



(12) 发明专利申请

(10) 申请公布号 CN 105635249 A

(43) 申请公布日 2016. 06. 01

(21) 申请号 201510959129. X

(22) 申请日 2015. 12. 18

(71) 申请人 小米科技有限责任公司  
地址 100085 北京市海淀区清河中街 68 号  
华润五彩城购物中心二期 13 层

(72) 发明人 高承星 霍东海 陈德嘉

(74) 专利代理机构 北京三高永信知识产权代理  
有限责任公司 11138  
代理人 鞠永善

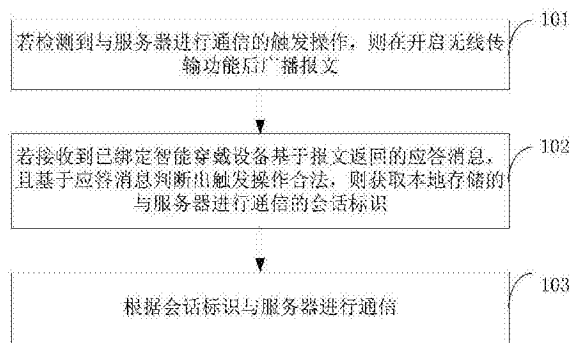
(51) Int. Cl.  
H04L 29/08(2006. 01)  
H04L 29/06(2006. 01)  
H04L 1/16(2006. 01)

权利要求书3页 说明书13页 附图6页

(54) 发明名称  
会话管理方法及装置

(57) 摘要

本公开是关于一种会话管理方法及装置,属于通信技术领域。所述方法包括:若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识;根据所述会话标识与所述服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险。



1. 一种会话管理方法,应用于智能终端,其特征在于,所述方法包括:

若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;

若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识;

根据所述会话标识与所述服务器进行通信。

2. 根据权利要求1所述的方法,其特征在于,所述若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识,包括:

在广播第一类型报文后,若接收到所述已绑定智能穿戴设备返回的第一应答消息,则检测所述第一应答消息中是否携带验证通过标识;

若所述第一应答消息中携带所述验证通过标识,则确定所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

其中,所述验证通过标识,用于表示所述已绑定智能穿戴设备接收到的所述第一类型报文的信号强度大于预设阈值,所述信号强度的数值越大,所述已绑定智能穿戴设备与智能终端之间的距离越小。

3. 根据权利要求1所述的方法,其特征在于,所述若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识,包括:

在广播第二类型报文后,若接收到所述已绑定智能穿戴设备返回的第二应答消息,则获取本地存储的验证字符串;

根据所述验证字符串对所述第二类型报文中的测试字符串进行加密,得到加密信息;

若所述第二应答消息与所述加密信息一致,则确定所述第二应答消息由所述已绑定智能穿戴设备返回,所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

其中,所述验证字符串由所述已绑定智能穿戴设备预先发送至智能终端,所述已绑定智能穿戴设备用于根据所述验证字符串对所述测试字符串进行加密,得到所述第二应答消息。

4. 一种会话管理方法,应用于智能穿戴设备,其特征在于,所述方法包括:

在开启无线传输功能后,接收已绑定的智能终端广播的报文;

生成与所述报文匹配的应答消息;

将所述应答消息返回至所述智能终端,所述应答消息用于指示所述智能终端与服务器进行通信的触发操作是否合法。

5. 根据权利要求4所述的方法,其特征在于,所述生成与所述报文匹配的应答消息,包括:

若所述报文为第一类型报文,则检测所述第一类型报文的信号强度,当所述信号强度大于预设阈值时,生成携带验证通过标识的第一应答消息,所述第一应答消息用于指示所述触发操作是否合法;

若所述报文为第二类型报文,则根据本地存储的验证字符串,对所述第二类型报文中的测试字符串进行加密,得到第二应答消息,所述第二应答消息用于指示所述触发操作是否合法。

6. 一种会话管理装置,其特征在于,所述装置包括:

广播模块,被配置为若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;

获取模块,被配置为若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识;

通信模块,被配置为根据所述会话标识与所述服务器进行通信。

7. 根据权利要求6所述的装置,其特征在于,所述获取模块,还被配置为在广播第一类型报文后,若接收到所述已绑定智能穿戴设备返回的第一应答消息,则检测所述第一应答消息中是否携带验证通过标识;若所述第一应答消息中携带所述验证通过标识,则确定所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

