户指标收集,其监视针对呼叫服务事件或由网络用户建立的会话的信令功能,或对这些呼叫、服务事件或会话的用户业务的处理,或经由这些呼叫、服务事件或会话的向用户的服务提供;以及计费数据转发,其接收收集的计费指标,并且根据一个或更多个指标的集合来确定可计费事件的发生,然后将与检测到的可计费事件匹配的计费事件组合,并且经由Rf接口将计费事件朝向计费数据功能转发。

[0054] CDF通过Rf参考点从CTF接收计费事件。然后,它使用计费事件中包含的信息来构造CDR。由CDF产生的CDR被立即经由Ga接口点传送到计费网关功能(CGF)。CGF执行诸如接近实时地经由Ga接口从CDF的CDR接收、CDR预处理、CDR的验证、合并和(重新)格式化、CDR误差处理、持久性CDR存储、CDR路由和滤波、CDR文件管理以及向计费域的CDR文件传送的功能。

[0055] 分组数据网络410经由Gi参考点连接到GGSN/PGW 404。分组数据网络410是移动设备300可以向其发送数据的公共或专用数据网络。策略和计费规则功能(PCRF)412经由Gx参考点连接到GGSN/PGW 404,并且是在GGSN/PGW 404中实施数据流策略的方法的一部分。PCRF 412负责收集规则并将它们传递给GGSN/PGW 404。PCRF 412提供关于服务数据流检测、选通(阻止或允许分组)、QoS控制和计费的网络控制。例如,当服务信息与订阅信息不一致时,PCRF 412可以拒绝从应用310接收的请求。

[0056] PCRF 412经由Sp参考点连接到订阅简档储存库(SPR)414。SPR 414包含通常基于每PDN存储的订户和订阅信息,并且将包括诸如订户的允许服务、关于订户的允许QoS的信息、订户的计费相关信息和订户类别的信息。PCRF 412可以访问SPR 414以查询每个相关用

户的简档。应用功能(AF)416经由Rx参考点连接到PCRF 412,并且允许外部应用逻辑改变PCRF规则。

[0057] GGSN/PGW 404使用策略强制规则功能(PCEF)418来强制实施PCRF412产生的规则。虽然GGSN/PGW 404允许基本路由功能以及VPN、网络地址转换(NAT)和基本防火墙的建立,但是所有这些服务都基于网络运营商配置,并且这些功能都不被导出以由服务的实际承载者(统称为客户的移动设备300及其所有者以及雇佣所有者的公司或其他组织)修改。它们还涉及连接内部和外部网络元件而不是来自移动设备300的特定分组业务。PCRF 412还使用黑名单(例如,禁止的移动设备300、网络位置、业务类型等的列表)来强制实施安全规则。

[0058] 图5是更详细地示出根据示例实施方式的MSOL 202的框图。MSOL202可以包含移动设备识别部件500,所述设备识别部件500用于识别已经向MSOL 202发送数据的移动设备300。数据可以包括任何数量的不同类型的通信,包括HTTP请求、TCP分组、语音呼叫、SMS消息等。移动设备识别部件500可以至少部分地基于数据本身来确定哪个移动设备300发送了该数据。例如,数据可以包括标识移动设备300的IMSI或类似唯一标识的字段。替选地,在语音呼叫的情况下,伴随语音呼叫的元数据可以包括唯一标识信息,诸如经由呼叫者ID机制的电话号码。无论移动设备300的标识的形式如何,移动设备识别部件500都可以将该标识转发到安全简档目录接口502,安全简档目录接口502可以用于形成从安全简档目录204请求与移动设备标识对应的简档的请求。

[0059] 然后,从安全简档目录204将相应的简档返回到安全简档目录接口502。然后,将简档发送到加密引擎504,加密引擎504用于使用来自简档的信息来加密数据。简档的格式可以根据实现方式并且基于用于向安全服务器118的传输的加密方案而极大地变化。在一些示例实施方式中,每个移动设备标识具有相应的单独的安全简档,即使在一些情况下特定单独安全简档中的信息可能与另外的单独安全简档中的信息完全匹配(诸如,在两个个体使用完全相同的用于安全加密的参数的情况下)。在这种情况下,安全简档可以在安全简档的字段中列出其应用于的特定移动设备标识,其可以在需要时由安全简档目录204搜索以获得安全简档。在其他示例实施方式中,可以在多个移动设备标识之间共享相应的安全简档。在这种情况下,安全简档可以指定安全简档所应用于的标识的分组或范围,其可以在需要时由安全简档目录204搜索以获得安全简档。

[0060] 应当注意,在一些示例实施方式中,移动运营商和/或终端订户可以经由诸如命令行接口、web接口或API的一个或更多个不同类型的接口来修改简档目录。

[0061] 加密引擎504可以是软件部件、硬件部件或其一些变型。某些类型的加密在硬件中实现比在软件中实现更有利。在一些示例实施方式中,加密引擎504被设计成基于安全简档中的信息来处理多种不同类型的加密。

[0062] 以其最简单的形式,安全简档可以标识出用于对从移动设备102到安全服务器118的数据进行加密的加密标准。例如,安全简档可以标识出应当使用HTTPS、TLS、VPN或安全实时传输协议(SRTP)加密来对从移动设备102到安全服务器118的数据进行加密。然而,在一些情况下,安全简档可能包含关于如何加密数据的其他详细信息,诸如凭证信息(例如,证书、用户名、口令等)、安全参数(例如,加密级别、子格式等)以及其他连接参数。

[0063] HTTPS简档的示例可以包括简档的名称、简档所属的移动设备标识、各种HTTPS安全字段(例如,要执行的安全检查的清单)以及各种HTTPS参数字段(例如,远程登录)。

[0064] TLS简档的示例可以包括简档的名称、简档所属的移动设备标识、各种TLS安全字段(例如,最小协议方法、密码、证书认证)以及各种TLS参数字段(例如,目前有效时间、传输类型)。

[0065] VPN简档的示例可以包括简档的名称、简档的描述、简档所属的移动设备标识、各种VPN安全字段(例如,客户端认证方法、使能口令持久性)以及标识连接参数的各种VPN参数字段(例如,使能自动网络检测、最大传输单元大小、在指示连接失败之前等待的时间量、使能主机ID检查)。

[0066] 当从安全服务器118接收到响应时,加密引擎504可以用于使用相同的安全简档将响应解密成经解密的格式。然后可以将该经解密的响应转发到移动设备300。实际上,MSOL 202可以从许多不同的移动设备300以及从许多不同的安全服务器118接收许多数据。因此,在一些示例实施方式中,高速缓冲存储器(未示出)可以被保持在MSOL 202上以存储检索到的安全简档。该高速缓冲存储器可以基于时间调度(例如,简档已经在高速缓冲存储器中保持了多长时间)或者基于会话调度(例如,只要在相应的移动设备300与安全服务器118之间保持会话,则在高速缓冲存储器中保持安全简档)被清除。

[0067] 图6是示出根据示例实施方式的对移动设备分组执行超文本传输协议安全(HTTPS)加密的方法600的交互图。该方法600利用移动设备(MD)602、MD 602连接到的移动网络604、MSOL 606、安全简档目录(SPD)608、因特网610和安全服务器612。在操作614处,通过移动网络604从移动设备602发送HTTP请求,该HTTP请求在操作616处被转发到MSOL 606。在操作618处,MSOL 606从SPD 608请求设备简档。这可以包括识别MD 602的唯一标识符诸如IMSI以及将其转发到SPD 608。然后,SPD 608在操作620处返回HTTPS加密简档。HTTPS加密简档可以是与由诸如IMSI的唯一标识符所标识的MD 602对应的HTTPS加密简档。在操作622处,MSOL 606使用该HTTPS加密简档来加密HTTP请求,从而形成HTTPS请求。在操作624处,MSOL 606将该HTTPS请求朝向安全服务器612发送到因特网610,安全服务器612在操作626处接收该HTTPS请求。然后,安全服务器612可以执行HTTPS解密以读取请求并相应地起作用,以形成加密为HTTPS响应的HTTP响应,HTTPS响应在操作628处被发送并且在操作630处在MSOL 606处被接收。在操作632处,MSOL 606然后使用设备简档对HTTPS响应进行解密,并且在操作634处将经解密的HTTP响应发送到移动网络604,移动网络604在操作636处将其转发到MD 602。

[0068] 图7是示出根据示例实施方式的对移动设备分组执行TLS加密的方法700的交互图。该方法700利用移动设备(MD)702、MD 702连接到的移动网络704、MSOL 706、安全简档目录(SPD)708、因特网710和安全服务器712。在操作714处,通过移动网络704从移动设备702发送TCP业务,TCP业务在操作716处被转发到MSOL 706。在操作718处,MSOL 706从SPD 708请求设备简档。这可以包括识别MD 702的唯一标识符诸如IMSI以及将其转发到SPD 708。然后,SPD 708在操作720处返回TLS加密简档。TLS加密简档可以是与由诸如EVISI的唯一标识符所标识的MD 702对应的TLS加密简档。在操作722处,MSOL 706发起与安全服务器712的TLS握手,该TLS握手在操作724处经由因特网710由安全服务器712接收。在操作726处,安全服务器712可以向MSOL 706发送握手响应,该握手响应在操作728处经由因特网710由MSOL 706接收。

[0069] 在操作730处,MSOL 706使用TLS加密简档来加密TCP业务,从而形成基于TLS的TCP

业务。在操作732处，MSOL 706将该基于TLS的TCP业务朝向安全服务器712发送到因特网710，安全服务器712在操作734处接收基于TLS的TCP业务。然后，安全服务器712可以执行TLS解密以读取业务并且相应地起作用，以形成加密为基于TLS的TCP业务的响应TCS业务，响应TCS业务在操作736处被发送并且在操作738处在MSOL 706处被接收。在操作740处，MSOL 706然后对基于TLS的TCP业务进行解密，并且在操作742处将经解密的TCP业务发送到移动网络704，移动网络704在操作744处将其转发到MD 702。

[0070] 图8是示出根据示例实施方式的对移动设备分组执行诸如IPSEC加密的VPN加密的方法800的交互图。该方法800利用移动设备(MD)802、MD 802连接到的移动网络804、MSOL 806、安全简档目录(SPD)808、因特网810和安全服务器812。在操作814处，通过移动网络804从移动设备802发送IP业务，IP业务在操作816处被转发到MSOL 806。在操作818处，MSOL 806从SPD 808请求设备简档。这可以包括识别MD 802的唯一标识符诸如IMSI以及将其转发到SPD 808。然后，在操作820处，SPD 808返回VPN加密简档。VPN加密简档可以是与由诸如IMSI的唯一标识符所标识的MD 802对应的VPN加密简档。在操作822处，MSOL 806发起与安全服务器812的VPN连接的启动，该VPN连接的启动在操作824处经由因特网810由安全服务器812接收。在操作826处，安全服务器812可以向MSOL 806发送VPN连接响应，该VPN连接响应在操作828处经由因特网810由MSOL 806接收。

[0071] 在操作830处，MSOL 806使用VPN加密简档来加密IP业务，从而形成基于VPN的IP业务。在操作832处，MSOL 806将该基于VPN的IP业务朝向安全服务器812发送到因特网810，安全服务器812在操作834处接收基于VPN的IP业务。然后，安全服务器812可以执行VPN解密以读取业务并且相应地起作用，以形成加密为基于VPN的IP业务的响应IP业务，响应IP业务在操作836处被发送并且在操作838处在MSOL 806处被接收。在操作840处，MSOL 806然后对基于VPN的IP业务进行解密，并且在操作842处将经解密的IP业务发送到移动网络804，移动网络804在操作844处将其转发到MD 802。

[0072] 图9是示出根据示例实施方式的对短消息发送服务(SMS)分组执行TLS加密的方法900的交互图。该方法900利用移动设备(MD)902、MD 902连接到的移动网络904、MSOL 906、安全简档目录(SPD)908、因特网910和安全服务器912。在操作914处，通过移动网络904从移动设备902发送SMS消息，SMS消息在操作916处被转发到MSOL 906。这可以经由信令系统7(SS7)或短消息对等(SMPP)承载器来执行。在操作918处，MSOL 906从SPD 908请求设备简档。这可以包括识别MD 902的唯一标识符诸如IMSI以及将其转发到SPD 908。然后，在操作920处，SPD 908返回TLS加密简档。TLS加密简档可以是与由诸如IMSI的唯一标识符标识的MD 902对应的TLS加密简档。在操作922处，MSOL 906发起与安全服务器912的TLS握手，该TLS握手在操作924处经由因特网910由安全服务器912接收。在操作926处，安全服务器912可以向MSOL 906发送TLS握手响应，该TLS握手响应在操作928处经由因特网910由MSOL 906接收。

[0073] 在操作930处，MSOL 906使用TLS加密简档来加密SMS消息，从而形成经由基于TLS的TCP的SMS业务。在操作932处，MSOL 906将该经由基于TLS的TCP的SMS业务朝向安全服务器912发送到因特网910，安全服务器912在操作934处接收经由基于TLS的TCP的SMS业务。然后，安全服务器912可以执行TLS解密以读取SMS消息并且诸如通过将SMS消息转发给接收者并且从接收者接收SMS响应来相应地起作用。然后，其可以使用TLS对SMS响应进行加密，以

