

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 1 月 26 日 (26.01.2017)



(10) 国际公布号
WO 2017/012142 A1

- (51) 国际专利分类号:
H04W 12/08 (2009.01)
- (21) 国际申请号: PCT/CN2015/085860
- (22) 国际申请日: 2015 年 7 月 31 日 (31.07.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510434054.3 2015 年 7 月 22 日 (22.07.2015) CN
- (71) 申请人: 宇龙计算机通信科技(深圳)有限公司
(YULONG COMPUTER TELECOMMUNICATION
SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中
国广东省深圳市南山区科技园北区梦溪道 2 号,
Guangdong 518057 (CN)。
- (72) 发明人: 蒋颁 (JIANG, Ban); 中国广东省深圳市南
山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。

- (74) 代理人: 广州三环专利代理有限公司 (GUANG-
ZHOU SCIHEAD PATENT AGENT CO., LTD); 中
国广东省广州市越秀区先烈中路 80 号汇华商贸大厦
1508 室, Guangdong 510070 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保
护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,
CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU,
LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA,
RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST,
SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保
护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA,
RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,
BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH,
CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE,
IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,
RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: DUAL-CONNECTION SECURITY COMMUNICATION METHOD AND APPARATUS

(54) 发明名称: 一种双连接安全通讯的方法及装置

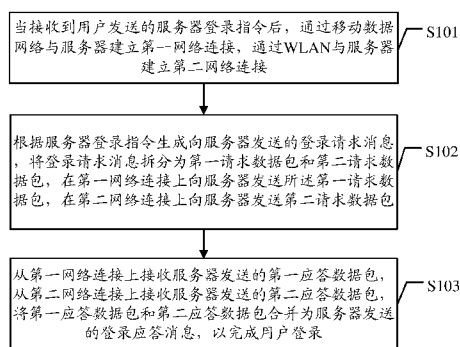


图 2

S101 AFTER RECEIVING A SERVER LOGIN INSTRUCTION SENT BY A USER, ESTABLISH A FIRST NETWORK CONNECTION WITH A SERVER BY MEANS OF A MOBILE DATA NETWORK, AND ESTABLISH A SECOND NETWORK CONNECTION WITH THE SERVER BY MEANS OF A WLAN

S102 GENERATE, ACCORDING TO THE SERVER LOGIN INSTRUCTION, A LOGIN REQUEST MESSAGE SENT TO THE SERVER, SPLIT THE LOGIN REQUEST MESSAGE INTO A FIRST REQUEST DATA PACKET AND A SECOND REQUEST DATA PACKET, SEND THE FIRST REQUEST DATA PACKET TO THE SERVER ON THE FIRST NETWORK CONNECTION, AND SEND THE SECOND REQUEST DATA PACKET TO THE SERVER ON THE SECOND NETWORK CONNECTION

S103 RECEIVE A FIRST ANSWER DATA PACKET, SENT BY THE SERVER, FROM THE FIRST NETWORK CONNECTION, RECEIVE A SECOND ANSWER DATA PACKET, SENT BY THE SERVER, FROM THE SECOND NETWORK CONNECTION, AND COMBINE THE FIRST ANSWER DATA PACKET AND THE SECOND ANSWER DATA PACKET INTO A LOGIN ANSWER MESSAGE SENT BY THE SERVER, SO AS TO COMPLETE USER LOGIN

(57) Abstract: Disclosed are a dual-connection security communication method and apparatus. The method comprises: establishing a first network connection with a server by means of a mobile data network, and establishing a second network connection with the server by means of a WLAN; splitting a login request message sent, by a terminal, to the server into a first request data packet and a second request data packet; sending the first request data packet on the first network connection, and sending the second request data packet on the second network connection; and receiving a first answer data packet from the first network connection, receiving a second answer data packet from the second network connection, and combining the first answer data packet and the second answer data packet into a login answer message sent, by the server, to the terminal, so as to complete user login. The present solution prevents a network attacker from intercepting a complete communication message of a user in a network, thereby improving the security of login modes of the user and a server.

(57) 摘要: 本发明实施例公开了一种双连接安全通讯的方法及装置, 包括: 通过移动数据网络与服务器建立第一网络连接, 通过 WLAN 与服务器建立第二网络连接; 将终端发送给服务器的登录请求消息拆分为第一请求数据包和第二请求数据包; 在第一网络连接的发送所述第一请求数据包, 在第二网络连接的发送第二请求数据包; 从第一网络连接的接收第一应答数据包, 在第二网络连接的接收第二应答数据包, 将第一应答数据包和第二应答数据包合并为服务器发送给终端的登录应答消息, 以完成用户登录。本方案避免了网络攻击者在网络中截获用户的完整通信消息, 从而增强用户跟服务器登录方式的安全性。

WO 2017/012142 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种双连接安全通讯的方法及装置

本申请要求于 2015 年 07 月 22 日提交中国专利局，申请号为 201510434054.3、发明名称为“一种双连接安全通讯的方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及通信技术领域，尤其涉及一种双连接安全通讯的方法及装置。

背景技术

10 随着移动设备的普及应用，用户通过移动终端登录网上服务器以获得网络服务已经成为人们生活中必不可少的活动，因此网络的安全问题也越来越受到人们的重视。目前有很多黑客利用网络软件的漏洞，通过对网关、路由器等网络设备的攻击、信息截获等手段获取用户的账号和密码信息，以谋取利益。用户的信息遭到泄露和篡改，侵害了用户的权益，严重的情况下，可能使用户受到经济损失。

15 目前提高网络安全性的方法主要是通过软件方式，如何通过提供可靠的通信方式提高用户登录服务器的安全性目前属于一项空白。

发明内容

20 本发明实施例公开了一种双连接安全通讯的方法及装置，将用户与服务器的通信消息拆分为不同的数据包，通过终端与服务器之间建立的两条网络连接的方式分别在两条连接上传输不同的数据包，同时将从两条连接上接收到的不同数据包合并为通信消息以完成安全通讯，可以避免网络攻击者在同一网络连接上截获用户的完整通信消息，从而增强用户跟服务器登录方式的安全性。

25 本发明实施例第一方面提供了一种双连接安全通讯的方法，用于终端设备，包括：

当接收到用户发送的服务器登录指令后，通过移动数据网络与服务器建立第一网络连接，通过无线局域网（WLAN，Wireless Local Access Network）与

服务器建立第二网络连接;

根据服务器登录指令生成向服务器发送的登录请求消息,将登录请求消息拆分为第一请求数据包和第二请求数据包,在第一网络连接上向服务器发送第一请求数据包,在第二网络连接上向服务器发送第二请求数据包;

- 5 从第一网络连接上接收服务器发送的第一应答数据包,从第二网络连接上接收服务器发送的第二应答数据包,将第一应答数据包和第二应答数据包合并为服务器发送的登录应答消息,以完成用户登录。

结合第一方面,在第一种可能的实现方式中,登录应答消息包括登录成功消息或登录失败消息;

- 10 在将第一应答数据包和第二应答数据包合并为服务器发送的登录应答消息之后,该方法还包括:

若服务器发送的登录应答消息为登录失败消息,则用户登录失败,断开通过移动数据网络与服务器建立的第一网络连接,并且断开通过 WLAN 与服务器建立的第二网络连接,以结束用户登录;

- 15 若服务器发送的登录应答消息为登录成功消息,则用户登录成功,断开通过移动数据网络与服务器建立的第一网络连接,以完成用户登录;或者,

若服务器发送的登录应答消息为登录成功消息,则用户登录成功,断开通过 WLAN 与服务器建立的第二网络连接,以完成用户登录。

- 20 结合第一方面,在第二种可能的实现方式中,在通过移动数据网络与服务器建立第一网络连接之前,该方法还包括:

在移动数据网络中发起网络注册,若网络注册成功,则通过移动数据网络与服务器建立第一网络连接;

在通过 WLAN 与服务器建立第二网络连接之前,该方法还包括:

- 25 在 WLAN 中发起安全认证,若安全认证成功,则通过 WLAN 与服务器建立第二网络连接;或者,在移动数据网络中发起网络注册,若网络注册成功,则通过 WLAN 与服务器建立第二网络连接。

本发明实施例第二方面提供了一种双连接安全通讯的方法,用于服务器,包括:

通过移动数据网络与终端建立第一网络连接,通过 WLAN 与终端建立第

二网络连接;

从第一网络连接上接收终端发送的第一请求数据包,从第二网络连接上接收终端发送的第二请求数据包,合并第一请求数据包和第二请求数据包,以得到终端发送的登录请求消息;

- 5 根据登录请求消息生成向终端发送的登录应答消息,将登录应答消息拆分为第一应答数据包和第二应答数据包,在第一网络连接上向终端发送第一应答数据包,在第二网络连接上向终端发送第二应答数据包,以完成用户登录。

结合第二方面,在第一种可能的实现方式中,登录应答消息包括登录成功消息或登录失败消息;

- 10 在向终端发送第一应答数据包和第二应答数据包的步骤之后,该方法还包括:

若登录应答消息为登录失败消息,则用户登录失败,断开通过移动数据网络与终端建立的第一网络连接,并且断开通过 WLAN 与终端建立的第二网络连接,以结束用户登录;

- 15 若登录应答消息为登录成功消息,则用户登录成功,断开通过移动数据网络与终端建立的第一网络连接,以完成用户登录;或者,

若登录应答消息为登录成功消息,则用户登录成功,断开通过 WLAN 与终端建立的第二网络连接,以完成用户登录。

本发明实施例第三方面提供了一种终端设备,包括:

- 20 接收单元,用于接收用户发送的服务器登录指令;

处理单元,用于通过移动数据网络与服务器建立第一网络连接,通过 WLAN 与服务器建立第二网络连接;

处理单元还用于,根据接收单元收到的服务器登录指令生成向服务器发送的登录请求消息,将登录请求消息拆分为第一请求数据包和第二请求数据包;

- 25 发送单元,用于在第一网络连接上向服务器发送第一请求数据包,在第二网络连接上向服务器发送第二请求数据包;

接收单元还用于,从第一网络连接上接收服务器发送的第一应答数据包,从第二网络连接上接收服务器发送的第二应答数据包;

处理单元还用于,将接收单元收到的第一应答数据包和第二应答数据包合

并为服务器发送的登录应答消息，以完成用户登录。

结合第三方面，在第一种可能的实现方式中，处理单元还用于：

若接收单元收到的服务器发送的登录应答消息为登录失败消息，则用户登录失败，断开通过移动数据网络与服务器建立的第一网络连接，并且断开通过
5 WLAN 与服务器建立的第二网络连接，以结束用户登录；