其中,所述验证通过标识,用于表示所述已绑定智能穿戴设备接收到的所述第一类型报文的信号强度大于预设阈值,所述信号强度的数值越大,所述已绑定智能穿戴设备与智能终端之间的距离越小。

8. 根据权利要求6所述的装置,其特征在于,所述获取模块,还被配置为在广播第二类型报文后,若接收到所述已绑定智能穿戴设备返回的第二应答消息,则获取本地存储的验证字符串;根据所述验证字符串对所述第二类型报文中的测试字符串进行加密,得到加密信息;若所述第二应答消息与所述加密信息一致,则确定所述第二应答消息由所述已绑定智能穿戴设备返回,所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

其中,所述验证字符串由所述已绑定智能穿戴设备预先发送至智能终端,所述已绑定智能穿戴设备用于根据所述验证字符串对所述测试字符串进行加密,得到所述第二应答消息。

9. 一种会话管理装置,其特征在于,所述装置包括:

接收模块,被配置为在开启无线传输功能后,接收已绑定的智能终端广播的报文;

生成模块,被配置为生成与所述报文匹配的应答消息;

发送模块,被配置为将所述应答消息返回至所述智能终端,所述应答消息用于指示所述智能终端与服务器进行通信的触发操作是否合法。

10. 根据权利要求9所述的装置,其特征在于,所述生成模块,被配置为若所述报文为第一类型报文,则检测所述第一类型报文的信号强度,当所述信号强度大于预设阈值时,生成携带验证通过标识的第一应答消息,所述第一应答消息用于指示所述触发操作是否合法;若所述报文为第二类型报文,则根据本地存储的验证字符串,对所述第二类型报文中的测试字符串进行加密,得到第二应答消息,所述第二应答消息用于指示所述触发操作是否合法。

11. 一种会话管理装置,其特征在于,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器被配置为:若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于

所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识;根据所述会话标识与所述服务器进行通信。

12.一种会话管理装置,其特征在于,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器被配置为:在开启无线传输功能后,接收已绑定的智能终端广播的报文;生成与所述报文匹配的应答消息;将所述应答消息返回至所述智能终端,所述应答消息用于指示所述智能终端与服务器进行通信的触发操作是否合法。

## 会话管理方法及装置

### 技术领域

[0001] 本公开涉及通信技术领域,特别涉及一种会话管理方法及装置。

### 背景技术

[0002] 会话(Session),指代终端与服务器进行通信的一个具体场景。通常指用户从登入网站到离开网站进行的所有交互动作。具体到网络应用中,一个会话可以简单理解为:用户通过终端打开一个浏览器,访问某一个网站,在这个网站点击多个超链接,访问服务器存储的多个网络资源,直到用户空闲时间超过了某一个时间界限,才会释放该会话资源,整个过程称之为一个会话。

[0003] 由于会话机制在B/S(Browser/Server,浏览器/服务器)架构中使用频繁,因此需对各个会话进行管理。相关技术在进行会话管理时,通常采取下述方式:每当一个新用户A通过终端成功登录时,服务器会创建一个新的会话标识,并将该会话标识下发至新用户A的终端。该终端将该会话标识存储在本地。若在用户空闲时间未超过时间界限内,新用户A再次通过该终端向该服务器发送操作请求,则自动获取存储在本地的该会话标识,在每个操作请求中携带该会话标识。服务器在基于携带的会话标识确定请求发起者为新用户A后,再向新用户A返回操作请求的响应结果。

### 发明内容

[0004] 为克服相关技术中存在的问题,本公开提供一种会话管理方法及装置。

[0005] 根据本公开实施例的第一方面,提供一种会话管理方法,所述方法包括:

[0006] 若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;

[0007] 若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识;

[0008] 根据所述会话标识与所述服务器进行通信。

[0009] 在另一个实施例中,所述若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识,包括:

[0010] 在广播第一类型报文后,若接收到所述已绑定智能穿戴设备返回的第一应答消息,则检测所述第一应答消息中是否携带验证通过标识;

[0011] 若所述第一应答消息中携带所述验证通过标识,则确定所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