形成经由基于TLS的TCP的响应SMS业务，经由基于TLS的TCP的响应SMS业务在操作936处被发送并且在操作938处在MSOL 906处被接收。在操作940处，MSOL 906然后对经由基于TLS的TCP的SMS业务进行解密，并且在操作942处将经解密的SMS响应发送到移动网络904，移动网络904在操作944处将其转发到MD 902。

[0074] 图10是示出根据示例实施方式的对语音呼叫执行基于TLS的会话发起协议(SIPS)/安全实时协议(SRTP)加密的方法1000的交互图。该方法1000利用移动设备(MD)1002、MD 1002连接到的移动网络1004、MSOL 1006、安全简档目录(SPD)1008、因特网1010和安全服务器1012。在操作1014处，通过移动网络1004从移动设备1002向系统号码发起语音呼叫，该语音呼叫在操作1016处被转发到MSOL 1006。在操作1018处，MSOL 1006从SPD 1008请求设备简档。这可以包括识别MD 1002的唯一标识符诸如IMSI。然后，在操作1020处，SPD 1008返回STRP加密简档。STRP加密简档可以是与由诸如IMSI的唯一标识符标识的MD1002对应的STRP加密简档。在操作1022处，MSOL 1006向安全服务器1012发起SIP邀请，该SIP邀请在操作1024处经由因特网1010由安全服务器1012接收。该SIP邀请可以被加密。在操作1026处，安全服务器1012可以向MSOL 1006发送SIP响应200 OK消息，SIP响应200OK消息在操作1028处经由因特网1010由MSOL 1006接收。

[0075] 在操作1030处，MSOL 1006使用SRTP加密简档来加密语音呼叫，从而形成SRTP业务。在操作1032处，MSOL 1006将该SRTP业务朝向安全服务器1012发送到因特网1010，安全服务器1012在操作1034处接收该SRTP业务。然后，安全服务器1012可以执行SRTP解密以接收语音呼叫并且例如通过将语音呼叫转发给接收者并从接收者接收语音呼叫响应来相应地起作用。然后，其可以使用SRTP对语音呼叫响应进行加密，从而形成响应SRTP业务，响应SRTP业务在操作1036处被发送并且在操作1038处在MSOL 1006被接收。在操作1040处，MSOL 1006然后对SRTP业务进行解密，并且在操作1042处将语音呼叫响应作为TCP业务发送到移动网络1004，移动网络1004在操作1044处将其转发到MD 1002。

[0076] 移动设备1002可能需要登录到远程服务器、云服务或其他远程服务中。为了登录，在设备连接到云服务器并使用预定义用户名或设备标识以及偶尔地使用口令的情况下发生登录过程。然而，这不是非常安全的，因为标识和口令被存储在设备本身上，其可能被黑客检索到，该黑客可能使用该信息伪装为该设备并入侵远程服务器。在示例实施方式中，引入了“基于网络的信任锚”的概念。基于网络的信任锚是MSOL 1006的某个特征，所述特征是安全服务器1012可以是移动设备1002是其声称的移动设备的确认手段。在一个示例实施方式中，移动设备1002使用SIM卡向移动网络进行认证。然后，MSOL 1006可以执行设备的登录或向该登录添加确认其确实是实际设备的凭证。当移动设备1002尝试执行登录时，它将请求发送到MSOL 1006或者网络拦截该请求并将其路由到MSOL 1006。然后，MSOL 1006将识别该请求通过移动网络1004来自实际经认证的移动设备1002并且将执行登录，或者向该登录添加附加凭证，使得安全服务器1012将完全肯定该登录来自所期望的设备。可以与安全服务器1012预先共享这样的凭证以加强认证有效性。

[0077] 图11是示出根据示例实施方式的MSOL将网络凭证添加到登录过程的交互图。该方法1100利用移动设备(MD)1102、MD 1102连接到的移动网络1104、MSOL 1106、安全简档目录(SPD)1108、因特网1110和安全服务器1112。在操作1114处，在MD 1102上开始登录过程。在操作1116处，移动网络1104接收该登录过程启动并将其路由或重新路由到MSOL 1106。在操

作1118处,MSOL 1106通过访问SPD 1108来认证设备,SPD 1108在操作1120处返回认证凭证。在操作1122处,然后由该MSOL1106启动登录过程,其中认证凭证被注入登录过程中。在操作1124处,安全服务器1112接收具有认证凭证的登录过程,并且使用该认证凭证登录到移动设备1102中。在操作1126处,安全服务器1112发送登录成功消息,该登录成功消息在操作1128处由MSOL 1106接收。然后,MSOL1106在操作1130处向MD 1102发送该登录成功消息,MD 1102在操作1132处接收该登录成功消息。

[0078] 图12是示出根据示例实施方式的能够将网络凭证添加到登录过程的MSOL 1200的框图。MSOL 1200可以包含移动设备识别部件1202,移动设备识别部件1202用于识别已经向安全服务器1112发送了(已经被MSOL 1200拦截的)登录过程的请求的移动设备1102。该标识的一部分可以包括移动设备1102的网络标识诸如IMSI。安全简档目录接口1204然后将该标识传递到安全简档目录204,安全简档目录204用于基于该标识来创建认证凭证,并且将该认证凭证返回到MSOL 1200。然后,认证凭证注入部件1206将认证凭证注入到开始登录过程的请求中。然后,分组交换网络接口1208经由分组交换网络将开始登录过程的请求路由到安全服务器1112。

[0079] 应当注意,MSOL 1200和MSOL 202可以是不同的部件,或者在一些示例实施方式中,可以存在组合的MSOL,其具有执行其所有功能的MSOL 202或MSOL 1200中的所有部件。

[0080] 模块、部件和逻辑

[0081] 在本文中将某些实施方式描述为包括逻辑或多个部件、模块和机制。模块可以构成软件模块(例如,机器可读介质上包含的代码)或硬件模块。“硬件模块”是能够执行某些操作的有形单元,并且可以以某种物理方式来配置或布置。在各种示例实施方式中,一个或更多个计算机系统(例如,独立计算机系统、客户端计算机系统或服务器计算机系统)或计算机系统的一个或更多个硬件模块(例如,处理器或处理器组)可以通过软件(例如,应用310或应用部分)被配置为进行操作以执行如本文所描述的某些操作的硬件模块。

[0082] 在一些实施方式中,硬件模块可以机械地、电子地或以其任何合适的组合来实现。例如,硬件模块可以包括永久地配置成执行某些操作的专用电路或逻辑。例如,硬件模块可以是专用处理器,诸如现场可编程门阵列(FPGA)或专用集成电路(ASIC)。硬件模块还可以包括通过软件被临时配置成执行某些操作的可编程逻辑或电路。例如,硬件模块可以包括由通用处理器或其他可编程处理器执行的软件。一旦通过这样的软件被配置,则硬件模块成为特定的机器(或机器的特定部件),其被唯一地定制成执行配置的功能并且不再是通用处理器。应当理解,在专用和永久配置的电路中或在临时配置(例如,通过软件配置)的电路中机械地实现硬件模块的决策可以由成本和时间考虑来驱动。

[0083] 因此,短语“硬件模块”应当被理解成包含有形实体,即为被物理构造、永久配置(例如,硬连线)或临时配置(例如,编程)成以某种方式操作或者执行本文所描述的某些操作的实体。如本文所使用的,“硬件实现的模块”指的是硬件模块。考虑其中硬件模块被临时配置(例如,编程)的实施方式,不需要在任一个时刻处配置或实例化每个硬件模块。例如,在硬件模块包括通过软件配置而成为专用处理器的通用处理器的情况下,通用处理器可以在不同时间处被配置成分别不同的专用处理器(例如,包括不同的硬件模块)。软件相应地配置一个或更多个特定处理器以例如在一个时刻处构成特定硬件模块并且在不同的时刻处构成不同的硬件模块。

[0084] 硬件模块可以向其他硬件模块提供信息并从其他硬件模块接收信息。因此，所描述的硬件模块可以被视为通信地耦接。在同时存在多个硬件模块的情况下，可以通过在两个或更多个硬件模块之间或之中的信号传输(例如，通过适当的电路和总线)来实现通信。在其中多个硬件模块在不同时间处被配置或实例化的实施方式中，可以例如通过在多个硬件模块可以访问的存储器结构中存储并且检索信息来实现这样的硬件模块之间的通信。例如，一个硬件模块可以执行操作并将该操作的输出存储在与其通信地耦接的存储器设备中。然后，另外的硬件模块可以在之后的时间访问存储器设备以检索和处理存储的输出。硬件模块还可以发起与输入或输出设备的通信，并且可以对资源(例如，信息的集合)进行操作。

[0085] 本文描述的示例方法的各种操作可以至少部分地由临时配置(例如，通过软件)或永久配置成执行相关操作的一个或更多个处理器来执行。无论是临时配置还是永久配置，这样的处理器可以构成进行操作以执行本文描述的一个或更多个操作或功能的处理器实现的模块。如本文所使用，“处理器实现的模块”指的是使用一个或更多个处理器实现的硬件模块。

[0086] 类似地，本文描述的方法可以是至少部分地由处理器实现的，其中，一个或更多个特定处理器是硬件的示例。例如，方法的至少一些操作可以由一个或更多个处理器或处理器实现的模块来执行。此外，一个或更多个处理器还可以进行操作以支持“云计算”环境中的相关操作的执行或操作为“软件即服务”(SaaS)。例如，至少一些操作可以由计算机组(作为包括处理器的机器的示例)执行，其中，这些操作是经由网络(例如，因特网1110)以及经由一个或更多个适当的接口(例如，应用程序接口(API))可访问的。

[0087] 某些操作的执行可以被分布在多个处理器之间，不仅驻留在单个机器内，而且被跨多个机器部署。在一些示例实施方式中，处理器或处理器实现的模块可以位于单个地理位置(例如，在家庭环境、办公室环境或服务器群内)。在其他示例实施方式中，处理器或处理器实现的模块可以跨多个地理位置分布。

[0088] 机器和软件架构

[0089] 在一些实施方式中，在机器和相关软件架构的背景下实现了结合图1-12描述的模块、方法、应用310等。以下部分描述了适于与所公开的实施方式一起使用的代表性软件架构和机器(例如，硬件)架构。

[0090] 软件架构与硬件架构结合使用，以创建针对特定目的而定制的设备和机器。例如，与特定软件架构耦合的特定硬件架构将创建移动设备1102，诸如移动电话、平板设备等。稍微不同的硬件和软件架构可以产生用于“物联网”的智能设备，而另一种组合产生用于云计算架构内的服务器计算机。这里并未呈现这样的软件和硬件架构的所有组合，因为本领域技术人员可以容易地理解如何在与本文包含的公开内容不同的背景下实现本发明的主题。

[0091] 软件架构

[0092] 图13是示出可以与本文描述的各种硬件架构结合使用的代表性软件架构1302的框图1300。图13仅是软件架构1302的非限制性示例，并且应当理解，可以实现许多其他架构以有助于本文描述的功能。软件架构1302可以在诸如图14的机器1400的硬件上执行，机器1400包括处理器1410、存储器/储存器1430和I/O部件1450等。示出了代表性硬件层1304，代表性硬件层1304可以表示例如图14的机器1400。代表性硬件层1304包括具有相关联的可执

行指令1308的一个或更多个处理单元1306。可执行指令1308表示包括图1至图12的方法、模块等的实现的软件架构1302的可执行指令。硬件层1304还包括存储器和/或存储模块1310，存储器和/或存储模块1310也具有可执行指令1308。硬件层1304还可以包括代表硬件层1304的任何其他硬件的其他硬件1312，诸如作为机器1400的一部分示出的其他硬件。

[0093] 在图13的示例架构中，软件架构1302可以被概念化为层的堆栈，其中，每个层提供特定功能。例如，软件架构1302可以包括诸如操作系统1314、库1316、框架/中间件1318、应用1320和表示层1344的层。在操作上，应用1320和/或所述层中的其他部件可以通过软件栈激活应用编程接口(API)调用1324，并且响应于API调用1324来接收被示出为消息1326的响应、返回值等。所示出的层本质上是代表性的，并非所有软件架构都具有所有的层。例如，一些移动或专用操作系统1314可能不提供框架/中间件1318，而其他的可以提供这样的层。其他软件架构可以包括另外的层或不同的层。

[0094] 操作系统1314可以管理硬件资源并提供公共服务。操作系统1314可以包括例如核1328、服务1330和驱动器1332。核1328可以用作硬件与其他软件层之间的抽象层。例如，核1328可以负责存储器管理、处理器管理(例如，调度)、部件管理、联网、安全设置等。服务1330可以向其他软件层提供其他公共服务。驱动器1332可以负责控制底层硬件或与底层硬件对接。例如，取决于硬件配置，驱动器1332可以包括显示驱动器、相机驱动器、Bluetooth®驱动器、闪存驱动器、串行通信驱动器(例如，通用串行总线(USB)驱动器)、Wi-Fi®驱动器、音频驱动器、电源管理驱动器等。

[0095] 库1316可以提供可以由应用1320和/或其他部件和/或层利用的公共架构。库1316通常提供允许其他软件模块以相比于与底层操作系统1314功能(例如，核1328、服务1330和/或驱动器1332)直接对接的方式的较为容易的方式来执行任务的功能。库1316可以包括系统库1334(例如，C标准库)，系统库1334可以提供诸如存储器分配功能、字符串操作功能、数学功能等的功能。另外，库1316可以包括API库1336，诸如媒体库(例如，用于支持诸如MPEG4、H.264、MP3、AAC、AMR、JPG、PNG的各种媒体格式的呈现和操作的库)、图形库(例如，可以用于在显示器上呈现图形内容中的2D和3D的OpenGL框架)、数据库库(例如，可以提供各种关系数据库功能的SQLite)、web库(例如，可以提供web浏览功能的WebKit)等。库1316还可以包括各种其他库1338，以向应用1320和其他软件部件/模块提供许多其他API。