若接收单元收到的服务器发送的登录应答消息为登录成功消息，则用户登录成功，断开通过移动数据网络与服务器建立的第一网络连接，以完成用户登录；或者，

若接收单元收到的服务器发送的登录应答消息为登录成功消息，则用户登
10 录成功，断开通过 WLAN 与服务器建立的第二网络连接，以完成用户登录。

结合第三方面，在第二种可能的实现方式中，处理单元具体用于：

在移动数据网络中发起网络注册，若网络注册成功，则通过移动数据网络与服务器建立第一网络连接；

在 WLAN 中发起安全认证，若安全认证成功，则通过 WLAN 与服务器建
15 立第二网络连接；或者，在移动数据网络中发起网络注册，若网络注册成功，则通过 WLAN 与服务器建立第二网络连接。

本发明实施例第四方面提供了一种服务器设备，包括：

处理单元，用于通过移动数据网络与终端建立第一网络连接，通过 WLAN
与终端建立第二网络连接；

20 接收单元，用于从第一网络连接上接收终端发送的第一请求数据包，从第二网络连接上接收终端发送的第二请求数据包；

处理单元还用于，合并接收单元收到的第一请求数据包和第二请求数据包，以得到终端发送的登录请求消息；并且，根据登录请求消息生成向终端发送的登录应答消息，将登录应答消息拆分为第一应答数据包和第二应答数据
25 包；

发送单元，用于在第一网络连接上向终端发送第一应答数据包，在第二网络连接上向终端发送第二应答数据包，以完成用户登录。

结合第四方面，在第一种可能的实现方式中，登录应答消息包括登录成功消息或登录失败消息；

处理单元还用于：

若登录应答消息为登录失败消息，则用户登录失败，断开通过移动数据网络与终端建立的第一网络连接，并且断开通过 WLAN 与终端建立的第二网络连接，以结束用户登录；

5 若登录应答消息为登录成功消息，则用户登录成功，断开通过移动数据网络与终端建立的第一网络连接，以完成用户登录；或者，

若登录应答消息为登录成功消息，则用户登录成功，断开通过 WLAN 与终端建立的第二网络连接，以完成用户登录。

10 本发明实施例提供的技术方案能够通过移动数据网络与服务器建立第一网络连接，通过 WLAN 与服务器建立第二网络连接；将用户发送的服务器登录请求消息拆分为第一请求数据包和第二请求数据包，将第一请求数据包和第二请求数据包分别通过两个网络连接发送到服务器，再分别通过两个网络连接接收第一应答数据包和第二应答数据包并合并为服务器发送的登陆应答消息，以完成用户到服务器的登录。本方案可以避免网络攻击者在网络设备中截获用户

15 的完整通信消息，从而增强用户跟服务器登录方式的安全性。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些

20 些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明实施例一提供的一种双连接安全通讯的网络示意图；

图 2 是本发明实施例一提供的一种双连接安全通讯的方法的流程示意图；

图 3 是本发明实施例二提供的一种双连接安全通讯的方法的流程示意图；

25 图 4 是本发明实施例三提供的一种双连接安全通讯的方法的流程示意图；

图 5 是本发明实施例四提供的一种双连接安全通讯的方法的流程示意图；

图 6 是本发明实施例五提供的一种双连接安全通讯的方法的流程示意图；

图 7 是本发明实施例六提供的一种终端设备的结构示意图；

图 8 是本发明实施例六提供的另一种终端设备的结构示意图；

图 9 是本发明实施例七提供的一种服务器设备的结构示意图；

图 10 是本发明实施例七提供的另一种服务器设备的结构示意图。

5

具体实施方式

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

10 以下分别对每个实施例进行说明。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

本领域的研究人员在研发过程中发现，在目前的网络通讯中，移动终端都是通过一条网络连接与服务器进行通讯，例如通过 WLAN 或通过移动数据网络与服务器进行通讯，网络攻击者较容易在网络设备上通过截获用户与服务器之间的通讯消息对用户与服务器之间的通讯消息进行篡改或伪造，从而使网络通信的安全性降低。

25 本发明实施例提供了一种双连接安全通讯的方法及装置，用于实现移动终端到应用服务器的安全登录，避免网络攻击者在同一个网络中窃取用户的完整通信消息，从而泄露用户信息或篡改用户信息，侵害用户的权益。

本申请将围绕可包括多个设备、组件、模块等的系统来呈现各个方面、实施例或特征。应当理解和明白的是，各个系统可以包括另外的设备、组件、模块等，并且/或者可以并不包括结合附图讨论的所有设备、组件、模块等。此

外, 还可以使用这些方案的组合。

本发明实施例中, “应用服务器”和“服务器”, 两者可以混用, 应当指出的是, 在不强调其区别时, 其所要表达的含义是一致的。

5 本发明实施例描述的网络架构以及业务场景是为了更加清楚的说明本发明实施例的技术方案, 并不构成对于本发明实施例提供的技术方案的限定, 本领域普通技术人员可知, 随着网络架构的演变和新业务场景的出现, 本发明实施例提供的技术方案对于类似的技术问题, 同样适用。

10 本发明实施例依托使用 3GPP 网络与 WLAN 网络的场景进行说明, 应当指出的是, 本发明实施例中的方案还可以应用于使用其他移动通信网络与 WLAN 的场景, 例如 3GPP2 的 HRPD 和 IEEE 的 WiMAX, 相应的名称也可以用其他无线通信网络中的对应功能的名称进行替代。

15 首先参见图 2, 图 2 为本发明实施例一提供的一种双连接安全通讯的方法的流程示意图。本发明实施例一提供的一种双连接安全通讯的方法, 用于移动终端设备, 移动终端设备支持移动数据网络和 WLAN 传输, 可以包括以下步骤:

S101、当接收到用户发送的服务器登录指令后, 通过移动数据网络与服务器建立第一网络连接, 通过无线局域网 (WLAN, Wireless Local Area Network) 与服务器建立第二网络连接。

20 终端在接收到用户发送的服务器登录指令后, 可以分别通过移动数据网络, 例如 3GPP 网络 (WCDMA, LTE 或 TD-SCDMA), 和 WLAN 建立两条连接 (TCP 或 UDP 连接), 即通过移动数据网络与服务器建立第一网络连接, 通过 WLAN 与服务器建立第二网络连接。如图 1 所示, 终端分别通过移动数据网络和 WLAN 与服务器建立第一网络连接和第二网络连接, 终端中设有移动数据网络收发器和移动网络协议栈软件用于处理第一网络连接, 并且设有
25 WLAN 收发器和 WLAN 协议栈软件用于处理第二网络连接。

在 3GPP 组织提出的 3GPP 网络与非 3GPP 网络 (包括 WLAN) 融合的技术中, 支持终端同时在 3GPP 网络和非 3GPP 网络中进行网络注册和认证, 终端可同时通过 3GPP 网络和 WLAN 进行 IP 流传输, 可以由 3GPP 网络提供对 WLAN 用户的鉴权和认证, WLAN 也可以连接到 3GPP 网络的分组数据网关。

但是目前在 3GPP 系统中引入的 3GPP 网络与非 3GPP 网络融合的技术方案中不支持通过 3GPP 网络和非 3GPP 网络与同一个服务器建立网络连接。

通过移动数据网络与应用服务器建立第一网络连接,包括在移动数据网络中网络注册成功之后通过移动数据网络与应用服务器建立第一网络连接;通过
5 WLAN 与服务器建立第二网络连接,包括在通过 WLAN 的安全认证之后通过 WLAN 与服务器建立第二网络连接,或者在通过移动数据网络的安全认证之后通过 WLAN 与服务器建立第二网络连接。第一网络连接和第二网络连接可以是 TCP/IP 连接或 UDP/IP 连接,用发送端口号、接收端口号、源 IP 地址和目标 IP 地址标识。

10 在具体实现中,终端在移动数据网络中注册成功后,才能通过移动数据网络与应用服务器建立第一网络连接,终端通过 WLAN 的安全认证之后,才能通过 WLAN 与服务器建立第二网络连接。举例来说,在 3GPP 系统中,终端开机后即可发起分组网络注册,网络注册的过程包括鉴权过程、安全激活过程和建立分组数据网络连接等,当终端在 LTE 网络中完成分组网络注册后才
15 可以与应用服务器建立第一网络连接(TCP 或 UDP 连接)。又举例来说,WLAN 中的终端用户首先要通过 WLAN 的本地安全认证,之后通过 WLAN 与应用服务器建立第二网络连接(TCP 或 UDP 连接);在一些 3GPP 网络和 WLAN 网络融合的场景中,WLAN 中的终端通过 3GPP 网络服务器进行安全认证,通过 3GPP 网络的安全认证的终端才可以通过 WLAN 与应用服务器建立第二网络
20 连接。

S102、根据服务器登录指令生成向服务器发送的登录请求消息,将登录请求消息拆分为第一请求数据包和第二请求数据包,在第一网络连接上向服务器发送第一请求数据包,在第二网络连接上向服务器发送第二请求数据包。

在通过移动数据网络与服务器建立第一网络连接,通过 WLAN 与服务器
25 建立第二网络连接之后,终端可以根据用户的服务器登录指令,生成用户的服务器登录请求消息,用户的服务器登录请求消息中包含用户的账号和密码信息。由于第一网络连接和第二网络连接是不同的传输连接,通过第一网络连接和通过第二网络连接传输的数据可经过不同的网络设备,为了避免用户的登录请求消息被网络攻击者在网络设备(如网关或路由器)处截获,终端可以将用

户的登录请求消息拆分成两个数据包,分别在建立的第一网络连接和第二网络连接上发送,具体来说,将用户的服务器登录请求消息拆分为第一请求数据包和第二请求数据包,在第一网络连接上向服务器发送第一请求数据包,在第二网络连接上向服务器发送第二请求数据包。

- 5 S103、从第一网络连接上接收服务器发送的第一应答数据包,从第二网络连接上接收服务器发送的第二应答数据包,将第一应答数据包和第二应答数据包合并为服务器发送的登录应答消息,以完成用户登录。

- 当服务器从第一网络连接上接收到终端发送的第一请求数据包,从第二网络连接上接收到终端发送的第二请求数据包之后,将第一请求数据包和第二请求数据包进行合并,以得到终端发送的登录请求消息。
- 10