[0012] 其中,所述验证通过标识,用于表示所述已绑定智能穿戴设备接收到的所述第一类型报文的信号强度大于预设阈值,所述信号强度的数值越大,所述已绑定智能穿戴设备与智能终端之间的距离越小。

[0013] 在另一个实施例中,所述若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进

行通信的会话标识,包括:

[0014] 在广播第二类型报文后,若接收到所述已绑定智能穿戴设备返回的第二应答消息,则获取本地存储的验证字符串;

[0015] 根据所述验证字符串对所述第二类型报文中的测试字符串进行加密,得到加密信息;

[0016] 若所述第二应答消息与所述加密信息一致,则确定所述第二应答消息由所述已绑定智能穿戴设备返回,所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

[0017] 其中,所述验证字符串由所述已绑定智能穿戴设备预先发送至智能终端,所述已绑定智能穿戴设备用于根据所述验证字符串对所述测试字符串进行加密,得到所述第二应答消息。

[0018] 根据本公开实施例的第二方面,提供一种会话管理方法,应用于智能穿戴设备,所述方法包括:

[0019] 在开启无线传输功能后,接收已绑定的智能终端广播的报文;

[0020] 生成与所述报文匹配的应答消息;

[0021] 将所述应答消息返回至所述智能终端,所述应答消息用于指示所述智能终端与服务器进行通信的触发操作是否合法。

[0022] 在另一个实施例中,所述生成与所述报文匹配的应答消息,包括:

[0023] 若所述报文为第一类型报文,则检测所述第一类型报文的信号强度,当所述信号强度大于预设阈值时,生成携带验证通过标识的第一应答消息,所述第一应答消息用于指示所述触发操作是否合法;

[0024] 若所述报文为第二类型报文,则根据本地存储的验证字符串,对所述第二类型报文中的测试字符串进行加密,得到第二应答消息,所述第二应答消息用于指示所述触发操作是否合法。

[0025] 根据本公开实施例的第三方面,提供一种会话管理装置,所述装置包括:

[0026] 广播模块,被配置为若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;

[0027] 获取模块,被配置为若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识;

[0028] 通信模块,被配置为根据所述会话标识与所述服务器进行通信。

[0029] 在另一个实施例中,所述获取模块,还被配置为在广播第一类型报文后,若接收到所述已绑定智能穿戴设备返回的第一应答消息,则检测所述第一应答消息中是否携带验证通过标识;若所述第一应答消息中携带所述验证通过标识,则确定所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

[0030] 其中,所述验证通过标识,用于表示所述已绑定智能穿戴设备接收到的所述第一类型报文的信号强度大于预设阈值,所述信号强度的数值越大,所述已绑定智能穿戴设备与智能终端之间的距离越小。

[0031] 在另一个实施例中,所述获取模块,还被配置为在广播第二类型报文后,若接收到

所述已绑定智能穿戴设备返回的第二应答消息,则获取本地存储的验证字符串;根据所述验证字符串对所述第二类型报文中的测试字符串进行加密,得到加密信息;若所述第二应答消息与所述加密信息一致,则确定所述第二应答消息由所述已绑定智能穿戴设备返回,所述触发操作合法,获取本地存储的与所述服务器进行通信的会话标识;

[0032] 其中,所述验证字符串由所述已绑定智能穿戴设备预先发送至智能终端,所述已绑定智能穿戴设备用于根据所述验证字符串对所述测试字符串进行加密,得到所述第二应答消息。

[0033] 根据本公开实施例的第四方面,提供一种会话管理装置,所述装置包括:

[0034] 接收模块,被配置为在开启无线传输功能后,接收已绑定的智能终端广播的报文;

[0035] 生成模块,被配置为生成与所述报文匹配的应答消息;

[0036] 发送模块,被配置为将所述应答消息返回至所述智能终端,所述应答消息用于指示所述智能终端与服务器进行通信的触发操作是否合法。

[0037] 在另一个实施例中,所述生成模块,被配置为若所述报文为第一类型报文,则检测所述第一类型报文的信号强度,当所述信号强度大于预设阈值时,生成携带验证通过标识的第一应答消息,所述第一应答消息用于指示所述触发操作是否合法;若所述报文为第二类型报文,则根据本地存储的验证字符串,对所述第二类型报文中的测试字符串进行加密,得到第二应答消息,所述第二应答消息用于指示所述触发操作是否合法。