[0096] 框架/中间件1318(有时也称为中间件)可以提供可以由应用1320和/或其他软件部件/模块利用的更高级的公共基础结构。例如，框架/中间件1318可以提供各种图形用户界面(GUI)功能、高级资源管理、高级位置服务等。框架/中间件1318可以提供可以由应用1320和/或其他软件部件/模块利用的广泛的其他API，其中一些可以特定于特定操作系统1314或平台。

[0097] 应用1320包括内置应用1340和/或第三方应用1342。代表性内置应用1340的示例可以包括但不限于联系人应用、浏览器应用、书籍阅读器应用、位置应用、媒体应用、消息发送应用和/或游戏应用。第三方应用1342可以包括任何的内置应用1340以及各种其他应用。在特定示例中，第三方应用1342(例如，由除了特定平台的供应商以外的实体使用Android™或iOS™软件开发工具包(SDK)开发的应用)可以是在诸如iOS™、Android™、Windows® Phone的移动操作系统1314或其他移动操作系统1314上运行的移动软件。在该示例中，第三

方应用1342可以激活由诸如操作系统1314的移动操作系统提供的API调用1324，以有助于本文描述的功能。

[0098] 应用1320可以利用内置操作系统功能(例如，核1328、服务1330和/或驱动器1332)、库(例如，系统库1334、API库1336和其他库1338)、框架/中间件1318来创建用户接口以与系统的用户交互。替选地或另外地，在一些系统中，与用户的交互可以通过表示层诸如表示层1344来发生。在这些系统中，应用/模块“逻辑”可以与和用户交互的应用/模块的方面分开。

[0099] 一些软件架构利用虚拟机。在图13的示例中，这由虚拟机1348示出。虚拟机1348创建软件环境，在该软件环境中，应用/模块可以像在硬件机器(例如，图14的机器1400)上执行一样执行。虚拟机1348由主机操作系统(图13中的操作系统1314)托管，并且通常但并非总是具有虚拟机监视器1346，虚拟机监视器1346管理虚拟机1348的操作以及与主机操作系统(即操作系统1314)的对接。软件架构在诸如操作系统1350、库1352、框架/中间件1354、应用1356和/或表示层1358的虚拟机1348内执行。在虚拟机1348内执行的这些软件架构层可以与先前描述的相应层相同或可以是不同的。

[0100] 示例机器架构和机器可读介质

[0101] 图14是示出根据一些示例实施方式的能够从机器可读介质(例如，机器可读存储介质)读取指令1416并执行本文所讨论的任一种或更多种方法的机器1400的部件的框图。具体地，图14示出了计算机系统示例形式的机器1400的图解表示，其中，指令1416(例如，软件、程序、应用1356、小应用、应用或其他可执行代码)用于使机器1400执行以上关于上述端点(例如，移动设备1102、外部网络中的设备)描述的方法。指令1416将通用的未编程的机器1400变换成特定机器，该特定机器被编程为以所描述的方式执行所描述和示出的功能。在替选实施方式中，机器1400作为独立设备操作或者可以耦接(例如，联网)到其他机器。在联网部署中，机器1400可以在服务器客户端网络环境中以服务器机器或客户端机器的身份来操作，或者操作为对等(或分布式)网络环境中的对等机器。机器1400可以包括但不限于服务器计算机、客户端计算机、个人计算机(PC)、平板计算机、膝上型计算机、上网本、机顶盒(STB)、个人数字助理(PDA)、娱乐媒体系统、蜂窝电话、智能电话、移动设备1102、可穿戴设备(例如，智能手表)、智能家居设备(例如，智能家用电器)、其他智能设备、网络设备、网络路由器、网络交换机、网络桥接器或能够顺序地或其他方式执行指定机器1400要采取的动作的指令1416的任何机器1400。此外，虽然仅示出了单个机器1400，但是术语“机器”还应当被视为包括单独地或联合地执行指令1416以执行本文所讨论的任一种或更多种方法的机器1400的集合。

[0102] 机器1400可以包括处理器1410、存储器/储存器1430和I/O部件1450，处理器1410、存储器/储存器1430和I/O部件1450可以被配置成例如经由总线1402相互通信。在示例实施方式中，处理器1410(例如，中央处理单元(CPU)、精简指令集计算(RISC)处理器、复杂指令集计算(CISC)处理器、图形处理单元(GPU)、数字信号处理器(DSP)、专用集成电路(ASIC)、射频集成电路(RFIC)、另外的处理器或其任何合适的组合)可以包括例如可以执行指令1416的处理器1412和处理器1414。术语“处理器”旨在包括多核处理器1412、1414，多核处理器1412、1414可以包括可以同时执行指令1416的两个或更多个独立处理器1412、1414(有时称为“核”)。尽管图14示出了多个处理器1410，但是机器1400可以包括具有单个核的单个处

理器1412、1414、具有多个核的单个处理器1412、1414(例如,多核处理器1412、1414)、具有单个核的多个处理器1412、1414、具有多个核的多个处理器1412、1414或它们的任意组合。

[0103] 存储器/储存器1430可以包括诸如主存储器或其他存储器的存储器1432以及存储单元1436,上述两者都是诸如经由总线1402而可由处理器1410访问的。存储单元1436和存储器1432存储体现本文描述的方法或功能中的任一个或更多个的指令1416。指令1416还可以在其由机器1400执行期间完全地或部分地驻留在存储器1432内、存储单元1436内、处理器1410中的至少一个内(例如,在处理器1412、1414的高速缓冲存储器内)或其任何合适的组合内。因此,存储器1432、存储单元1436和处理器1410的存储器是机器可读介质的示例。

[0104] 如本文所使用,“机器可读介质”意指能够临时或永久地存储指令1416和数据的设备,并且可以包括但不限于随机存取存储器(RAM)、只读存储器(ROM)、缓冲存储器、闪速存储器、光学介质、磁介质、高速缓冲存储器、其他类型的存储器(例如,可擦除可编程只读存储器(EEPROM))和/或其任何合适的组合。术语“机器可读介质”应当被视为包括能够存储指令1416的单个介质或多个介质(例如,集中式或分布式数据库,或相关联的高速缓冲存储器和服务器)。术语“机器可读介质”还应当被视为包括能够存储或携载用于由机器(例如,机器1400)执行的指令(例如,指令1416)的任何介质或多个介质的组合,使得指令1416在由机器1400的一个或更多个处理器(例如,处理器1410)执行时使机器1400执行本文所描述的任一种或更多种方法。因此,“机器可读介质”指的是单个存储装置或设备以及包括多个存储装置或设备的“基于云的”存储系统或存储网络。

[0105] I/O部件1450可以包括各种部件以接收输入、提供输出、产生输出、发送信息、交换信息、捕获测量等。包括在特定机器中的特定I/O部件1450将取决于机器1400的类型。例如,诸如移动电话的便携式机器可能包括触摸输入设备或其他这样的输入机构,而无头服务器机器可能不包括这样的触摸输入设备。应当理解,I/O部件1450可以包括图14中未示出的许多其他部件。I/O部件1450仅为了简化以下讨论而根据功能被分组,并且该分组决不是限制性的。在各种示例实施方式中,I/O部件1450可以包括输出部件1452和输入部件1454。输出部件1452可以包括视觉部件(例如,诸如等离子显示板(PDP)、发光二极管(LED)显示器、液晶显示器(LCD)、投影仪或阴极射线管(CRT)的显示器)、听觉部件(例如,扬声器)、触觉部件(例如,振动马达、阻力机构)、其他信号发生器等。输入部件1454可以包括字母数字输入部件(例如,键盘、配置成接收字母数字输入的触摸屏、光电键盘或其他字母数字输入部件)、基于点的输入部件(例如,鼠标、触摸板、轨迹球、操纵杆、运动传感器或其他指向仪器)、触觉输入部件(例如,物理按钮、提供触摸或触摸手势的位置和/或力的触摸屏或其他触觉输入部件)、音频输入部件(例如,麦克风)等。

[0106] 在其他示例实施方式中,I/O部件1450可以包括广泛的其他部件中的生物识别部件1456、运动部件1458、环境部件1460或定位部件1462。例如,生物识别部件1456可以包括用于检测表达(例如,手表达、面部表情、声音表达、身体姿势或眼睛跟踪)、测量生物信号(例如,血压、心率、体温、出汗或脑波)、识别人(例如,声音识别、视网膜识别、面部识别、指纹识别或基于脑电图的识别)等的部件。运动部件1458可以包括加速度传感器部件(例如,加速度计)、重力传感器部件、旋转传感器部件(例如,陀螺仪)等。环境部件1460可以包括例如照明传感器部件(例如,光度计)、温度传感器部件(例如,检测环境温度的一个或更多个温度计)、湿度传感器部件、压力传感器部件(例如,气压计)、声音传感器部件(例如,检测背

景噪声的一个或更多个麦克风)、接近度传感器部件(例如,检测附近物体的红外传感器)、气体传感器(例如,用于检测危险气体的浓度以确保安全或用于测量大气中的污染物的气体检测传感器)或可以提供与周围物理环境对应的指示、测量或信号的其他部件。位置部件1462可以包括位置传感器部件(例如,全球定位系统(GPS)接收器部件)、海拔高度传感器部件(例如,检测气压的高度计或气压计,根据所述气压可以得到海拔高度)、方向传感器部件(例如,磁力计)等。

[0107] 可以使用各种技术来实现通信。I/O部件1450可以包括通信部件1464,通信部件1464可操作以分别经由耦接1482和耦接1472将机器1400耦接到网络1480或设备1470。例如,通信部件1464可以包括网络接口部件或与网络1480对接的其他合适的设备。在其他示例中,通信部件1464可以包括有线通信部件、无线通信部件、蜂窝通信部件、近场通信(NFC)部件、Bluetooth®部件(例如,低功耗Bluetooth®)、Wi-Fi®部件和经由其他形式提供通信的其他通信部件。设备1470可以是另外的机器或各种外围设备中的任一种(例如,经由通用串行总线(USB)耦接的外围设备)。

[0108] 此外,通信部件1464可以检测标识符或包括可操作以检测标识符的部件。例如,通信部件1464可以包括射频标识(RFID)标签读取器部件、NFC智能标签检测部件、光学读取器部件(例如,用于检测诸如通用产品代码(UPC)条形码的一维条形码、诸如快速响应(QR)码、Aztec码、数据矩阵、Dataglyph、MaxiCode、PDF417、Ultra Code、UCC RSS-2D条形码的多维条形码和其他光学代码的光学传感器)或声学检测部件(例如,用于识别标记的音频信号的麦克风)。另外,可以经由通信部件1464得到各种信息,诸如经由因特网协议(IP)地理位置的位置、经由Wi-Fi®信号三角测量的位置、经由检测可以指示特定位置的NFC信标信号的位置等。

[0109] 传输介质

[0110] 在各种示例实施方式中,网络1480的一个或更多个部分可以是自组织网络、内联网、外联网、虚拟专用网络(VPN)、局域网(LAN)、无线LAN(WLAN)、广域网(WAN)、无线WAN(WWAN)、城域网(MAN)、因特网1110、因特网1110的一部分、公共交换电话网(PSTN)的一部分、普通老式电话服务(POTS)网络、蜂窝电话网络、无线网络、Wi-Fi®网络、另外的类型的网络或两个或更多个这样的网络的组合。例如,网络1480或网络1480的一部分可以包括无线或蜂窝网络,并且耦接1482可以是码分多址(CDMA)连接、全球移动通信系统(GSM)连接或其他类型的蜂窝或无线耦接。在该示例中,耦接1482可以实现各种类型的数据传输技术中的任一种,诸如单载波无线电传输技术(1xRTT)、演进数据优化(EVDO)技术、通用分组无线服务(GPRS)技术、GSM演进的增强数据率(EDGE)技术、包括3G的第三代合作伙伴计划(3GPP)、第四代无线(4G)网络、通用移动电信系统(UMTS)、高速分组接入(HSPA)、全球微波接入互操作性(WiMAX)、长期演进(LTE)标准、由各种标准设置组织定义的其他标准、其他远程协议或其他数据传输技术。

[0111] 指令1416可以经由网络接口设备(例如,包括在通信部件1464中的网络接口部件)使用传输介质并且利用许多公知的传输协议中的任一传输协议(例如,超文本传输协议(HTTP))通过网络1480来发送或接收。类似地,可以使用传输介质经由耦接1472(例如,对等耦接)将指令1416发送或接收到设备1470。术语“传输介质”应当被视为包括能够存储、编码或携载用于由机器1400执行的指令1416的任何无形介质,并且包括数字或模拟通信信号或

有助于这样的软件的通信的其他无形介质。

[0112] 传输介质是机器可读介质的实施方式。

[0113] 以下所编号的示例是实施方式。

[0114] 1.一种移动安全卸载器(MSOL),包括:

[0115] 移动设备识别部件,被配置成在移动无线电网络中从移动设备接收未加密数据并且根据未加密数据来确定移动设备的移动设备标识;