- 服务器根据终端发送的登录请求消息生成的登录应答消息包括登录成功消息和登录失败消息。当服务器接收到登录请求消息后,先验证该用户是否为有效用户,若为无效用户(例如用户账号不存在或密码错误),服务器可直接断开与终端通过移动数据网络建立的第一网络连接和断开与终端通过 WLAN 建立的第二网络连接。当终端接收到服务器发送的第一网络连接断开请求时,或在终端发送第一请求数据包和第二请求数据包之后的时间超过指定时间后,断开第一网路连接,当终端接收到服务器发送的第二网络连接断开请求时,或在发送第一请求数据包和第二请求数据包之后的时间超过指定时间后,断开第二网路连接;只要断开两条网络连接中的一条,即结束用户登录。若服务器验证用户为有效用户,可根据用户信息或其他条件,如服务器的连接总数、处理能力或网速,来生成登录应答消息,包括登录成功消息或登录失败消息,例如,若用户优先级较低并且服务器的连接总数较多的情况下服务器可能为用户生成登录失败消息。
- 15
- 20

- 与终端发送登录请求消息的方法相类似,为了防止网络攻击者从网络中截获用户消息,服务器将所生成的登录应答消息拆分为第一应答数据包和第二应答数据包,分别在第一网络连接上向终端发送第一应答数据包,在第二网络连接上向终端发送第二应答数据包。服务器发送之后终端从第一网络连接上可接收服务器发送的第一应答数据包,在第二网络连接上可接收服务器发送的第二应答数据包。
- 25

终端获取第一应答数据包和第二应答数据之后,可将两者合并为服务器发送的登录应答消息。在一些可行的实施方式中,若登录应答消息为登录失败消息,则用户登录失败,终端断开通过移动数据网络与服务器建立的第一网络连接,并且断开通过 WLAN 与服务器建立的第二网络连接,以结束用户登录。

- 5 所述断开可以是终端主动发起的连接断开,如终端发起的 TCP 连接的关闭或终端自动断开 UDP 连接,也可以是服务器在发送了登录失败消息后发起的连接断开,如服务器发起的 TCP 连接的关闭;所述断开可以是接收到登录失败应答消息后立即断开,也可以是经过多次登录尝试后依然失败的情况下的断开。若服务器发送的登录应答消息为登录成功消息,则用户登录成功,终端可以断开通过移动数据网络与服务器建立的第一网络连接,或者,断开通过
- 10 WLAN 与服务器建立的第二网络连接,又或者,保持第一网络连接和第二网络连接不断开,当终端完成用户登录后,可以使用未断开的网络连接传输业务数据。终端接收到的登录成功消息,可能是多次用户登录尝试中的一次的成功消息。所述断开可以是终端主动发起的连接断开,如终端发起的 TCP 连接的关闭或终端自动断开 UDP 连接,也可以是服务器在发送了登录失败消息后发起的连接断开,如服务器发起的 TCP 连接的关闭。
- 15

可见,本发明实施例提供的技术方案能够使终端通过移动数据网络与服务器建立第一网络连接,通过 WLAN 与服务器建立第二网络连接;将终端发送给服务器的登录请求消息拆分为第一请求数据包和第二请求数据包,将第一请求数据包和第二请求数据包分别通过两个网络连接发送到服务器,再分别通过

20 两个网络连接接收第一应答数据包和第二应答数据包并合并为服务器发送给终端的登录应答消息,以完成用户到服务器的安全登录。本方案可以避免网络攻击者在网络设备中截获用户的完整通信消息,从而增强用户跟服务器登录方式的安全性。

- 25 本发明实施例二提供了一种双连接安全通讯的方法,用于移动终端设备,参见图 3,图 3 为本发明实施例二提供的一种双连接安全通讯的方法的流程示意图。其中,如图 3 所示,本方法可包括以下步骤:

S201、当接收到用户发送的服务器登录指令后,通过移动数据网络与服务器建立第一网络连接,通过 WLAN 与服务器建立第二网络连接。

终端在接收到用户发送的服务器登录指令后，可以分别通过移动数据网络，例如 3GPP 网络（WCDMA，LTE 或 TD-SCDMA），和 WLAN 建立两条连接（TCP 或 UDP 连接），即通过移动数据网络与服务器建立第一网络连接，通过无线局域网 WLAN 与服务器建立第二网络连接。

5 关于步骤 S201 的具体描述可参见上述实施例一的步骤 S101，此处不再赘述。

S202、根据服务器登录指令生成向服务器发送的登录请求消息，将登录请求消息拆分为第一请求数据包和第二请求数据包，在第一网络连接上向服务器发送第一请求数据包，在第二网络连接上向服务器发送第二请求数据包。

10 关于步骤 S202 的具体描述可参见上述实施例一的步骤 S102，此处不再赘述。

S203、从第一网络连接上接收服务器发送的第一应答数据包，从第二网络连接上接收服务器发送的第二应答数据包，将第一应答数据包和第二应答数据包合并为服务器发送的登录应答消息。

15 当服务器从第一网络连接上接收到终端发送的第一请求数据包，从第二网络连接上接收到终端发送的第二请求数据包之后，将第一请求数据包和第二请求数据包进行合并，以得到终端发送的登录请求消息。之后服务器根据登录请求消息生成登录应答消息，与终端发送登录请求消息的方法相类似，为了防止网络攻击者从网络中截获用户消息，服务器将所生成的登录应答消息拆分为
20 第一应答数据包和第二应答数据包，分别在第一网络连接上向终端发送第一应答数据包，在第二网络连接上向终端发送第二应答数据包。服务器发送之后终端从第一网络连接上可接收服务器发送的第一应答数据包，在第二网络连接上可接收服务器发送的第二应答数据包。

25 终端获取第一应答数据包和第二应答数据之后，可将两者合并为服务器发送的登录应答消息，以完成用户登录过程。

S204、判断登录应答消息是登录成功消息还是登录失败消息。

终端将第一应答数据包和第二应答数据包合并为登录应答消息，登录应答消息包括登录成功消息和登录失败消息，若为登录成功消息，则用户登录服务器成功，若为登录失败消息，则用户登录服务器失败。

S205、若登录应答消息为登录失败消息，则用户登录失败，断开通过移动数据网络与服务器建立的第一网络连接，并且断开通过 WLAN 与服务器建立的第二网络连接，以结束用户登录。

5 若登录应答消息为登录失败消息，终端断开通过移动数据网络与服务器建立的第一网络连接，并且断开通过 WLAN 与服务器建立的第二网络连接。所述断开可以是终端主动发起的连接断开，如终端发起的 TCP 连接的关闭或终端自动断开 UDP 连接，也可以是服务器在发送了登录失败消息后发起的连接断开，如服务器发起的 TCP 连接的关闭；所述断开可以是终端接收到登录失败应答消息后立即断开，也可以是经过多次登录尝试时每次终端收到的都是登录失败消息之后的断开。

10

S206、若登录应答消息为登录成功消息，则用户登录成功，断开通过移动数据网络与服务器建立的第一网络连接，或者断开通过 WLAN 与服务器建立的第二网络连接，以完成用户登录。

15 若登录应答消息为登录成功消息，断开通过移动数据网络与服务器建立的第一网络连接，或者，断开通过 WLAN 与服务器建立的第二网络连接，或者，保持第一网络连接和第二网络连接不断开，当终端完成用户登录后，可以使用未断开的网络连接传输业务数据。终端接收到的登录成功消息，可能是多次登录尝试中的一次登录成功消息。所述断开可以是终端主动发起的连接断开，如终端发起的 TCP 连接的关闭或终端自动断开 UDP 连接，也可以是服务器在发送了登录失败消息后发起的连接断开，如服务器发起的 TCP 连接的关闭。

20

可见，本发明实施例提供的技术方案能够使终端通过移动数据网络与服务器建立第一网络连接，通过 WLAN 与服务器建立第二网络连接；将终端发送给服务器的登录请求消息拆分为第一请求数据包和第二请求数据包，将第一请求数据包和第二请求数据包分别通过两个网络连接发送到服务器，再分别通过两个网络连接接收第一应答数据包和第二应答数据包并合并为服务器发送给终端的登录应答消息，根据用户登录是否成功断开或保持网络连接，从而达到安全登录的目的。本方案可以避免网络攻击者在网络设备中截获用户的完整通信消息，从而增强用户跟服务器登录方式的安全性。

25

本发明实施例三提供了一种双连接安全通讯的方法，用于移动终端设备，参见图 4，图 4 为本发明实施例三提供的一种双连接安全通讯的方法的流程示意图。其中，如图 4 所示，本方法可包括以下步骤：

5 S301、当接收到用户发送的服务器登录指令后，通过移动数据网络与服务器建立第一网络连接，通过 WLAN 与服务器建立第二网络连接。

步骤 S301 的具体实施可参考实施例一的步骤 S101，此处不再赘述。

S302、根据服务器登录指令生成向服务器发送的登录请求消息，将登录请求消息拆分为第一请求数据包和第二请求数据包，在第一网络连接上向服务器发送第一请求数据包，在第二网络连接上向服务器发送第二请求数据包。

10 步骤 S302 的具体实施可参考实施例一的步骤 S102，此处不再赘述。

S303、当终端接收到服务器发送的第一网络连接断开请求时，或在终端发送第一请求数据包和第二请求数据包之后的时间超过指定时间后，断开第一网路连接；当终端接收到服务器发送的第二网络连接断开请求时，或在发送第一请求数据包和第二请求数据包之后的时间超过指定时间后，断开第二网路连
15 接；结束用户登录。

当服务器从第一网络连接上接收到终端发送的第一请求数据包，从第二网络连接上接收到终端发送的第二请求数据包之后，将第一请求数据包和第二请求数据包进行合并，以得到终端发送给服务器的登录请求消息。

当服务器接收到登录请求消息后，先验证该用户是否为有效用户，若为无效用户（例如用户账号不存在或密码错误），服务器可直接断开与终端通过移动数据网络建立的第一网络连接和断开与终端通过 WLAN 建立的第二网络连接，服务器也可向终端发送无效用户指示信息之后再断开网络连接。若第一网络连接或第二网络连接为 TCP 连接，则服务器主动发起的 TCP 连接的关闭，若第一网络连接或第二网络连接为 UDP 连接，服务器自行断开 UDP 连接。当
20 终端接收到服务器的 TCP 连接关闭请求后，断开 TCP 连接，或者终端在发送登录请求消息超时后自行断开 UDP 连接，终端在断开连接之前可能收到服务器发送的无效用户指示信息。