[0038] 根据本公开实施例的第五方面,提供一种会话管理装置,包括:

[0039] 处理器;

[0040] 用于存储处理器可执行指令的存储器;

[0041] 其中,所述处理器被配置为:若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;若接收到已绑定智能穿戴设备基于所述报文返回的应答消息,且基于所述应答消息判断出所述触发操作合法,则获取本地存储的与所述服务器进行通信的会话标识;根据所述会话标识与所述服务器进行通信。

[0042] 根据本公开实施例的第六方面,提供一种会话管理装置,包括:

[0043] 处理器;

[0044] 用于存储处理器可执行指令的存储器;

[0045] 其中,所述处理器被配置为:在开启无线传输功能后,在开启无线传输功能后,接收已绑定的智能终端广播的报文;生成与所述报文匹配的应答消息;将所述应答消息返回至所述智能终端,所述应答消息用于指示所述智能终端与服务器进行通信的触发操作是否合法。

[0046] 本公开的实施例提供的技术方案可以包括以下有益效果:

[0047] 若智能终端检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险,效果

较佳。

[0048] 应当理解的是,以上的一般描述和后文的细节描述仅是示例性和解释性的,并不能限制本公开。

### 附图说明

[0049] 此处的附图被并入说明书中并构成本说明书的一部分,示出了符合本发明的实施例,并与说明书一起用于解释本发明的原理。

[0050] 图1是根据一示例性实施例示出的一种会话管理方法的流程图。

[0051] 图2是根据一示例性实施例示出的一种会话管理方法的流程图。

[0052] 图3A是根据一示例性实施例示出的一种会话管理方法的流程图。

[0053] 图3B是根据一示例性实施例示出的一种会话管理方法的流程图。

[0054] 图4是根据一示例性实施例示出的一种交互系统的框图。

[0055] 图5是根据一示例性实施例示出的一种会话管理装置的框图。

[0056] 图6是根据一示例性实施例示出的一种会话管理装置的框图。

[0057] 图7是根据一示例性实施例示出的一种会话管理装置的框图。

[0058] 图8是根据一示例性实施例示出的一种会话管理装置的框图。

[0059] 图9是根据一示例性实施例示出的一种会话管理装置的框图。

### 具体实施方式

[0060] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本发明相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本发明的一些方面相一致的装置和方法的例子。

[0061] 图1是根据一示例性实施例示出的一种会话管理方法的流程图,如图1所示,该方法用于智能终端中,包括以下步骤。

[0062] 在步骤101中、若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文。

[0063] 在步骤102中、若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识。

[0064] 在步骤103中、根据会话标识与服务器进行通信。

[0065] 本公开实施例提供的方法,若智能终端检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险,效果较佳。

[0066] 在另一个实施例中,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且



基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,包括:

[0067] 在广播第一类型报文后,若接收到已绑定智能穿戴设备返回的第一应答消息,则检测第一应答消息中是否携带验证通过标识;

[0068] 若第一应答消息中携带验证通过标识,则确定触发操作合法,获取本地存储的与服务器进行通信的会话标识;

[0069] 其中,验证通过标识,用于表示已绑定智能穿戴设备接收到的第一类型报文的信号强度大于预设阈值,信号强度的数值越大,已绑定智能穿戴设备与智能终端之间的距离越小。

[0070] 在另一个实施例中,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,包括:

[0071] 在广播第二类型报文后,若接收到已绑定智能穿戴设备返回的第二应答消息,则获取本地存储的验证字符串;

[0072] 根据验证字符串对第二类型报文中的测试字符串进行加密,得到加密信息;

[0073] 若第二应答消息与加密信息一致,则确定第二应答消息由已绑定智能穿戴设备返回,触发操作合法,获取本地存储的与服务器进行通信的会话标识;

[0074] 其中,验证字符串由已绑定智能穿戴设备预先发送至智能终端,已绑定智能穿戴设备用于根据验证字符串对测试字符串进行加密,得到第二应答消息。

[0075] 在另一个实施例中,该方法还包括:

[0076] 获取智能穿戴设备的第一设备标识;