[0116] 安全简档目录接口,被配置成使用移动设备标识从安全简档目录检索与移动设备标识相对应的安全简档,该安全简档标识了用于对来自与移动设备标识对应的移动设备的数据进行加密的安全协议;

[0117] 加密引擎,能够由一个或更多个处理器执行并且被配置成使用在安全简档中标识的安全协议对未加密数据进行加密;以及

[0118] 分组交换网络接口,被配置成经由分组交换网络将经加密的数据路由到在数据中标识的安全服务器。

[0119] 2.根据示例1的MSOL,其中,分组交换网络接口还被配置成从安全服务器接收经加密的响应数据,并且其中,加密引擎还被配置成基于安全简档对经加密的响应数据进行解密。

[0120] 3.根据示例2的MSOL,其中,安全简档目录接口还被配置成将安全简档存储在MSOL上的高速缓冲存储器中。

[0121] 4.根据示例1或示例2的MSOL,其中,移动无线电网络是2G/3G网络,并且未加密数据是经由服务通用分组无线业务(GPRS)支持节点(SGSN)来接收的。

[0122] 5.根据示例1或示例2的MSOL,其中,移动无线电网络是4G网络,并且未加密数据是经由服务网关(SGW)来接收的。

[0123] 6.根据示例1至5中任一项的MSOL,其中,安全简档在多个移动设备标识之间共享并且包含标识了所述多个移动设备标识的字段。

[0124] 7.根据示例1至6中任一项的MSOL,其中,安全简档数据库包含另外的安全简档,所述另外的安全简档标识了用于对来自相应移动设备的数据进行加密的不同安全协议。

[0125] 8.一种方法,包括:

[0126] 在移动安全卸载器(MSOL)处,在移动无线电网络中从移动设备接收未加密数据;

[0127] 根据未加密数据来确定移动设备的移动设备标识;

[0128] 使用移动设备标识从安全简档目录检索与移动设备标识对应的安全简档,该安全简档标识了用于对来自与移动设备标识对应的移动设备的数据进行加密的安全协议;

[0129] 使用在安全简档中标识的安全协议对未加密数据进行加密;以及

[0130] 经由分组交换网络将经加密的数据路由到在数据中标识的安全服务器。

[0131] 9.根据示例8的方法,其中,移动设备标识是国际移动订户标识(IMSI)。

[0132] 10.根据示例8的方法,其中,移动设备标识是移动台国际订户目录号码(MSISDN)。

[0133] 11.根据示例8或示例9的方法,其中,移动设备标识是电话号码。

[0134] 12.根据示例8至11中任一项的方法,还包括:

[0135] 从安全服务器接收经加密的响应数据;以及

[0136] 基于安全简档对经加密的响应数据进行解密。

[0137] 13.根据示例12的方法,还包括:将安全简档存储在MSOL上的高速缓冲存储器中。

[0138] 14.根据示例8至13中任一项的方法,其中,移动无线电网络是2G/3G网络,并且未加密数据是经由服务通用分组无线业务(GPRS)支持节点(SGSN)来接收的。

[0139] 15.根据示例8至13中任一项的方法,其中,移动无线电网络是4G网络,并且未加密数据是经由服务网关(SGW)来接收的。

[0140] 16.根据示例8至15中任一项的方法,其中,安全简档在多个移动设备标识之间共享并且包含标识所述多个移动设备标识的字段。

[0141] 17.示例8至15中任一项的方法,其中,安全简档数据库包含另外的安全简档,另外的安全简档标识了用于对来自相应移动设备的数据进行加密的不同安全协议。

[0142] 18.一种MSOL,包括:

[0143] 移动设备识别部件,被配置成经由移动无线电网络从移动设备接收在安全服务器上开始登录过程的请求并且根据该请求来确定移动设备的移动设备标识;

[0144] 安全简档目录接口,被配置成使用移动设备标识通过安全简档目录认证该移动设备并且响应于该认证从安全简档目录接收认证凭证;以及

[0145] 认证凭证注入部件,能够由一个或更多个处理器执行并且被配置成将认证凭证注入到开始登录过程的请求中;以及

[0146] 分组交换网络接口,被配置成经由分组交换网络将开始登录过程的请求路由到安全服务器。

[0147] 19.根据示例18的MSOL,其中,分组交换网络接口还被配置成从安全服务器接收登录成功消息并且经由移动无线电网络将登录成功消息转发到移动设备。

[0148] 20.一种方法,包括:

[0149] 在MSOL处,经由移动无线电网络从移动设备接收在安全服务器上开始登录过程的请求;

[0150] 根据请求来确定移动设备的移动设备标识;

[0151] 使用移动设备标识从安全简档目录获取与移动设备标识对应的认证凭证;

[0152] 将认证凭证注入到开始登录过程的请求中;以及

[0153] 经由分组交换网络将开始登录过程的请求路由到安全服务器。

[0154] 21.根据示例20的方法,其中,移动设备标识是国际移动订户标识(IMSI)。

[0155] 22.根据示例20或示例21的方法,其中,移动设备标识是移动台国际订户目录号码(MSISDN)。

[0156] 23.根据示例20至22中任一项的方法,还包括:

[0157] 从安全服务器接收登录成功消息并且经由移动无线电网络将登录成功消息转发到移动设备。

[0158] 24.一种携载指令的机器可读介质,所述指令在由机器的处理器执行时使机器执行示例8至17或示例20至23中任一项的方法。

[0159] 语言

[0160] 贯穿本说明书,多个实例可以实现被描述为单个实例的部件、操作或结构。尽管一种或更多种方法的各个操作被示出并描述为分开的操作,但是可以同时执行各个操作中的一个或更多个操作,并且不要求以所示的顺序执行操作。在示例配置中呈现为分开的部件

的结构和功能可以实现为组合结构或部件。类似地，呈现为单个部件的结构和功能可以实现为分开的部件。这些和其他变型、修改、添加和改进都落入本文的主题的范围内。

[0161] 尽管已经参考具体示例实施方式描述了本发明主题的概述，但是在不脱离本公开内容的实施方式的宽泛的范围的情况下，可以对这些实施方式进行各种修改和改变。本发明主题的这样的实施方式在本文中可以单独地或共同地通过术语“发明”来提及，仅是出于方便，而不意在在实际上公开了不止一个公开内容或发明构思的情况下将本申请的范围自主地限制于任何单个公开内容或发明构思。

[0162] 本文所示的实施方式被足够详细地描述以使本领域技术人员能够实践所公开的教导。可以使用并且根据其得到其他实施方式，使得可以在不脱离本公开内容的范围的情况下进行结构和逻辑替换和改变。因此，具体描述不应当被视为限制意义，并且各种实施方式的范围仅由所附权利要求连同这些权利要求所具有的等同方案的完全范围来限定。

[0163] 如本文所使用，术语“或”可以被解释成包括性或排他性意义。此外，可以针对在本文中被描述为单个实例的资源、操作或结构提供多个实例。另外，各种资源、操作、模块、引擎和数据存储装置之间的边界在某种程度上是任意的，并且在特定说明性配置的背景下示出了特定操作。设想了其他的功能分配，并且所述其他的功能分配可以落入本公开内容的各种实施方式的范围内。通常，在示例配置中呈现为分开的资源的结构和功能可以实现为组合结构或资源。类似地，呈现为单个资源的结构和功能可以实现为分开的资源。这些和其他变型、修改、添加和改进落入由所附权利要求表示的本公开内容的实施方式的范围内。因此，说明书和附图应当被视为说明性的而非限制性意义的。

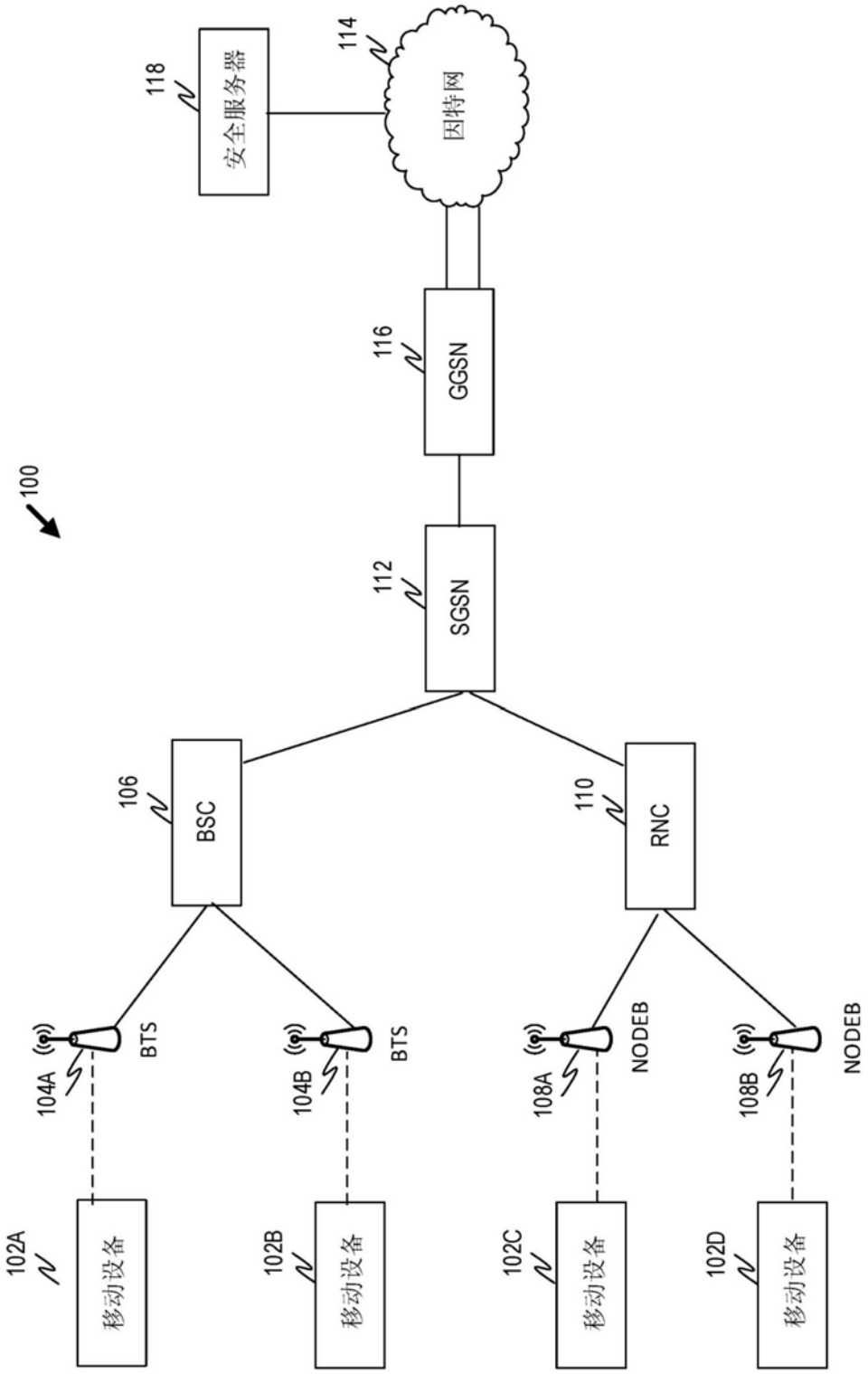

100
118
安全服务器
114
因特网
116
GGSN
112
SGSN
106
BSC
110
RNC
104A
BTS
104B
BTS
108A
NODEB
108B
NODEB
102A
移动设备
102B
移动设备
102C
移动设备
102D
移动设备