当终端接收到服务器发送的第一网络连接断开请求时断开第一网络连接，或在终端发送第一请求数据包和第二请求数据包之后的时间超过指定时间后

断开第一网路连接；当终端接收到服务器发送的第二网络连接断开请求时断开第二网络连接，或在发送第一请求数据包和第二请求数据包之后的时间超过指定时间后断开第二网路连接；只要断开两条网络连接中的一条，即结束用户登录。

- 5 可见，本发明实施例提供的技术方案能够使终端通过移动数据网络与服务器建立第一网络连接，通过 WLAN 与服务器建立第二网络连接；将终端发送给服务器的登录请求消息拆分为第一请求数据包和第二请求数据包，将第一请求数据包和第二请求数据包分别通过两个连接发送到服务器，在接收到服务器发送的登录应答消息前可以断开网络连接，从而达到安全登录的目的。本方案
- 10 可以避免网络攻击者在网络设备中截获用户的完整通信消息，从而增强用户跟服务器登录方式的安全性。

本发明实施例四提供了一种双连接安全通讯的方法，用于服务器，参见图 5，图 5 为本发明实施例四提供的一种双连接安全通讯的方法的流程示意图。其中，如图 5 所示，本方法可包括以下步骤：

- 15 S401、通过移动数据网络与终端建立第一网络连接，通过 WLAN 与终端建立第二网络连接。

终端在接收到用户的服务器登录指令后，可以分别通过移动数据网络，例如 3GPP 网络（WCDMA，LTE 或 TD-SCDMA），和 WLAN 建立两条连接（TCP 或 UDP 连接），即通过移动数据网络与服务器建立第一网络连接，通过无线局

20 域网 WLAN 与服务器建立第二网络连接。

在 3GPP 组织提出的 3GPP 网络与非 3GPP 网络（包括 WLAN）融合的技术中，支持终端同时在 3GPP 网络和非 3GPP 网络中进行网络注册和认证，终端可同时通过 3GPP 网络和 WLAN 进行 IP 流传输，可以由 3GPP 网络提供对 WLAN 用户的鉴权和认证，WLAN 也可以连接到 3GPP 网络的分组数据网关。

25 但是目前在 3GPP 系统中引入的 3GPP 网络与非 3GPP 网络融合的技术方案中不支持通过 3GPP 网络和非 3GPP 网络与同一个服务器建立网络连接。

服务器通过移动数据网络与终端建立第一网络连接，包括终端在移动数据网络中注册成功之后通过移动数据网络与终端建立第一网络连接；服务器通过 WLAN 与终端建立第二网络连接，包括在终端通过 WLAN 的安全认证之后通

过 WLAN 与终端建立第二网络连接, 或者在移动数据网络中发起网络注册, 若网络注册成功, 则通过 WLAN 与所述服务器建立所述第二网络连接。第一网络连接和第二网络连接可以是 TCP/IP 连接或 UDP/IP 连接, 用发送端口号、接收端口号、源 IP 地址和目标 IP 地址标识。

5 在具体实现中, 终端在移动数据网络中注册成功后, 才能通过移动数据网络与应用服务器建立第一网络连接, 因此终端通过 WLAN 的安全认证之后, 服务器才能通过 WLAN 与终端建立第二网络连接。举例来说, 在 3GPP 系统中, 终端开机后即可发起分组网络注册, 网络注册的过程包括鉴权过程、安全激活过程和建立分组数据网络连接等, 当终端在 LTE 网络中完成分组网络注册后才可以与应用服务器建立第一网络连接 (TCP 或 UDP 连接)。又举例来说, WLAN 中的终端用户首先要通过 WLAN 的本地安全认证, 然后通过 WLAN 与应用服务器建立第二网络连接 (TCP 或 UDP 连接); 在一些 3GPP 网络和 WLAN 网络融合的场景中, WLAN 中的终端通过 3GPP 网络服务器进行安全认证, 通过 3GPP 网络的安全认证的终端才可以通过 WLAN 与应用服务器建立第二网络连接。

15 S402、从第一网络连接上接收终端发送的第一请求数据包, 从第二网络连接上接收终端发送的第二请求数据包, 合并第一请求数据包和第二请求数据包, 以得到终端发送的登录请求消息。

20 在服务器通过移动数据网络与服务器建立第一网络连接, 通过 WLAN 与服务器建立第二网络连接之后, 终端可以根据服务器登录指令, 生成用户的服务器登录请求消息, 用户的服务器登录请求消息中包含用户的账号和密码信息。由于第一网络连接和第二网络连接是不同的传输连接, 通过第一网络连接和通过第二网络连接传输的数据可经过不同的网络设备, 为了避免用户的登录请求消息被网络攻击者在网络设备 (如网关或路由器) 处截获, 终端可以将用户的登录请求消息拆分成两个数据包, 分别在建立的第一网络连接和第二网络连接上发送, 具体来说, 将用户的服务器登录请求消息拆分为第一请求数据包和第二请求数据包, 在第一网络连接上向服务器发送第一请求数据包, 在第二网络连接上向服务器发送第二请求数据包。

25 当服务器从第一网络连接上接收到终端发送的第一请求数据包, 从第二

网络连接上接收到终端发送的第二请求数据包之后,将第一请求数据包和第二请求数据包进行合并,以得到终端发送的登录请求消息。

5 S403、根据登录请求消息生成向终端发送的登录应答消息,将登录应答消息拆分为第一应答数据包和第二应答数据包,在第一网络连接上向终端发送第一应答数据包,在第二网络连接上向终端发送第二应答数据包,以完成用户登录。

10 当服务器将第一请求数据包和第二请求数据包进行合并,得到终端发送的登录请求消息后,先验证该用户是否为有效用户,若为无效用户(例如用户账号不存在或密码错误),服务器可直接断开与终端通过移动数据网络建立的第一网络连接和断开与终端通过 WLAN 建立的第二网络连接;服务器也可能由于其他异常原因发起第一网络连接的断开或发起第二网络连接的断开,也可能不向终端发送登录应答消息并自行断开第一网络连接或第二网络连接,此时,只要断开两条网络连接中的一条,即结束用户登录。若服务器验证用户为有效用户,可根据用户信息或其他条件,如服务器的连接总数、处理能力或网速,15 生成登录应答消息,包括登录成功消息或登录失败消息,例如,若用户优先级较低并且服务器的连接总数较多的情况下服务器可能为用户生成登录失败消息。

与终端发送服务器登录请求的方法相类似,为了防止网络攻击者从网络中截获用户消息,服务器将所生成的登录应答消息拆分为第一应答数据包和第二20 应答数据包,分别在第一网络连接上向终端发送第一应答数据包,在第二网络连接上向终端发送第二应答数据包。服务器发送之后终端从第一网络连接上可接收服务器发送的第一应答数据包,在第二网络连接上可接收服务器发送的第二应答数据包。

25 在一些可行的实施方式中,若登录应答消息为服务器登录失败消息,服务器断开通过移动数据网络与服务器建立的第一网络连接,并且断开通过 WLAN 与服务器建立的第二网络连接。所述断开可以是服务器主动发起的连接断开,如服务发起的 TCP 连接的关闭或服务器自动断开 UDP 连接,也可以是终端在接收到登录失败消息后发起的连接断开,如终端发起的 TCP 连接的关闭;所述断开可以是服务器首次发送完登录失败应答消息后立即断开,也可

以是在服务器接收到多次用户登录请求消息时每次都发送用户登录失败消息后的断开。若登录应答消息为登录成功消息，服务器断开通过移动数据网络与服务器建立的第一网络连接，或者，断开通过 WLAN 与服务器建立的第二网络连接，或者，保持第一网络连接和第二网络连接不断开，当服务器发送完登录成功消息后，可以通过不断开的网络连接传输业务数据。服务器发送的登录成功消息，可能是多次登录尝试中的一次登录成功消息。所述断开可以是服务器主动发起的连接断开，如服务器发起的 TCP 连接的关闭或服务器自动断开 UDP 连接，也可以是终端在接收到登录失败消息后发起的连接断开，如终端发起的 TCP 连接的关闭。

10 可见，本发明实施例提供的技术方案能够使服务器通过移动数据网络与终端建立第一网络连接，通过 WLAN 与终端建立第二网络连接，服务器分别通过两个网络连接接收第一请求数据包和第二请求数据包并合并为终端发送给服务器的登录请求消息，将服务器发送给终端的登录应答请求消息拆分为第一应答数据包和第二应答数据包，分别通过两个网络连接发送到终端，以完成用
15 户到服务器的安全登录。本方案可以避免网络攻击者在网络设备中截获用户的完整通信消息，从而增强用户跟服务器登录方式的安全性。

S501、通过移动数据网络与终端建立第一网络连接，通过 WLAN 与终端建立第二网络连接。

20 终端在接收到用户的服务器登录指令后，可以分别通过移动数据网络，例如 3GPP 网络(WCDMA, LTE 或 TD-SCDMA)，和 WLAN 建立两条连接(TCP 或 UDP 连接)，即通过移动数据网络与服务器建立第一网络连接，通过无线局域网 WLAN 与服务器建立第二网络连接。

在 3GPP 组织提出的移动网络与 WLAN 融合的技术中，支持终端通过 3GPP 网络和 WLAN 建立两条分组数据网络连接，同时通过 3GPP 网络和
25 WLAN 进行 IP 流传输，可以由 3GPP 网络提供对 WLAN 用户的鉴权和认证，WLAN 也可以连接到 3GPP 网络的分组数据网关。

关于步骤 S501 的具体描述可参见上述实施例四的步骤 S401，此处不再赘述。

S502、从第一网络连接上接收终端发送的第一请求数据包，从第二网络连

接上接收终端发送的第二请求数据包，合并第一请求数据包和第二请求数据包，以得到终端发送的登录请求消息。

关于步骤 S502 的具体描述可参见上述实施例四的步骤 S402，此处不再赘述。

5 S503、根据登录请求消息判断用户是否为无效用户。

当服务器合并第一请求数据包和第二请求数据包，得到终端发送的登录请求消息，该登录请求消息中包含用户的账户和密码等信息，先根据该登陆请求消息验证该用户是否为有效用户。

10 S504、若验证该用户为无效用户，断开通过移动数据网络与终端建立的第一网络连接，并且断开通过 WLAN 与终端建立的第二网络连接，以结束用户登录。

若验证为无效用户（例如用户账号不存在或密码错误），服务器可直接断开与终端通过移动数据网络建立的第一网络连接并断开与终端通过 WLAN 建立的第二网络连接，服务器也可向终端发送无效用户指示信息之后再断开网络连接。若第一网络连接或第二网络连接为 TCP 连接，则服务器主动发起的 TCP 连接的关闭，若第一网络连接或第二网络连接为 UDP 连接，服务器自行断开 UDP 连接。当终端接收到服务器的 TCP 连接关闭请求后，断开 TCP 连接，或者终端在向服务器发送登录请求消息之后的时间超过指定时间阈值后，自行断开 UDP 连接，终端在断开连接之前可能收到服务器发送的无效用户指示信息。