[0077] 建立第一设备标识与智能终端的第二设备标识之间的绑定关系。

[0078] 上述所有可选技术方案,可以采用任意结合形成本公开的可选实施例,在此不再一一赘述。

[0079] 图2是根据一示例性实施例示出的一种会话管理方法的流程图,如图2所示,该方法用于智能穿戴设备中,包括以下步骤。

[0080] 在步骤201中、在开启无线传输功能后,接收已绑定的智能终端广播的报文;

[0081] 在步骤202中、获取与该报文匹配的应答消息;

[0082] 在步骤203中、将该应答消息返回至智能终端,该应答消息用于指示智能终端与服务器进行通信的触发操作是否合法。

[0083] 本公开实施例提供的方法,在开启无线传输功能后,接收已绑定的智能终端广播的报文,并生成与报文匹配的应答消息,将应答消息返回至智能终端,由智能终端在接收到已绑定智能穿戴设备返回的应答消息后,若基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识;根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险,效果较佳。

[0084] 在另一个实施例中,生成与报文匹配的应答消息,包括:

[0085] 若报文为第一类型报文,则检测第一类型报文的信号强度,当信号强度大于预设阈值时,生成携带验证通过标识的第一应答消息,第一应答消息用于指示触发操作是否合法;

[0086] 若报文为第二类型报文,则根据本地存储的验证字符串,对第二类型报文中的测试字符串进行加密,得到第二应答消息,第二应答消息用于指示触发操作是否合法。

[0087] 在另一个实施例中,该方法还包括:

[0088] 获取智能终端的第二设备标识;

[0089] 建立智能穿戴设备的第一设备标识与第二设备标识之间的绑定关系。

[0090] 上述所有可选技术方案,可以采用任意结合形成本公开的可选实施例,在此不再一一赘述。

[0091] 图3A是根据一示例性实施例示出的一种会话管理方法的流程图,如图3A所示,本实施例的交互主体包括智能终端、服务器和智能穿戴设备,包括以下步骤:

[0092] 在步骤301a中,智能终端获取智能穿戴设备的第一设备标识,智能终端建立第一设备标识与智能终端的第二设备标识之间的绑定关系。

[0093] 参见图4,图4是根据一示例性实施例示出的一种交互系统的框图,该交互系统包括智能终端、服务器和智能穿戴设备。其中,智能终端与该服务器之间通过网络连接,智能终端和智能穿戴设备绑定。智能终端可以为手机、平板电脑等,智能穿戴设备可为智能手环,本公开实施例对此不进行具体限定。第一设备标识通常指代智能穿戴设备的MAC(Media Access Control,介质访问控制)地址,第二设备标识通常指代智能终端的MAC地址,本公开实施例对此同样不进行具体限定。

[0094] 其中,第一设备标识可由用户手动通过智能终端提供的输入页面输入,或者通过接收智能穿戴设备通过蓝牙或红外等途径发送的数据包得到,还可通过接收绑定服务器发送的绑定请求得到。针对第三种情况,智能穿戴设备事先将第一设备标识上传到绑定服务器。智能终端在得到第一设备标识后,建立第一设备标识与第二设备标识之间的绑定关系,以便后续过程中,在检测到用户登录网络系统或浏览网页时,对用户的身份进行验证,确保用户的隐私安全。

[0095] 在步骤302a中,智能穿戴设备获取智能终端的第二设备标识,智能穿戴设备建立智能穿戴设备的第一设备标识与第二设备标识之间的绑定关系。

[0096] 该步骤通上述步骤301a类似,此处不再赘述。

[0097] 在步骤303a中,智能终端在检测到与服务器进行通信的触发操作后,在开启无线传输功能后广播第一类型报文。

[0098] 在本公开实施例中,与服务进行通信的触发操作可为用户的网络系统登录或返回操作、浏览网页等操作,本公开实施例对此不进行具体限定。无线传输功能可为蓝牙功能。例如,智能终端和智能穿戴设备可以配置蓝牙功能,智能终端在开启蓝牙功能后,可以通过蓝牙功能广播报文,当智能穿戴设备位于智能终端的周围地理区域内时,智能穿戴设备可以通过蓝牙功能接收该报文。

[0099] 其中,第一类型报文可为beacons报文或者其他类型的报文,本实施例对此同样不进行具体限定。且,智能终端可以实时地广播该报文,也可以周期性地广播该报文,广播周期可以为1s、5s等,本实施例对此同样不进行具体限定。