图1

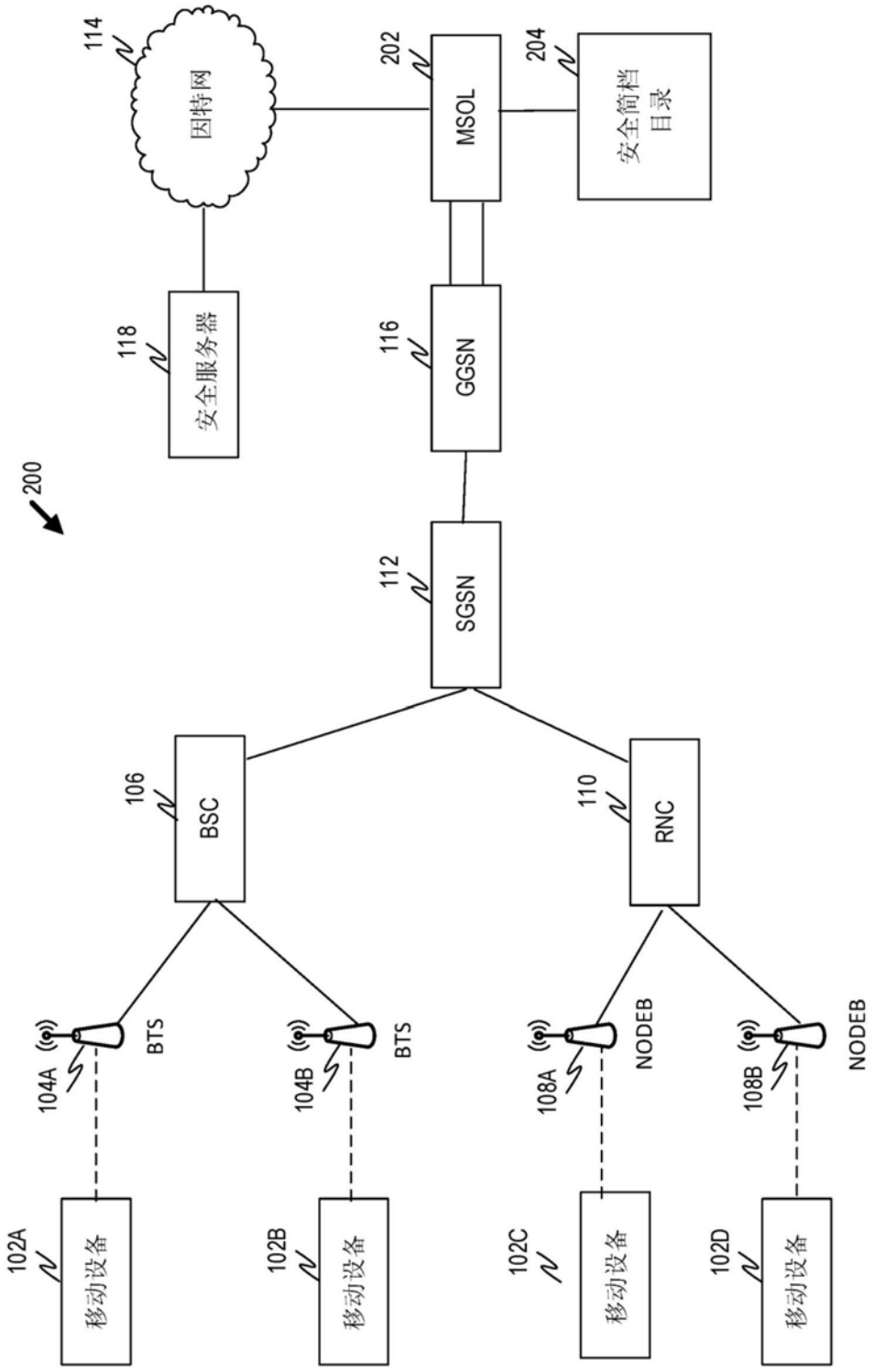

114
因特网
202
MSOL
204
安全简档目录
118
安全服务器
116
GGSN
200
112
SGSN
106
BSC
110
RNC
104A
BTS
104B
BTS
108A
NODEB
108B
NODEB
102A
移动设备
102B
移动设备
102C
移动设备
102D
移动设备

图2

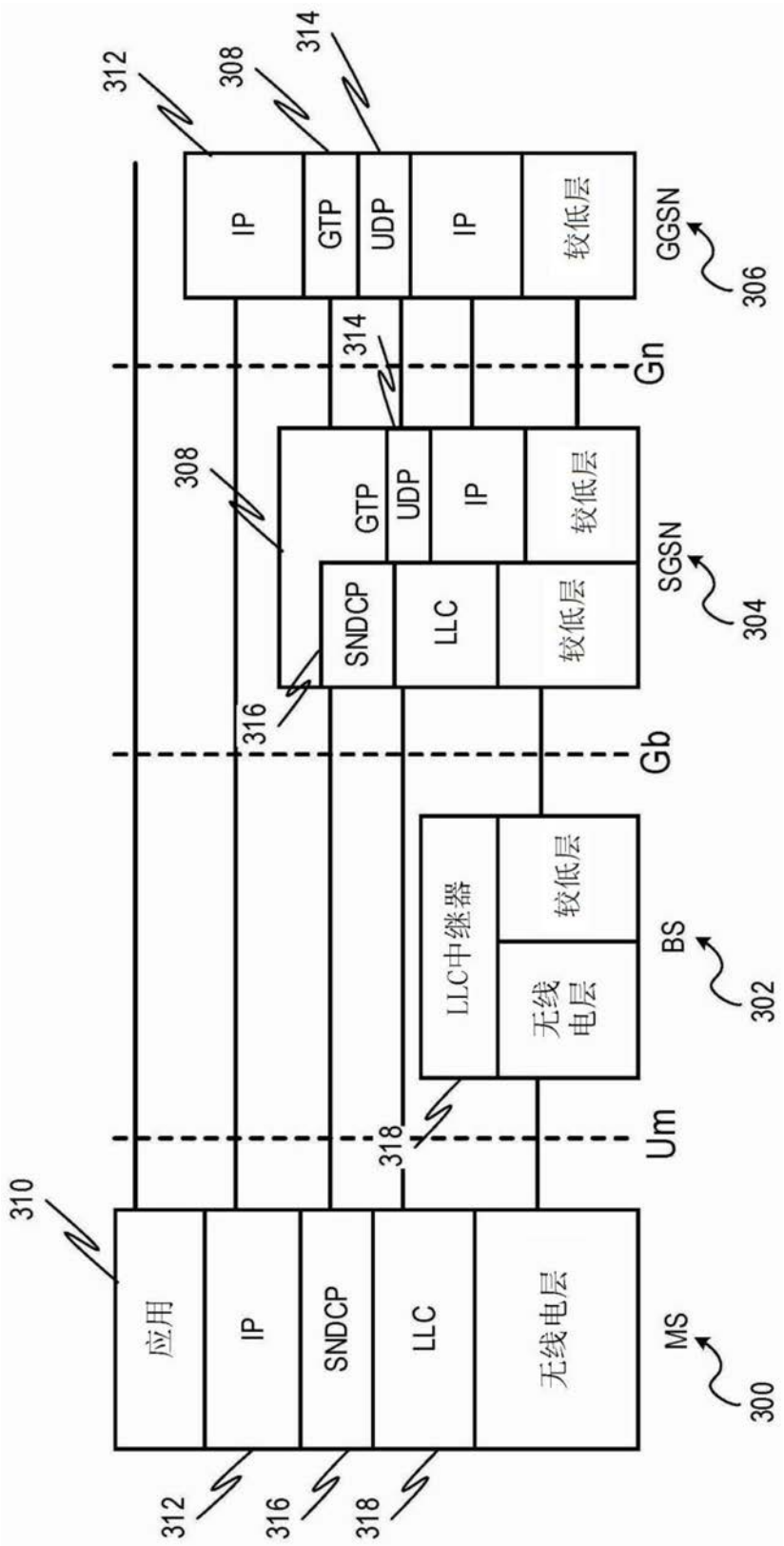

312
308
314
IP
GTP
UDP
IP
较低层
GGSN
306
Gn
314
308
GTP
UDP
IP
较低层
SNDCP
LLC
较低层
SGSN
304
316
Gb
LLC中继器
较低层
无线电层
BS
302
318
Um
310
应用
IP
SNDCP
LLC
无线电层
MS
300
312
316
318

图3

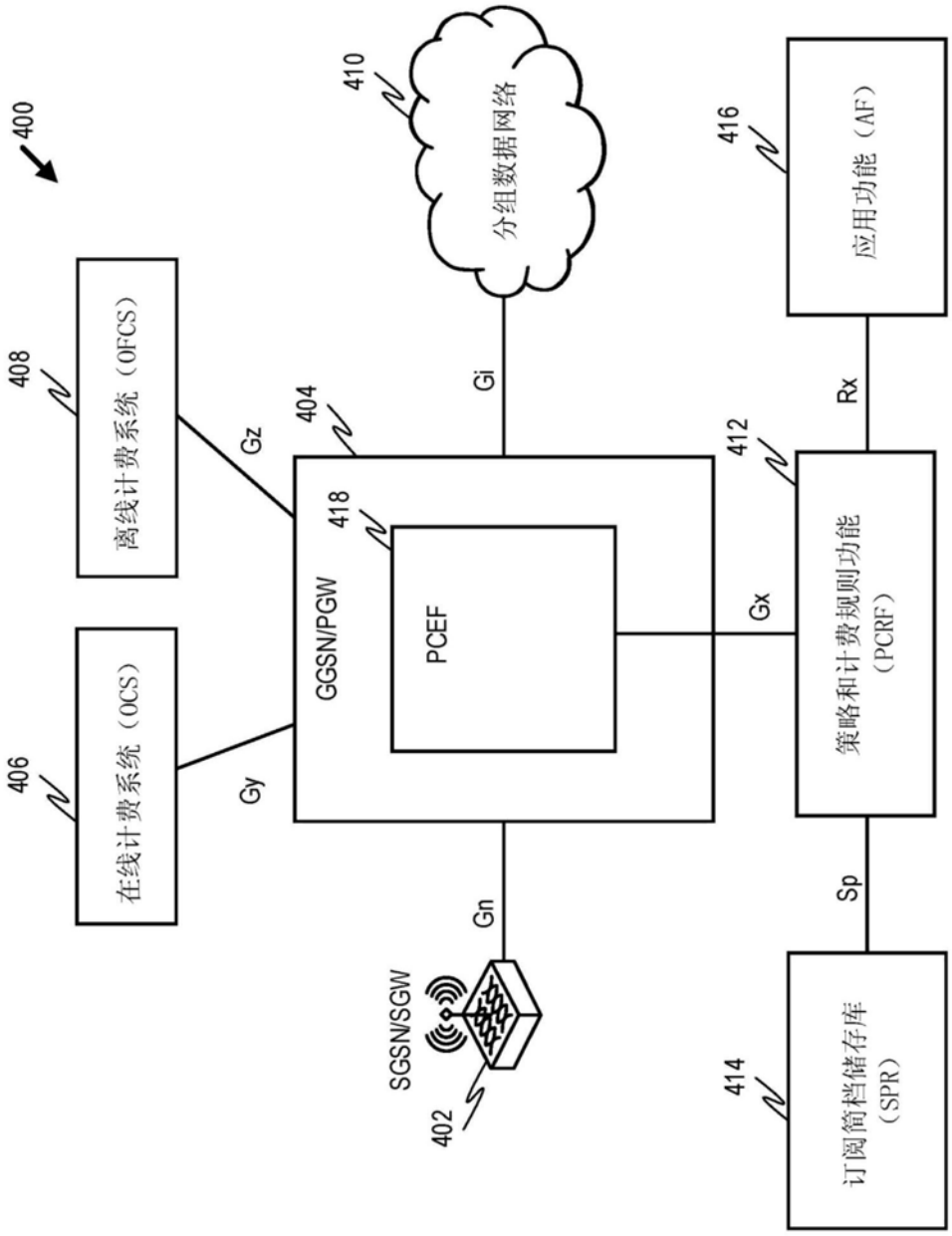

400
410
分组数据网络
416
应用功能（AF）
408
离线计费系统（OFCS）
Gz
404
Gi
Rx
412
418
GGSN/PGW
PCEF
Gx
策略和计费规则功能
（PCRF）
406
在线计费系统（OCS）
Gy
Gn
Sp
SGSN/SGW
402
414
订阅简档储存库
（SPR）

图4

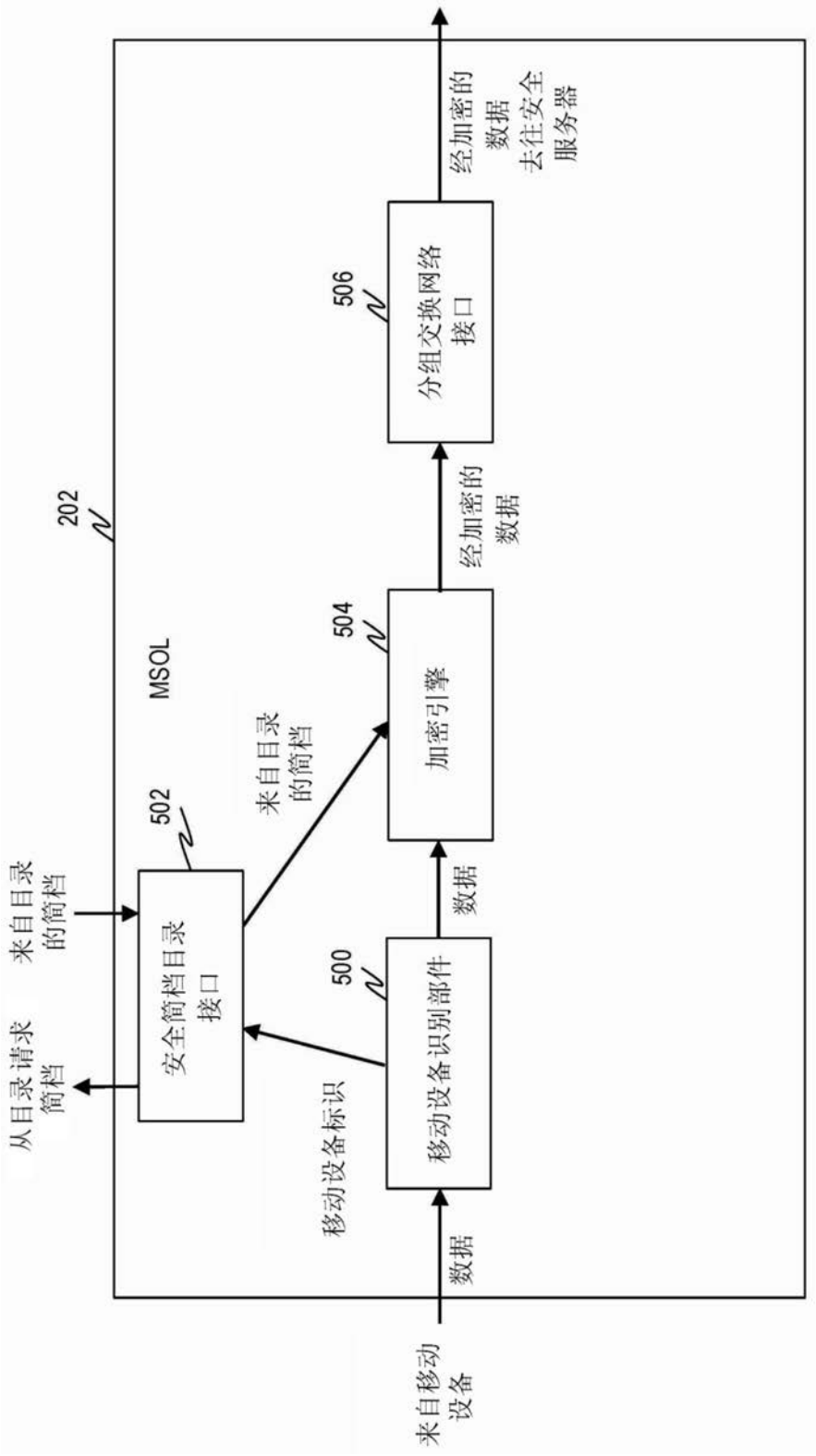

202
MSOL
502
安全简档目录接口
来自目录的简档
从目录请求简档
来自目录的简档
504
加密引擎
经加密的数据
506
分组交换网络接口
经加密的数据去往安全服务器
500
移动设备识别部件
移动设备标识
数据
数据
来自移动设备