20 S505、若验证该用户不为无效用户，根据服务器登录请求消息生成向终端发送的应答消息，将登录应答消息拆分为第一应答数据包和第二应答数据包，在第一网络连接上向终端发送第一应答数据包，在第二网络连接上向终端发送第二应答数据包。

当验证该用户不为无效用户，服务器可根据用户信息或其他条件，如服务器的连接总数、处理能力或网速，生成登录应答消息。登录应答消息包括登录成功消息或登录失败消息，例如，若用户优先级较低并且服务器的连接总数较多的情况下服务器可能为用户生成登录失败消息。

与终端发送服务器登录请求的方法相类似，为了防止网络攻击者从网络中截获用户消息，服务器将所生成的登录应答消息拆分为第一应答数据包和第二

应答数据包，分别在第一网络连接上向终端发送第一应答数据包，在第二网络连接上向终端发送第二应答数据包。服务器发送之后终端从第一网络连接上可接收服务器发送的第一应答数据包，在第二网络连接上可接收服务器发送的第二应答数据包。

5 S506、判断登录应答消息是登录成功消息还是登录失败消息。

当服务器在第一网络连接上向终端发送第一应答数据包，在第二网络连接上向终端发送第二应答数据包之后，判断登录应答消息是登录成功消息还是登录失败消息。

10 S507、若登录应答消息为登录失败消息，则用户登录失败，断开通过移动数据网络与终端建立的第一网络连接，并且断开通过 WLAN 与终端建立的第二网络连接，以结束用户登录。

若登录应答消息为登录失败消息，则用户登录失败，服务器断开通过移动数据网络与终端建立的第一网络连接，并且断开通过 WLAN 与终端建立的第二网络连接，以结束用户登录。所述断开可以是服务器主动发起的连接断开，如服务器发起的 TCP 连接的关闭或终端自动断开 UDP 连接，也可以是终端在接收到服务器发送的登录失败消息后发起的连接断开，如终端发起的 TCP 连接的关闭；所述断开可以是服务器发送完登录失败应答消息后立即断开，也可以是终端经过多次登录尝试时每次服务器向终端发送的都是登录失败消息之后的断开。

20 S508、若登录应答消息为登录成功消息，则用户登录成功，断开通过移动数据网络与终端建立的第一网络连接，或者断开通过 WLAN 与终端建立的第二网络连接，以完成用户登录。

若登录应答消息为登录成功消息，则用户登录成功，服务器断开通过移动数据网络与终端建立的第一网络连接，或者，断开通过 WLAN 与终端建立的第二网络连接，或者，保持第一网络连接和第二网络连接不断开，当服务器发送完用户的登录成功消息后，可以通过未断开的网络连接传输业务数据。服务器发送的登录成功消息，可能是终端多次登录尝试中的一次中服务器发送的登录成功消息。所述断开可以是服务器主动发起的连接断开，如服务器发起的 TCP 连接的关闭或服务器自动断开 UDP 连接，也可以是终端在接收到登录失

败消息后发起的连接断开，如终端发起的 TCP 连接的关闭。

可见，本发明实施例提供的技术方案能够使服务器通过移动数据网络与终端建立第一网络连接，通过 WLAN 与终端建立第二网络连接，服务器分别通过两个网络连接接收第一请求数据包和第二请求数据包并合并为终端发送的登录请求消息，服务器将向终端发送的登录应答请求消息拆分为第一应答数据包和第二应答数据包，分别通过两个网络连接发送到终端，根据是否为无效用户和用户登录是否成功断开或保持网络连接，从而达到用户安全登录的目的。本方案可以避免网络攻击者在网络设备中截获用户的完整通信消息，从而增强用户跟服务器登录方式的安全性。

10 本发明实施例六提供了一种终端设备，用于实现本发明提出的一种双连接安全通讯的方法。参见图 7，所述设备 a00 可包括接收单元 a10、处理单元 a20 和发送单元 a30。

接收单元 a10，用于接收用户发送的服务器登录指令；

15 处理单元 a20，用于通过移动数据网络与服务器建立第一网络连接，通过 WLAN 与服务器建立第二网络连接；

处理单元 a20 还用于，根据接收单元 a10 收到的服务器登录指令生成向服务器发送的登录请求消息，将登录请求消息拆分为第一请求数据包和第二请求数据包；

20 发送单元 a30，用于在第一网络连接上向服务器发送第一请求数据包，在第二网络连接上向服务器发送第二请求数据包；

接收单元 a10 还用于，从第一网络连接上接收服务器发送的第一应答数据包，从第二网络连接上接收服务器发送的第二应答数据包；

处理单元 a20 还用于，将接收单元收到的第一应答数据包和第二应答数据包合并为服务器发送的登录应答消息，以完成用户登录。

25 在一些可行的实施方式中，处理单元 a20 还用于：

若接收单元 a10 收到的服务器发送的登录应答消息为登录失败消息，则用户登录失败，断开通过移动数据网络与服务器建立的第一网络连接，并且断开通过 WLAN 与所述服务器建立的第二网络连接，以结束用户登录；

若接收单元 a10 收到的服务器发送的登录应答消息为登录成功消息，则用

户登录成功，断开通过移动数据网络与所述服务器建立的第一网络连接，以完成用户登录；或者，

若接收单元 a10 收到的服务器发送的登录应答消息为登录成功消息，则用户登录成功，断开所述通过 WLAN 与所述服务器建立的第二网络连接，以完成用户登录。

在一些可行的实施例中，处理单元 a20 具体用于：

在移动数据网络中发起网络注册，若网络注册成功，则通过移动数据网络与服务器建立所述第一网络连接；

在 WLAN 中发起安全认证，若安全认证成功，则通过 WLAN 与服务器建立第二网络连接；或者，在移动数据网络中发起网络注册，若网络注册成功，则通过 WLAN 与服务器建立第二网络连接。

可见，本发明实施例提供的技术方案可以避免网络攻击者在网络设备中截获用户的完整通信消息，从而增强用户跟服务器登录方式的安全性。

本发明实施例六提供了另一种终端设备，用于实现本发明提出的一种双连接安全通讯的方法。参见图 8，该设备 b00 包括处理器 b10、存储器 b20、总线系统 b30、接收器 b40 和发送器 b50。其中，处理器 b10、存储器 b20、接收器 b40 和发送器 b50 通过总线系统 b30 相连，该存储器 b20 用于存储指令，该处理器 b10 用于执行该存储器 b20 存储的指令，以控制接收器 b40 接收信号，并控制发送器 b50 发送信号，完成上述移动支付方法中的步骤。其中，接收器 b40 和发送器 b50 可以为相同或者不同的物理实体。

该设备 b00 完成的方法步骤至少可以包括：

当接收到用户发送的服务器登录指令后，通过移动数据网络与服务器建立第一网络连接，通过无线局域网 WLAN 与服务器建立第二网络连接；

根据服务器登录指令生成向服务器发送的登录请求消息，将登录请求消息拆分为第一请求数据包和第二请求数据包，在第一网络连接上向服务器发送第一请求数据包，在第二网络连接上向服务器发送第二请求数据包；

从第一网络连接上接收服务器发送的第一应答数据包，从第二网络连接上接收服务器发送的第二应答数据包，将第一应答数据包和第二应答数据包合并为服务器发送的登录应答消息，以完成用户登录。

上述终端设备所涉及的与本发明实施例提供的技术方案相关的概念，解释和详细说明及其他步骤请参见前述方法或实施例中关于这些内容的描述，此处不做赘述。

本发明实施例七提供了一种服务器设备，用于实现本发明提出的一种双连接安全通讯的方法。参见图 9，所述设备 c00 可包括处理单元 c10、接收单元 c20 和发送单元 c30。

处理单元 c10，用于通过移动数据网络与终端建立第一网络连接，通过 WLAN 与终端建立第二网络连接；

接收单元 c20，用于从第一网络连接上接收终端发送的第一请求数据包，
10 从第二网络连接上接收终端发送的第二请求数据包；

处理单元 c10 还用于，合并接收单元 c20 收到的第一请求数据包和第二请求数据包，以得到终端发送的登录请求消息；并且，根据登录请求消息生成向终端发送的登录应答消息，将登录应答消息拆分为第一应答数据包和第二应答数据包；

15 发送单元 c30，用于在第一网络连接上向终端发送第一应答数据包，在第二网络连接上向终端发送第二应答数据包，以完成用户登录。

登录应答消息包括登录成功消息或登录失败消息，在一些可行的实施方式中，处理单元 c10 还用于：

若登录应答消息为登录失败消息，则用户登录失败，断开通过移动数据网络与终端建立的第一网络连接，并且断开通过 WLAN 与终端建立的第二网络连接，以结束用户登录；
20

若登录应答消息为登录成功消息，则用户登录成功，断开通过移动数据网络与终端建立的第一网络连接，以完成用户登录；或者，

若登录应答消息为登录成功消息，则用户登录成功，断开通过 WLAN 与
25 终端建立的第二网络连接，以完成用户登录。

可见，本发明实施例提供的技术方案能够避免网络攻击者在网络设备中截获用户的完整通信消息，从而增强用户跟服务器登录方式的安全性。

本发明实施例七提供了另一种服务器设备，用于实现本发明提出的一种双连接安全通讯的方法。参见图 10，该设备 d00 包括处理器 d10、存储器 d20、

总线系统 d30、接收器 d40 和发送器 d50。其中，处理器 d10、存储器 d20、接收器 d40 和发送器 d50 通过总线系统 d30 相连，该存储器 d20 用于存储指令，该处理器 d10 用于执行该存储器 d20 存储的指令，以控制接收器 d40 接收信号，并控制发送器 d50 发送信号，完成上述移动支付方法中的步骤。其中，接收器 d40 和发送器 d50 可以为相同或者不同的物理实体。

该设备 d00 完成的方法步骤至少可以包括：

通过移动数据网络与终端建立第一网络连接，通过 WLAN 与终端建立第二网络连接；

从第一网络连接上接收终端发送的第一请求数据包，从第二网络连接上接收终端发送的第二请求数据包，合并第一请求数据包和第二请求数据包，以得到终端发送的登录请求消息；

根据登录请求消息生成向终端发送的登录应答消息，将登录应答消息拆分为第一应答数据包和第二应答数据包，在第一网络连接上向终端发送第一应答数据包，在第二网络连接上向终端发送第二应答数据包，以完成用户登录。

上述服务器设备所涉及的与本发明实施例提供的技术方案相关的概念，解释和详细说明及其他步骤请参见前述方法或实施例中关于这些内容的描述，此处不做赘述。

本领域普通技术人员将会理解，本发明的各个方面、或各个方面的可能实现方式可以被具体实施为系统、方法或者计算机程序产品。此外，本发明的各个方面、或各个方面的可能实现方式可以采用计算机程序产品的形式，计算机程序产品是指存储在计算机可读介质中的计算机可读程序代码。

计算机可读介质可以是计算机可读数据介质或者计算机可读存储介质。计算机可读存储介质包含但不限于电子、磁性、光学、电磁、红外或半导体系统、设备或者装置，或者前述的任意适当组合，如随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、光纤、便携式只读存储器 (CD-ROM)。

计算机中的处理器读取存储在计算机可读介质中的计算机可读程序代码，使得处理器能够执行在流程图中每个步骤、或各步骤的组合中规定的功能动作；生成实施在框图的每一块、或各块的组合中规定的功能动作的装置。

计算机可读程序代码可以完全在用户的计算机上执行、部分在用户的计算机上执行、作为单独的软件包、部分在用户的本地计算机上并且部分在远程计算机上，或者完全在远程计算机或者服务器上执行。也应该注意，在某些替代实施方案中，在流程图中各步骤、或框图中各块所注明的功能可能不按图中注

5 明的顺序发生。例如，依赖于所涉及的功能，接连示出的两个步骤、或两个块实际上可能被大致同时执行，或者这些块有时候可能被以相反顺序执行。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置，可通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，所述功能单元的划分，仅仅为一种逻辑功能划分，具体实现时可能有其他的划分方式，例

10 如多个单元可以结合到同一个子系统或模块中实现，或将一个单元拆分成几个单元实现，或一些实现特征可以忽略或不执行。

以上对本发明实施例公开的一种双连接安全通讯的方法、装置及设备进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于

15 本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权利要求

1、一种双连接安全通讯的方法，用于终端设备，其特征在于，所述方法包括：

- 5 当接收到用户发送的服务器登录指令后，通过移动数据网络与所述服务器建立第一网络连接，通过无线局域网 WLAN 与所述服务器建立第二网络连接；
 根据所述服务器登录指令生成向服务器发送的登录请求消息，将所述登录请求消息拆分为第一请求数据包和第二请求数据包，在所述第一网络连接上向所述服务器发送所述第一请求数据包，在所述第二网络连接上向所述服务器发送第二请求数据包；
- 10

 从所述第一网络连接上接收所述服务器发送的第一应答数据包，从所述第二网络连接上接收所述服务器发送的第二应答数据包，将所述第一应答数据包和所述第二应答数据包合并为所述服务器发送的登录应答消息，以完成用户登录。

- 15 2、根据权利要求 1 所述的方法，其特征在于，所述登录应答消息包括登录成功消息或登录失败消息；

 在所述将所述第一应答数据包和所述第二应答数据包合并为所述服务器发送的登录应答消息之后，所述方法还包括：

- 若所述服务器发送的登录应答消息为登录失败消息，则用户登录失败，断
20 开所述通过移动数据网络与所述服务器建立的第一网络连接，并且断开所述通过 WLAN 与所述服务器建立的第二网络连接，以结束用户登录；

 若所述服务器发送的登录应答消息为登录成功消息，则用户登录成功，断开所述通过移动数据网络与所述服务器建立的第一网络连接，以完成用户登录；或者，

- 25 若所述服务器发送的登录应答消息为登录成功消息，则用户登录成功，断开所述通过 WLAN 与所述服务器建立的第二网络连接，以完成用户登录。

3、根据权利要求 1 所述的方法，其特征在于，在所述通过移动数据网络与所述服务器建立第一网络连接之前，所述方法还包括：

 在移动数据网络中发起网络注册，若网络注册成功，则通过所述移动数据

网络与所述服务器建立所述第一网络连接;

在所述通过 WLAN 与所述服务器建立第二网络连接之前, 所述方法还包括:

5 在 WLAN 中发起安全认证, 若安全认证成功, 则通过 WLAN 与所述服务器建立所述第二网络连接; 或者, 在移动数据网络中发起网络注册, 若网络注册成功, 则通过 WLAN 与所述服务器建立所述第二网络连接。

4、一种双连接安全通讯的方法, 用于服务器, 其特征在于, 包括:

通过移动数据网络与终端建立第一网络连接, 通过 WLAN 与所述终端建立第二网络连接;

10 从所述第一网络连接上接收所述终端发送的第一请求数据包, 从所述第二网络连接上接收所述终端发送的第二请求数据包, 合并所述第一请求数据包和所述第二请求数据包, 以得到所述终端发送的登录请求消息;

根据所述登录请求消息生成向终端发送的登录应答消息, 将所述登录应答消息拆分为第一应答数据包和第二应答数据包, 在所述第一网络连接上向所述
15 终端发送第一应答数据包, 在所述第二网络连接上向所述终端发送第二应答数据包, 以完成用户登录。

5、根据权利要求 4 所述的方法, 其特征在于, 所述登录应答消息包括登录成功消息或登录失败消息;

20 所述在所述向所述终端发送第一应答数据包和第二应答数据包的步骤之后, 所述方法还包括:

若所述登录应答消息为登录失败消息, 则用户登录失败, 断开所述通过所述移动数据网络与所述终端建立的第一网络连接, 并且断开所述通过 WLAN 与所述终端建立的第二网络连接, 以结束用户登录;

25 若所述登录应答消息为登录成功消息, 则用户登录成功, 断开所述通过所述移动数据网络与所述终端建立的第一网络连接, 以完成用户登录; 或者,

若所述登录应答消息为登录成功消息, 则用户登录成功, 断开所述通过 WLAN 与所述终端建立的第二网络连接, 以完成用户登录。

6、一种终端设备, 其特征在于, 包括:

接收单元, 用于接收用户发送的服务器登录指令;

处理单元,用于通过移动数据网络与所述服务器建立第一网络连接,通过 WLAN 与所述服务器建立第二网络连接;

所述处理单元还用于,根据所述接收单元收到的服务器登录指令生成向服务器发送的登录请求消息,将所述登录请求消息拆分为第一请求数据包和第二请求数据包;

发送单元,用于在所述第一网络连接上向所述服务器发送所述第一请求数据包,在所述第二网络连接上向所述服务器发送第二请求数据包;

所述接收单元还用于,从所述第一网络连接上接收所述服务器发送的第一应答数据包,从所述第二网络连接上接收所述服务器发送的第二应答数据包;

所述处理单元还用于,将所述接收单元收到的所述第一应答数据包和所述第二应答数据包合并为所述服务器发送的登录应答消息,以完成用户登录。

7、根据权利要求 6 所述的设备,其特征在于,所述处理单元还用于:

若所述接收单元收到的所述服务器发送的登录应答消息为登录失败消息,则用户登录失败,断开所述通过移动数据网络与所述服务器建立的第一网络连接,并且断开所述通过 WLAN 与所述服务器建立的第二网络连接,以结束用户登录;

若所述接收单元收到的所述服务器发送的登录应答消息为登录成功消息,则用户登录成功,断开所述通过移动数据网络与所述服务器建立的第一网络连接,以完成用户登录;或者,

若所述接收单元收到的服务器发送的登录应答消息为登录成功消息,则用户登录成功,断开所述通过 WLAN 与所述服务器建立的第二网络连接,以完成用户登录。

8、根据权利要求 6 所述的设备,其特征在于,所述处理单元具体用于:

在移动数据网络中发起网络注册,若网络注册成功,则通过所述移动数据网络与所述服务器建立所述第一网络连接;

在 WLAN 中发起安全认证,若安全认证成功,则通过 WLAN 与所述服务器建立所述第二网络连接;或者,在移动数据网络中发起网络注册,若网络注册成功,则通过 WLAN 与所述服务器建立所述第二网络连接。

9、一种服务器设备,其特征在于,包括:

处理单元,用于通过移动数据网络与终端建立第一网络连接,通过 WLAN 与所述终端建立第二网络连接;

接收单元,用于从所述第一网络连接上接收所述终端发送的第一请求数据包,从所述第二网络连接上接收所述终端发送的第二请求数据包;

5 所述处理单元还用于,合并所述接收单元收到的所述第一请求数据包和所述第二请求数据包,以得到所述终端发送的登录请求消息;并且,根据所述登录请求消息生成向终端发送的登录应答消息,将所述登录应答消息拆分为第一应答数据包和第二应答数据包;

10 发送单元,用于在所述第一网络连接上向所述终端发送第一应答数据包,在所述第二网络连接上向所述终端发送第二应答数据包,以完成用户登录。

10、根据权利要求 9 所述的设备,其特征在于,所述登录应答消息包括登录成功消息或登录失败消息;

所述处理单元还用于:

15 若所述登录应答消息为服务器登录失败消息,则用户登录失败,断开所述通过所述移动数据网络与所述终端建立的第一网络连接,并且断开所述通过 WLAN 与所述终端建立的第二网络连接,以结束用户登录;