图5

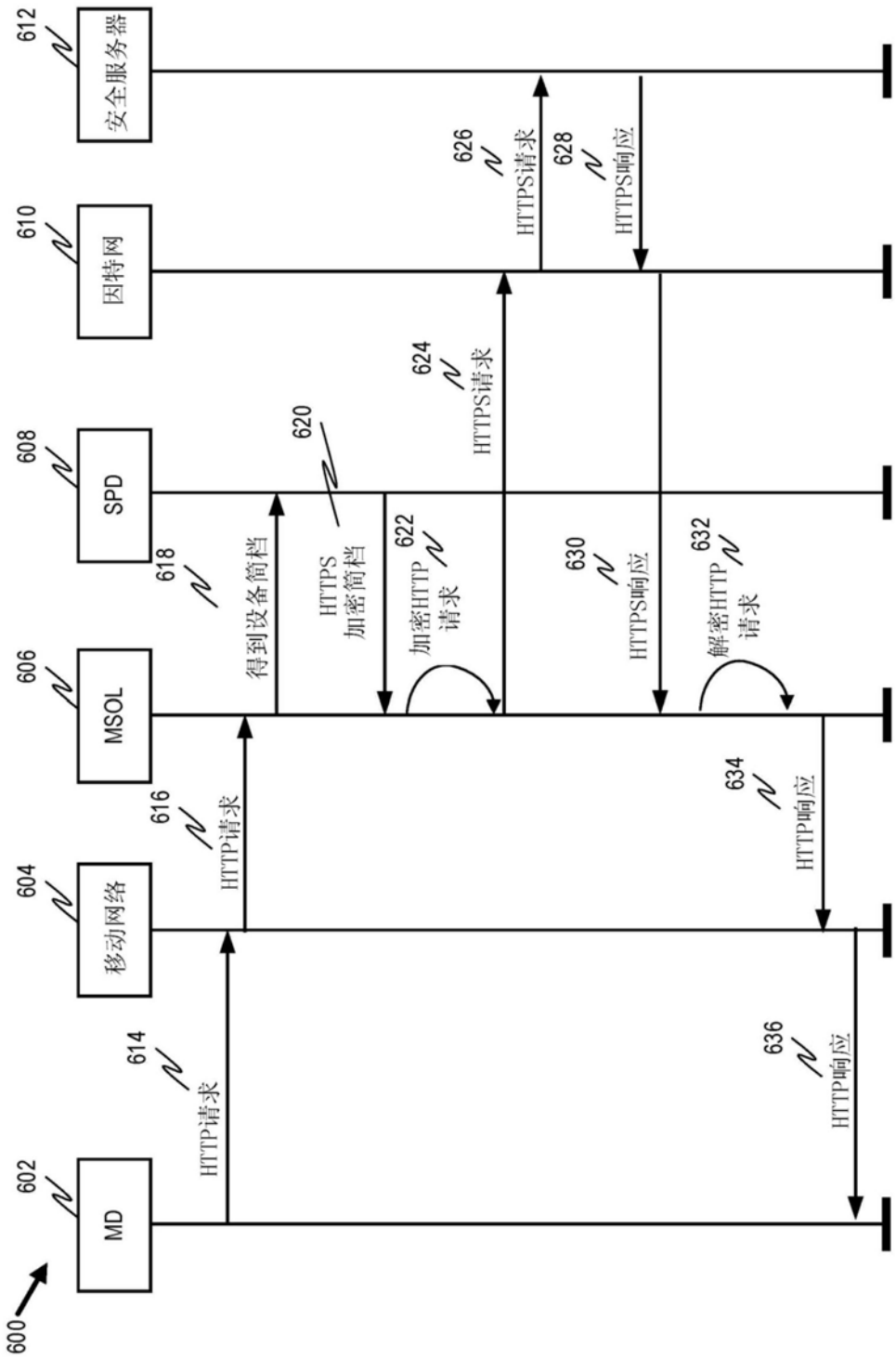

600
602
MD
604
移动网络
606
MSOL
608
SPD
610
因特网
612
安全服务器
614
HTTP请求
616
HTTP请求
618
得到设备简档
620
HTTPS
加密简档
622
加密HTTP
请求
624
HTTPS请求
626
HTTPS请求
628
HTTPS响应
630
HTTPS响应
632
解密HTTP
请求
634
HTTP响应
636
HTTP响应

图6

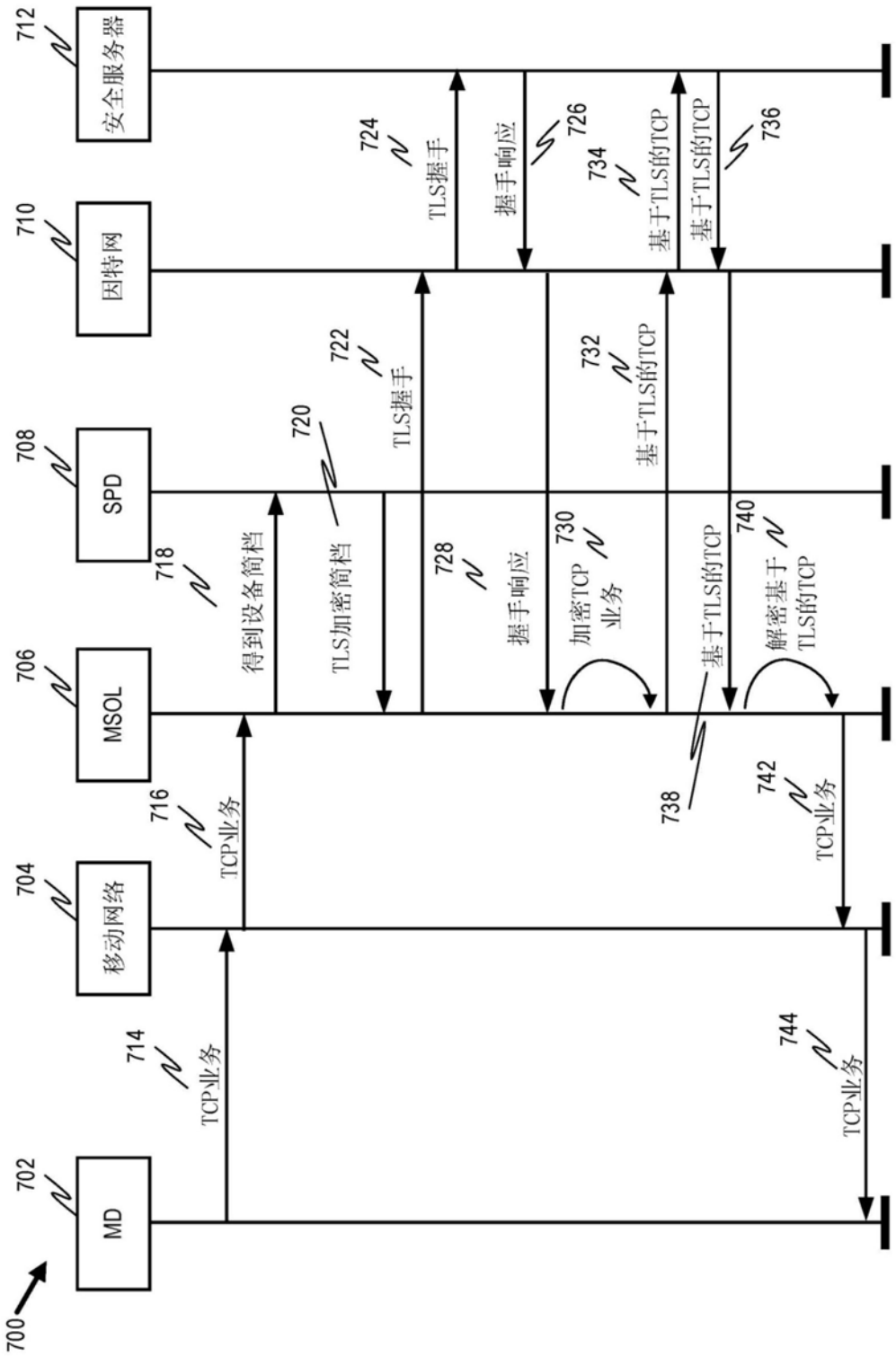

700
MD
702
移动网络
704
MSOL
706
SPD
708
因特网
710
安全服务器
712
TCP业务
714
TCP业务
716
得到设备简档
718
TLS加密简档
720
TLS握手
722
握手响应
728
加密TCP业务
730
基于TLS的TCP
732
基于TLS的TCP
734
TLS握手
724
握手响应
726
基于TLS的TCP
736
解密基于TLS的TCP
740
基于TLS的TCP
738
TCP业务
742
TCP业务
744

图7

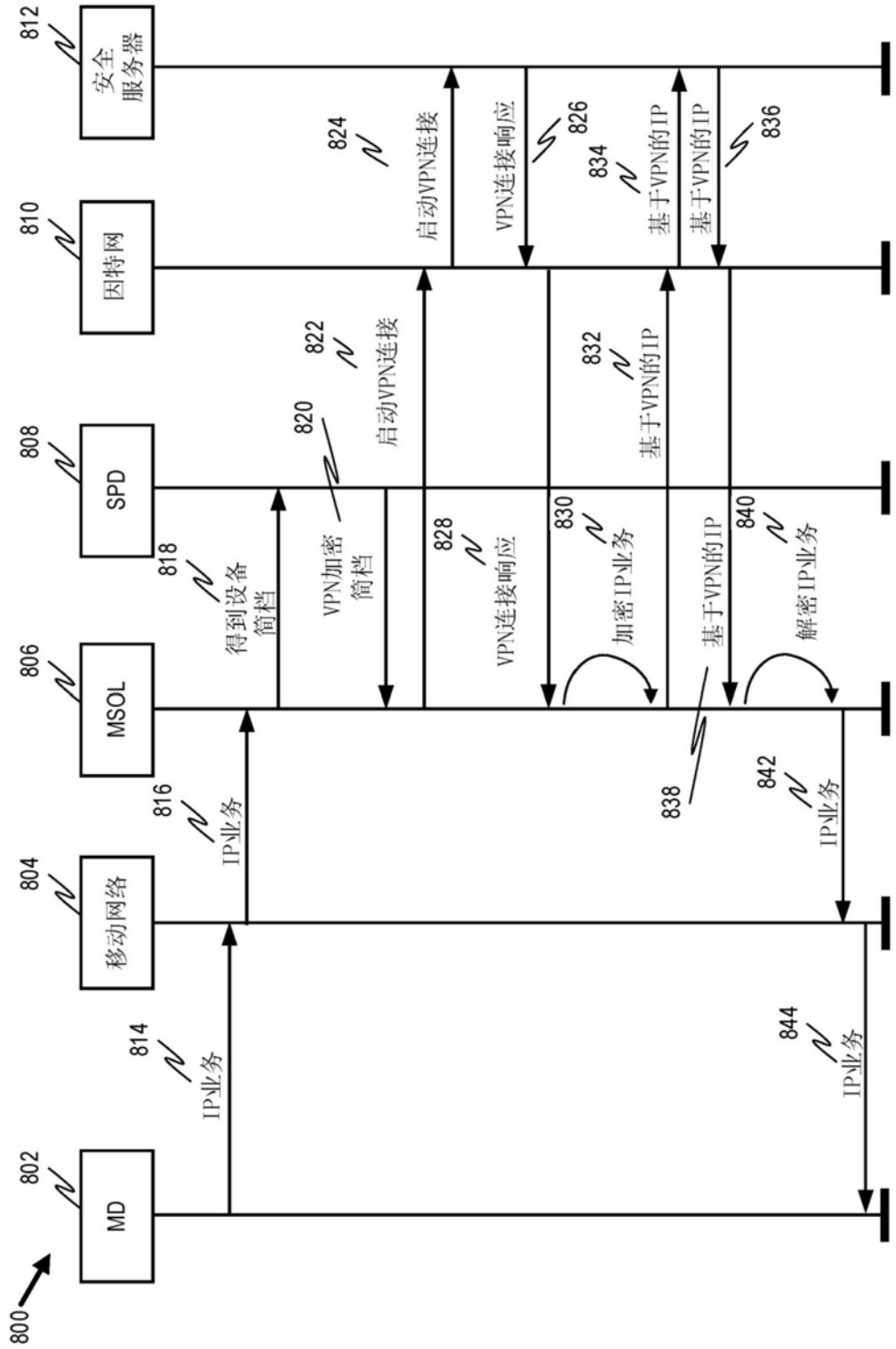

800
802
MD
804
移动网络
806
MSOL
808
SPD
810
因特网
812
安全服务器
814
IP业务
816
IP业务
818
得到设备简档
820
VPN加密简档
822
启动VPN连接
824
启动VPN连接
826
VPN连接响应
828
VPN连接响应
830
加密IP业务
832
基于VPN的IP
834
基于VPN的IP
836
基于VPN的IP
838
840
解密IP业务
842
IP业务
844
IP业务