若所述登录应答消息为登录成功消息,则用户登录成功,断开所述通过所述移动数据网络与所述终端建立的第一网络连接,以完成用户登录;或者,

20 若所述登录应答消息为登录成功消息,则用户登录成功,断开所述通过 WLAN 与所述终端建立的第二网络连接,以完成用户登录。

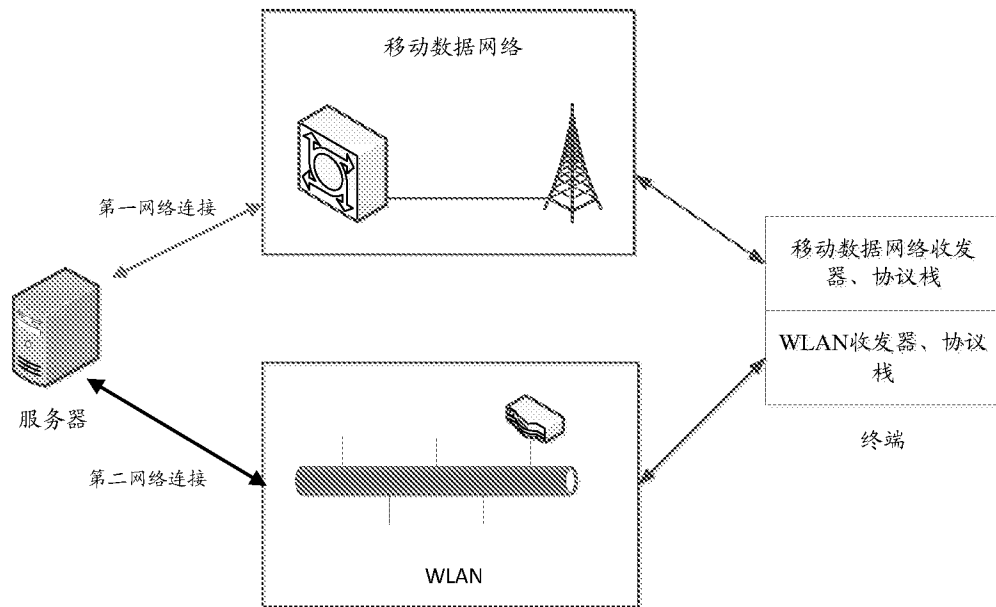


图 1

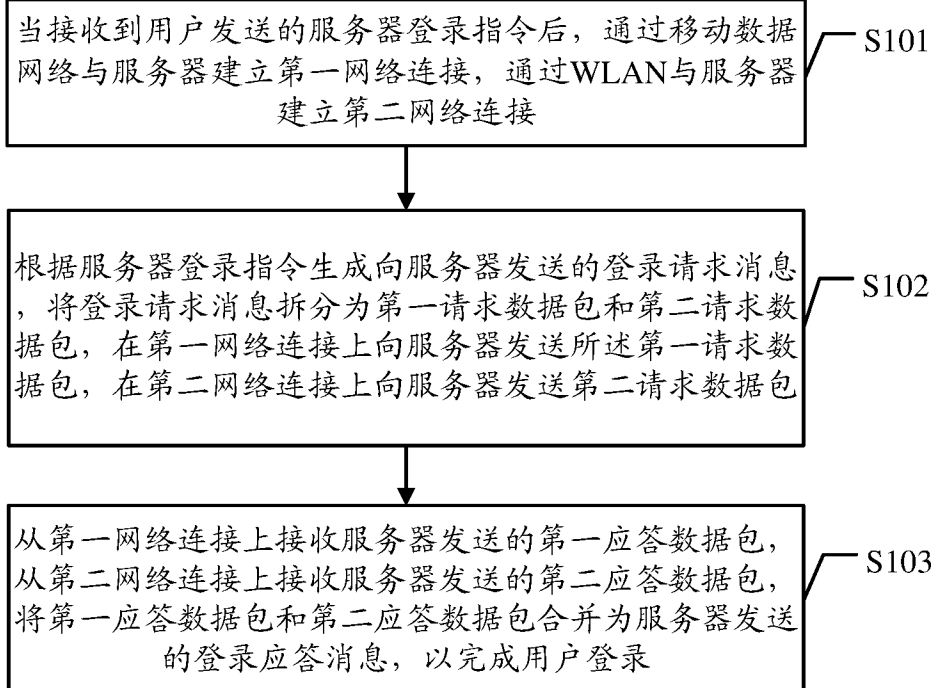


图 2

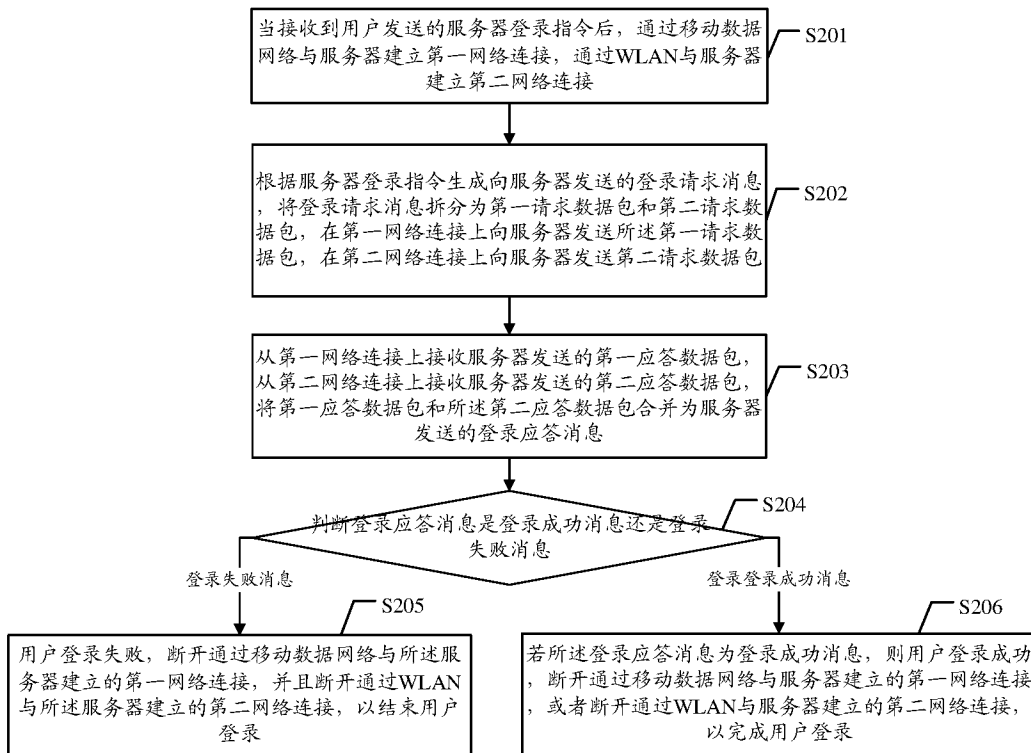


图 3

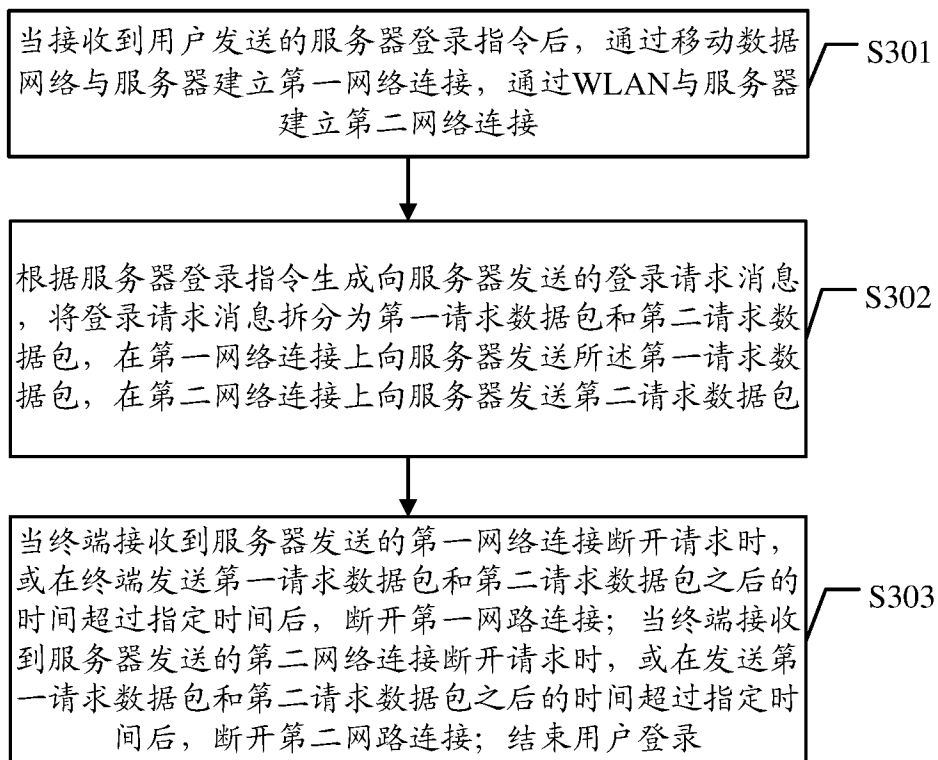


图 4

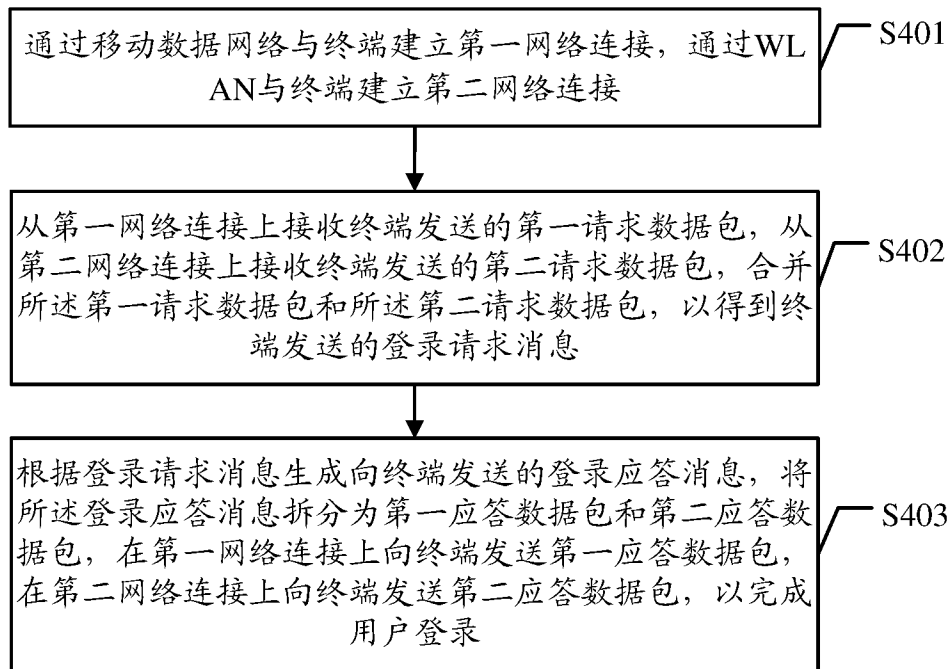


图 5

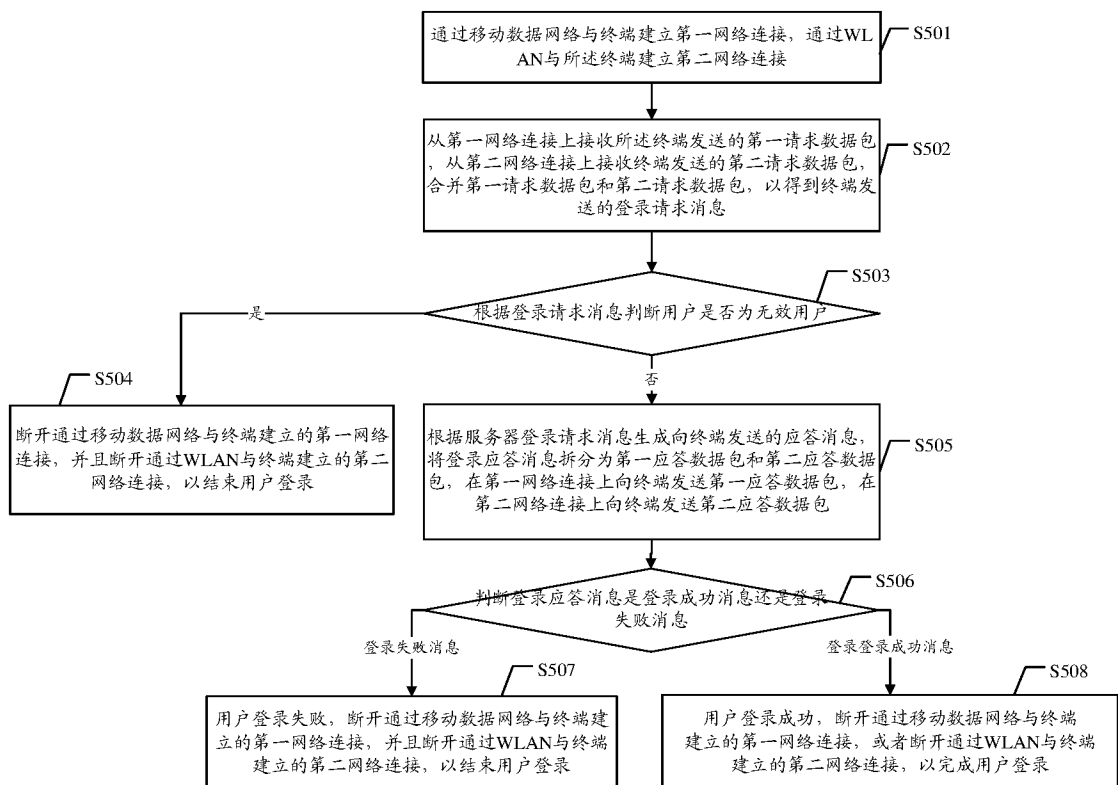


图 6

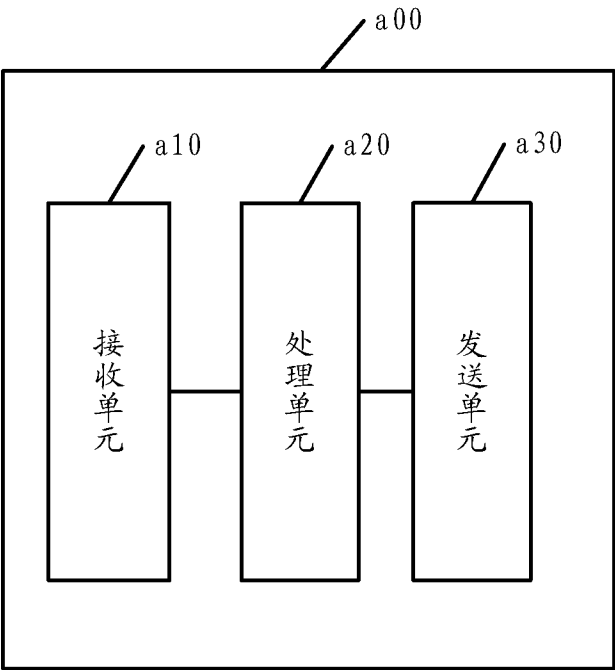


图 7

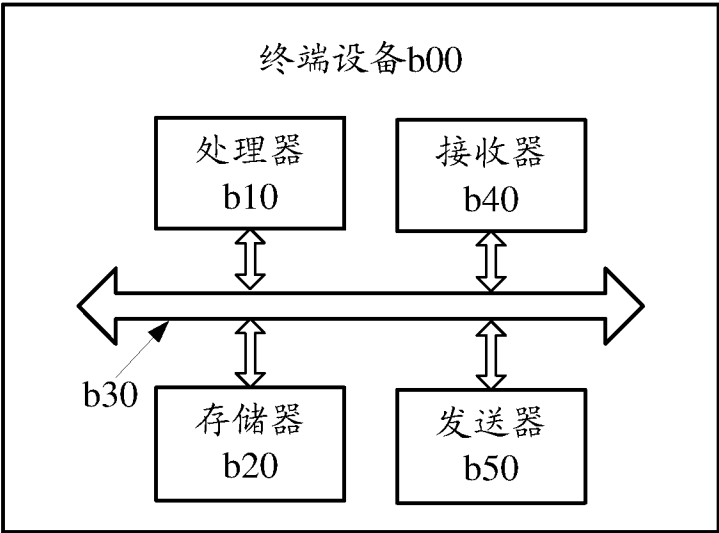


图 8

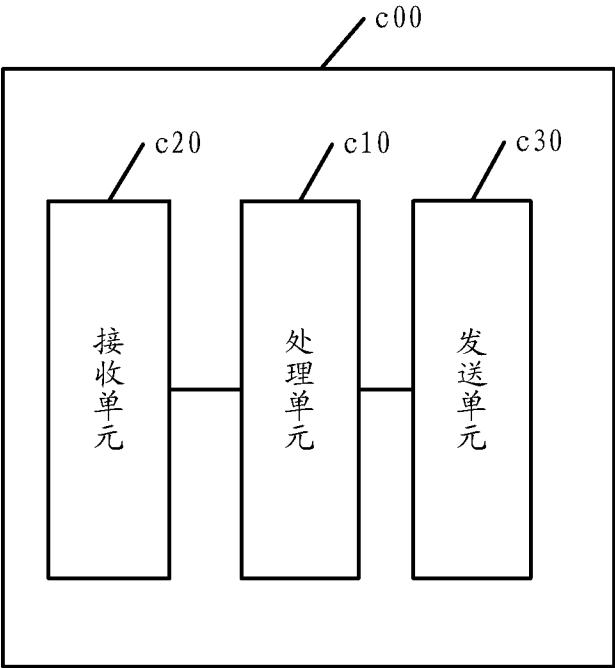


图 9

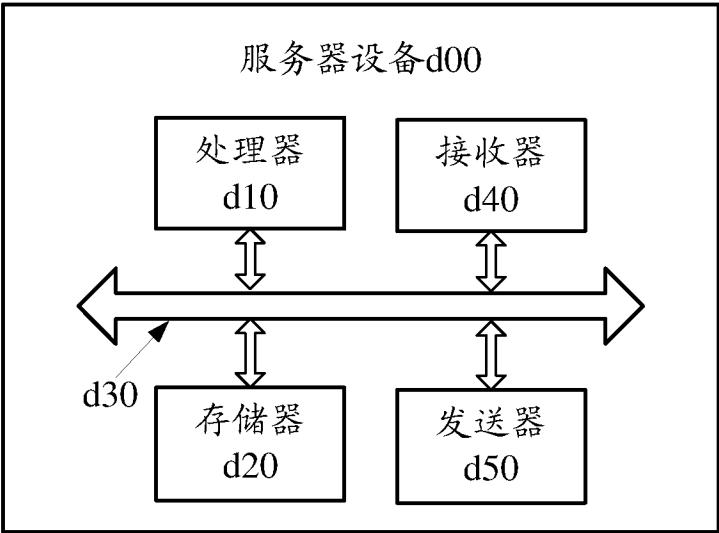


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/085860**A. CLASSIFICATION OF SUBJECT MATTER**

H04W 12/08 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04Q; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: dual link, server, login, logon, split, combination, packet, multi-channel, multi-connection, instruction, request, respond

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 1684410 A (HITACHI LTD.), 19 October 2005 (19.10.2005), description, pages 9-10, and figure 5	1-10
Y	CN 103780375 A (CHINA TELECOM CO., LTD.), 07 May 2014 (07.05.2014), description, paragraphs [0004]-[0030]	1-10
A	CN 1852284 A (PAN, Guogang et al.), 25 October 2006 (25.10.2006), the whole document	1-10
A	EP 2273417 A2 (UNILOC USA, INC.), 12 January 2011 (12.01.2011), the whole document	1-10

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

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 11 April 2016 (11.04.2016)	Date of mailing of the international search report 28 April 2016 (28.04.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer ZHANG, Qi Telephone No.: (86-10) 62413262