图8

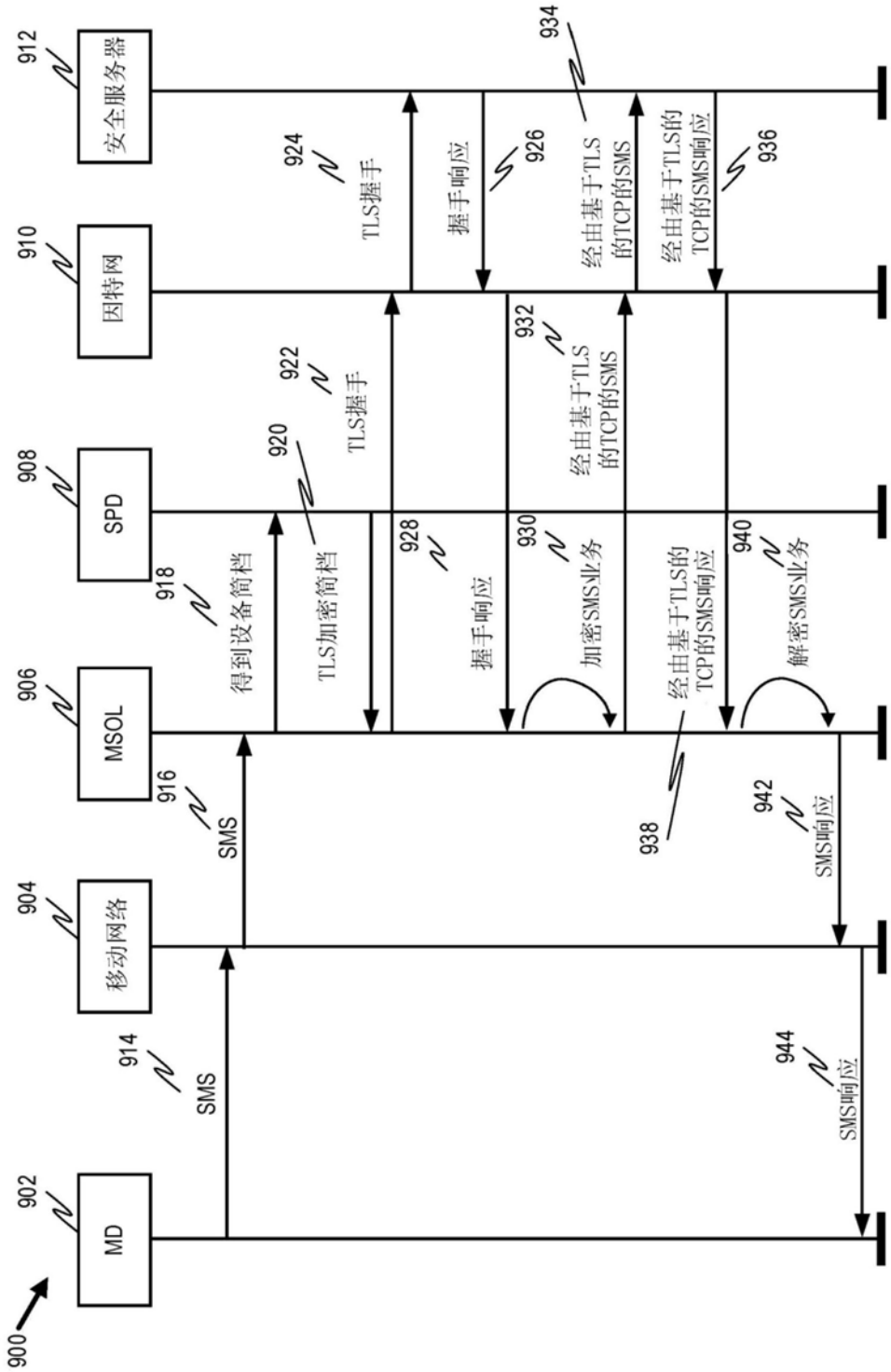

900
902
MD
904
移动网络
906
MSOL
908
SPD
910
因特网
912
安全服务器
914
SMS
916
SMS
918
得到设备简档
920
TLS加密简档
922
TLS握手
924
TLS握手
926
握手响应
928
握手响应
930
加密SMS业务
932
经由基于TLS的TCP的SMS
934
经由基于TLS的TCP的SMS
936
经由基于TLS的TCP的SMS响应
938
经由基于TLS的TCP的SMS响应
940
解密SMS业务
942
SMS响应
944
SMS响应

图9

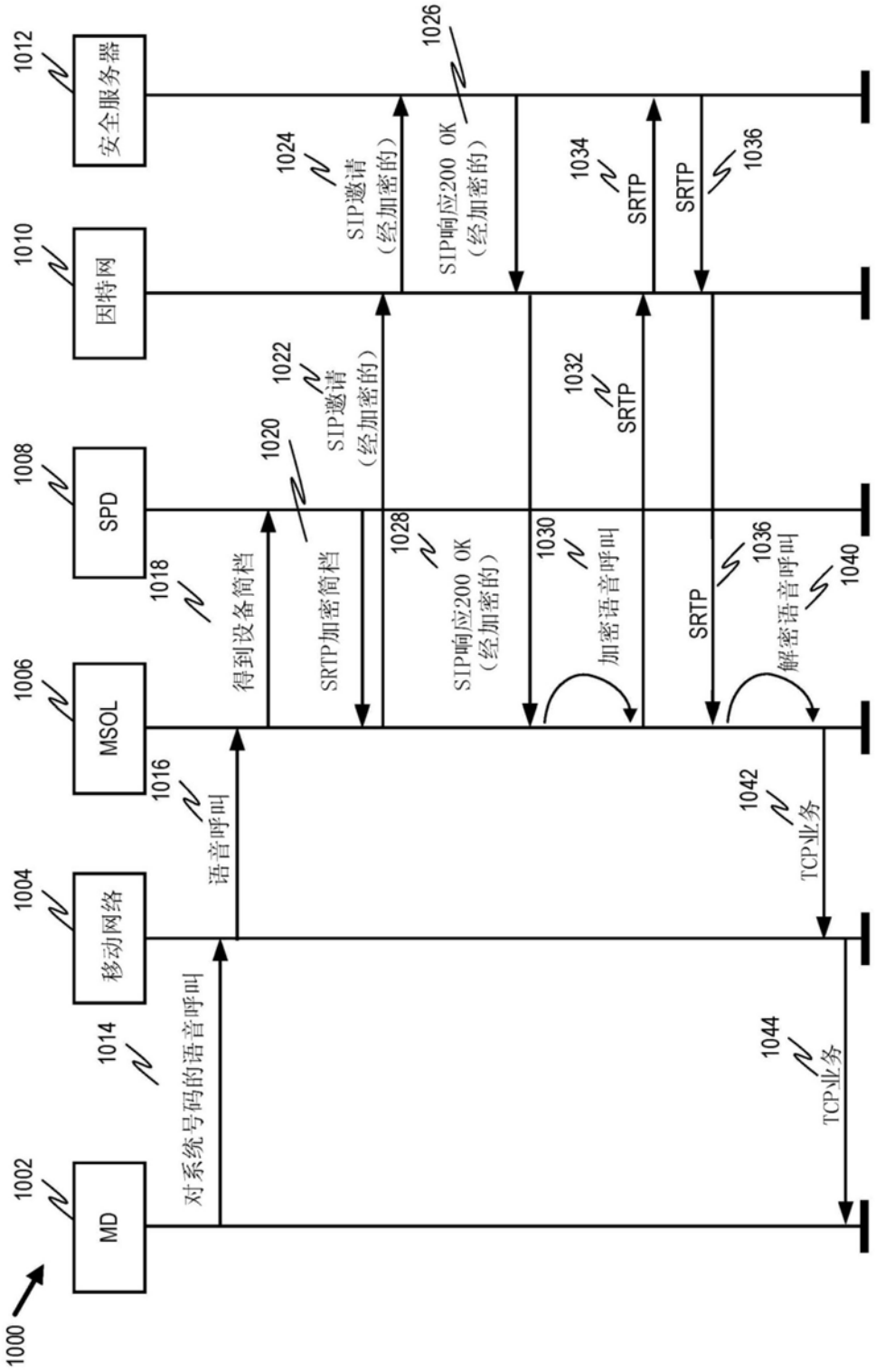

1000
1002
MD
1004
移动网络
1006
MSOL
1008
SPD
1010
因特网
1012
安全服务器
1014
对系统号码的语音呼叫
1016
语音呼叫
1018
得到设备简档
1020
SRTP加密简档
1022
SIP邀请
（经加密的）
1024
SIP邀请
（经加密的）
1026
SIP响应200 OK
（经加密的）
1028
SIP响应200 OK
（经加密的）
1030
加密语音呼叫
1032
SRTP
1034
SRTP
1036
SRTP
1036
解密语音呼叫
1040
1042
TCP业务
1044
TCP业务

图10

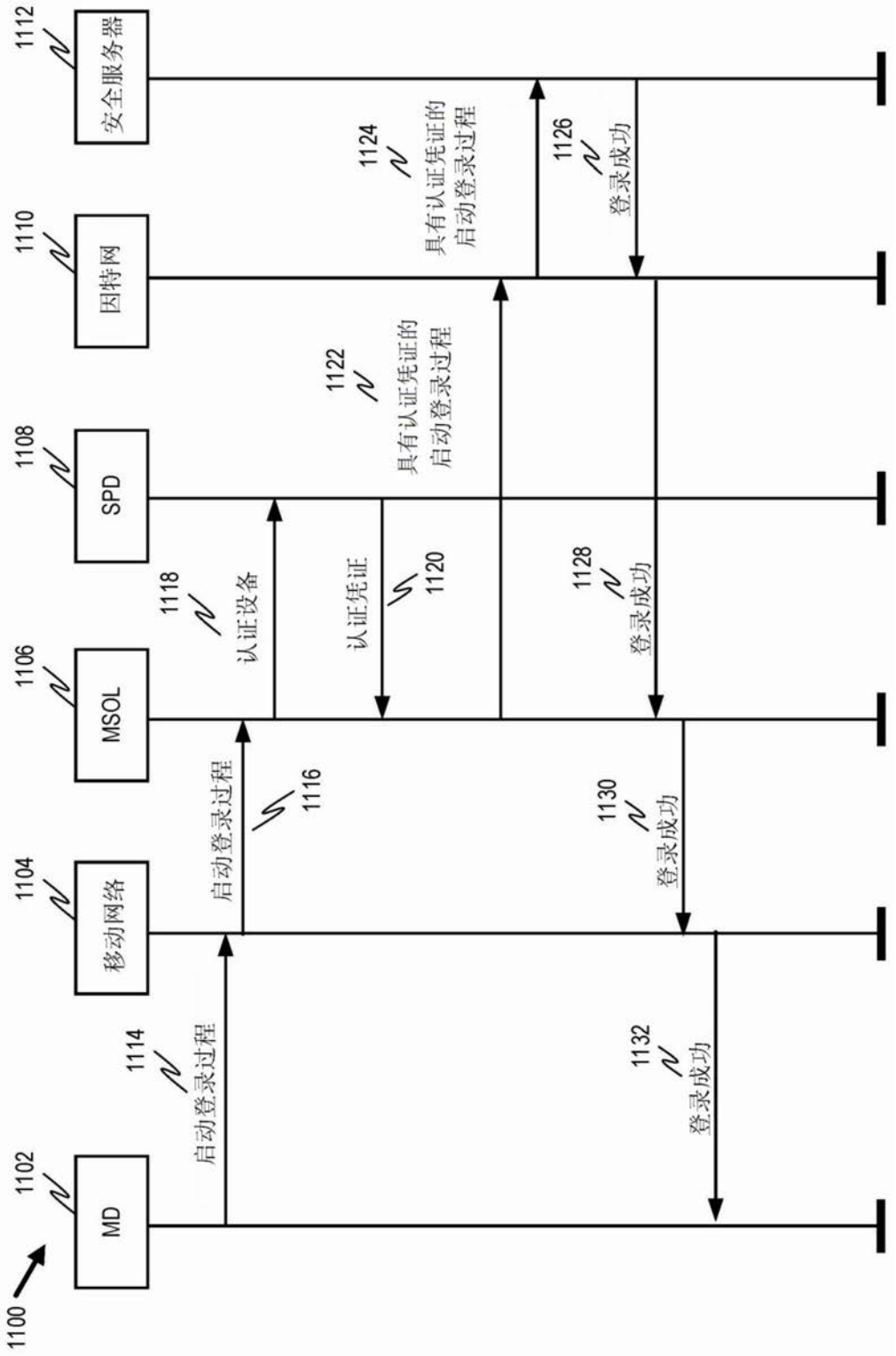

1100
1102
MD
1104
移动网络
1106
MSOL
1108
SPD
1110
因特网
1112
安全服务器
1114
启动登录过程
1116
启动登录过程
1118
认证设备
1120
认证凭证
1122
具有认证凭证的启动登录过程
1124
具有认证凭证的启动登录过程
1126
登录成功
1128
登录成功
1130
登录成功
1132
登录成功