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/085860

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1684410 A	19 October 2005	JP 2005327235 A	24 November 2005
		TW 200534660 A	16 October 2005
		US 2005228994 A1	13 October 2005
		EP 1586973 A2	19 October 2005
		KR 20050100334 A	18 October 2005
CN 103780375 A	07 May 2014	None	
CN 1852284 A	25 October 2006	None	
EP 2273417 A2	12 January 2011	US 2010325040 A1	23 December 2010

国际检索报告

国际申请号

PCT/CN2015/085860

A. 主题的分类

H04W 12/08(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04Q; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI, WPI, EPDOC: 双连接, 服务器, 登录, 拆分, 合并, 数据包, 多通道, 多连接, 指令, 请求, 应答, dual link, server, login, logon, split, combination, packet, multi-channel, multi-connection, instruction, request, respond

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 1684410 A (株式会社日立制作所) 2005年 10月 19日 (2005 - 10 - 19) 说明书第9-10页、附图5	1-10
Y	CN 103780375 A (中国电信股份有限公司) 2014年 5月 7日 (2014 - 05 - 07) 说明书第[0004]-[0030]段	1-10
A	CN 1852284 A (潘国纲等) 2006年 10月 25日 (2006 - 10 - 25) 全文	1-10
A	EP 2273417 A2 (UNILOC USA, INC.) 2011年 1月 12日 (2011 - 01 - 12) 全文	1-10

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 4月 11日

国际检索报告邮寄日期

2016年 4月 28日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

张琦

电话号码 (86-10)62413262

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/085860

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	1684410	A	2005年 10月 19日	JP	2005327235	A	2005年 11月 24日
				TW	200534660	A	2005年 10月 16日
				US	2005228994	A1	2005年 10月 13日
				EP	1586973	A2	2005年 10月 19日
				KR	20050100334	A	2005年 10月 18日
CN	103780375	A	2014年 5月 7日	无			
CN	1852284	A	2006年 10月 25日	无			
EP	2273417	A2	2011年 1月 12日	US	2010325040	A1	2010年 12月 23日

表 PCT/ISA/210 (同族专利附件) (2009年7月)