图11

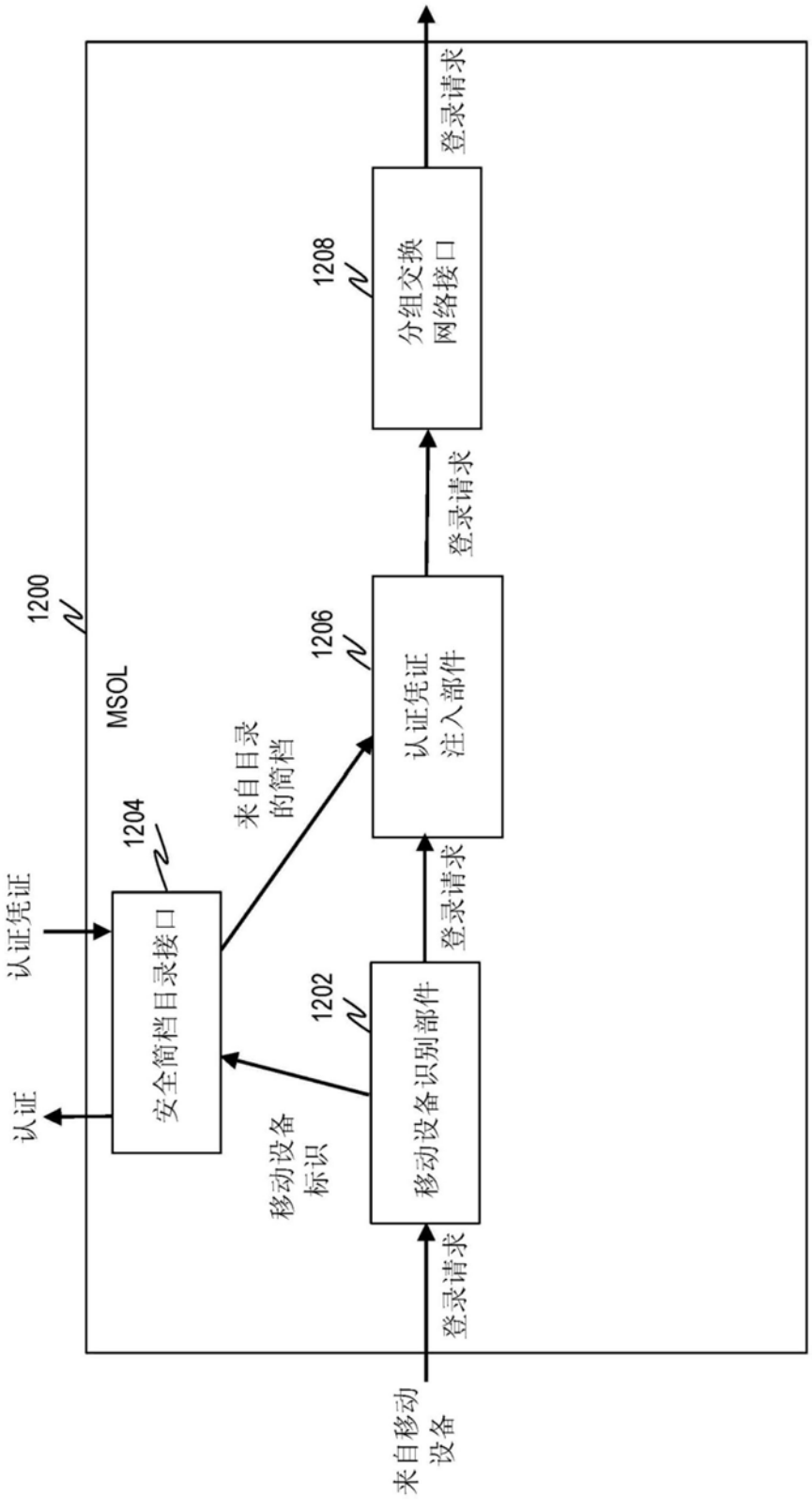

1200
MSOL
1202
移动设备识别部件
1204
安全简档目录接口
1206
认证凭证注入部件
1208
分组交换网络接口
来自移动设备
登录请求
登录请求
登录请求
登录请求
移动设备标识
来自目录的简档
认证凭证
认证

图12

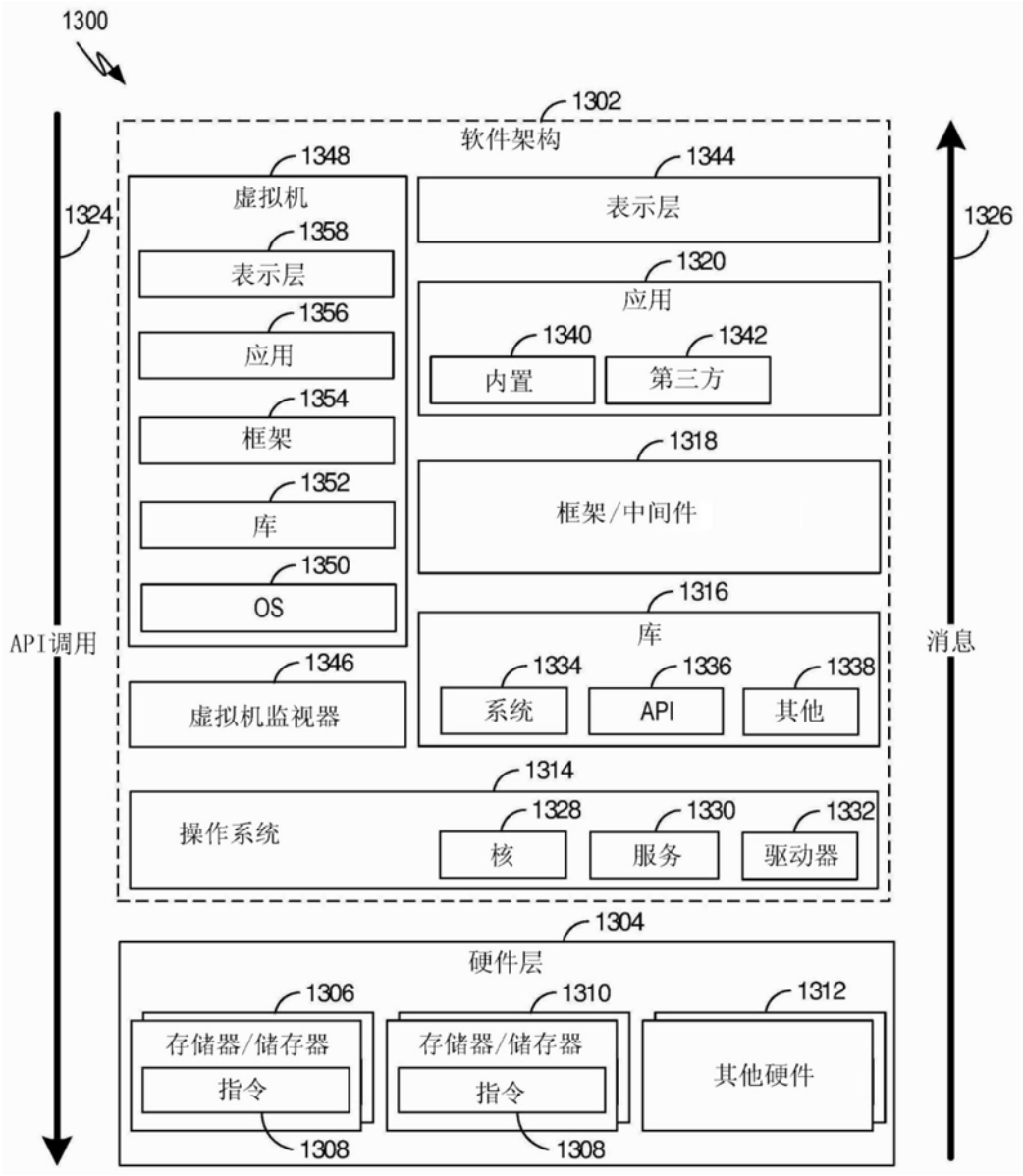

1300
1302
软件架构
1348
虚拟机
1358
表示层
1356
应用
1354
框架
1352
库
1350
OS
1346
虚拟机监视器
1344
表示层
1320
应用
1340
内置
1342
第三方
1318
框架/中间件
1316
库
1334
系统
1336
API
1338
其他
1314
操作系统
1328
核
1330
服务
1332
驱动器
1324
API调用
1326
消息
1304
硬件层
1306
存储器/储存器
指令
1308
1310
存储器/储存器
指令
1308
1312
其他硬件

图13

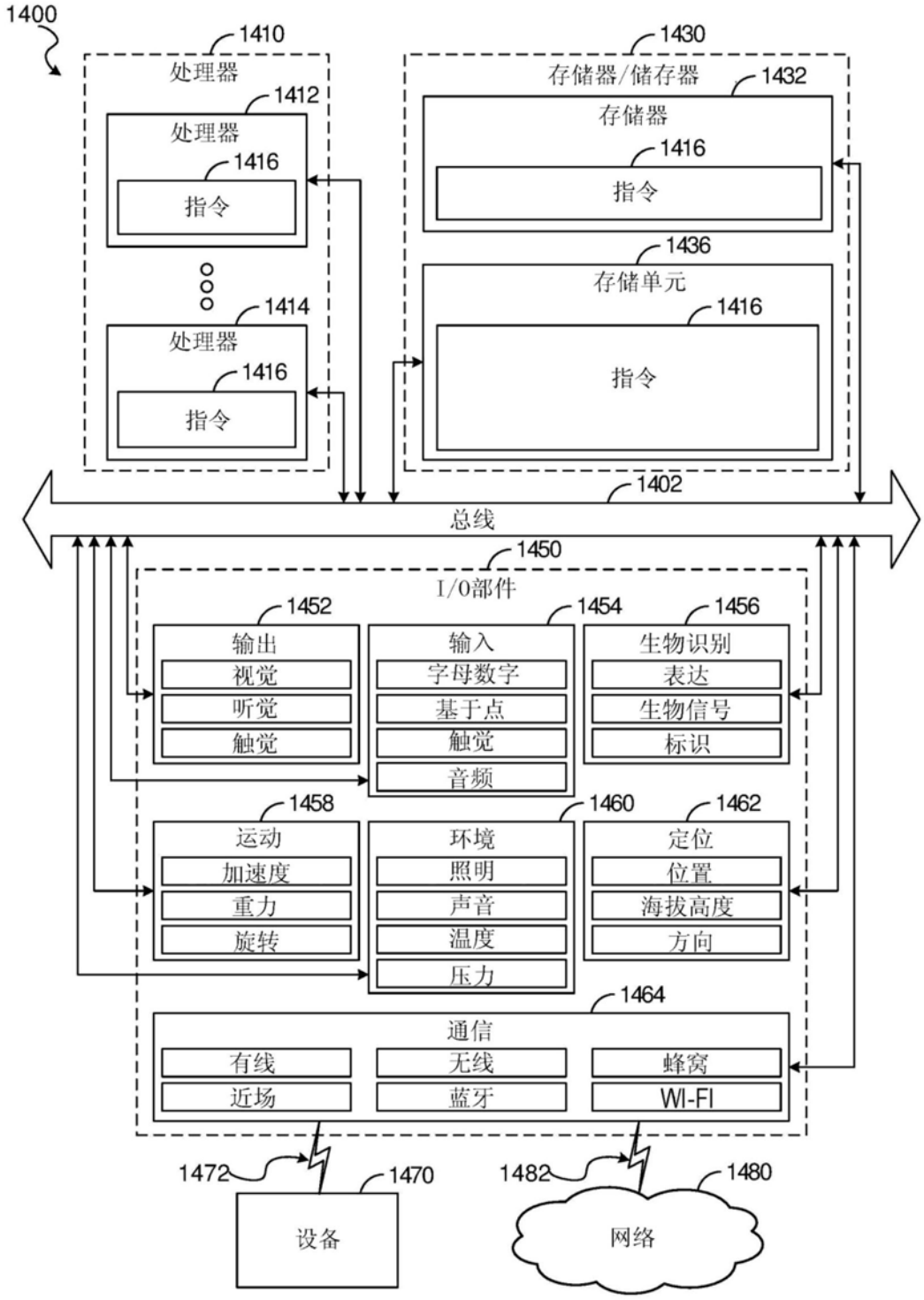

1400
1410
处理器
1412
处理器
1416
指令
1414
处理器
1416
指令
1430
存储器/储存器
1432
存储器
1416
指令
1436
存储单元
1416
指令
1402
总线
1450
I/O部件
1452
输出
视觉
听觉
触觉
1454
输入
字母数字
基于点
触觉
音频
1456
生物识别
表达
生物信号
标识
1458
运动
加速度
重力
旋转
1460
环境
照明
声音
温度
压力
1462
定位
位置
海拔高度
方向
1464
通信
有线
近场
无线
蓝牙
蜂窝
WI-FI
1472
1470
设备
1482
1480
网络

图14