[0100] 在步骤304a中,智能穿戴设备在开启无线传输功能后,接收智能终端广播的第一类型报文。

[0101] 当智能穿戴设备位于智能终端的周围地理区域时,若智能穿戴设备同样开启了无线传输功能,则智能设备便可接收到智能终端广播的第一类型报文。且二者之间的距离越近,第一类型报文的信号强度越大。其中,第一类型报文中携带了第二设备标识。这样,智能穿戴设备根据第二设备标识,便可知道该第一类型报文由与其建立绑定关系的智能终端发起。

[0102] 在步骤305a中,智能穿戴设备检测第一类型报文的信号强度,当信号强度大于预设阈值时,生成携带验证通过标识的第一应答消息,并将第一应答消息返回至智能终端。

[0103] 其中,第一类型报文的信号强度可以为该报文的RSSI(Received Signal Strength Indication,接收信号的强度指示)或者其他用于表示信号强度的参数,本公开实施例对此不进行具体限定。预设阈值可由用户进行设置,本公开实施例对预设阈值的大小同样不进行具体限定。

[0104] 信号强度大于阈值,则证明智能终端与智能穿戴设备之间的距离很小。而智能穿戴设备一般佩戴在用户本人的身上。所以,当智能穿戴设备检测到信号强度大于预设阈值时,即确定智能终端由用户本人拿在手里,当前在智能终端上执行的操作由用户本人发起,处于安全状态,生成携带验证通过标识的第一应答消息,并将第一应答消息返回至智能终端。其中,验证通过标识可为一个flag标识位,1表示大于预设阈值,0表示小于预设阈值等,本公开实施例对此同样不进行具体限定。第一应答消息中还携带了第一设备标识。这样,智能终端根据第一设备标识,便可知道该第一应答消息由与其建立绑定关系的智能穿戴设备返回。

[0105] 在步骤306a中,智能终端检测第一应答消息中是否携带验证通过标识;若第一应答消息中携带验证通过标识,则确定该触发操作合法,获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。

[0106] 若第一应答消息中携带验证通过标识,比如flag=1,则确定该触发操作由用户本人发起,该触发操作合法。由于每当一个新用户A通过客户端成功登录时,服务器会创建一个新的会话标识,并将该会话标识下发至新用户A的客户端。该客户端将该会话标识存储在本地。所以,在确定该触发操作合法后,智能终端可将本地存储的与服务器通信的会话标识取出,根据该会话标识和用户操作生成操作请求,该操作请求中均会携带该会话标识。服务器在基于携带的会话标识确定该操作请求发起者为新用户A后,再向新用户A返回该操作请求的响应结果。

[0107] 本公开实施例提供的方法,若智能终端检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取从而造成用户隐私泄露的风险,效果更佳。

[0108] 图3B是根据一示例性实施例示出的一种会话管理方法的流程图,如图3B所示,本实施例的交互主体包括智能终端、服务器和智能穿戴设备,包括以下步骤:

[0109] 在步骤301b中,智能终端获取智能穿戴设备的第一设备标识,智能终端建立第一设备标识与智能终端的第二设备标识之间的绑定关系。

[0110] 该步骤通上述步骤301a类似,此处不再赘述。

[0111] 在步骤302b中,智能穿戴设备获取智能终端的第二设备标识,智能穿戴设备建立智能穿戴设备的第一设备标识与第二设备标识之间的绑定关系。

[0112] 该步骤通上述步骤301a类似,此处不再赘述。

[0113] 在步骤303b中,智能终端在检测到与服务器进行通信的触发操作后,在开启无线传输功能后广播第二类型报文。

[0114] 在本公开实施例中,智能穿戴设备与智能终端之间为了方便地进行身份验证,智能穿戴设备事先发送一个验证字符串给智能终端,智能终端将该验证字符串存储在本地,以便进行后续过程中在检测到与服务器进行通信的触发操作后,对用户身份进行验证。其中,该验证字符串本质上为二者之间约定好的一个key或token。第二类型报文中携带了测试字符串,该测试字符串可由纯数字、纯字母、数字和字母混合组成,位数不限。

[0115] 在步骤304b中,智能穿戴设备在开启无线传输功能后,接收智能终端广播的第二类型报文,根据本地存储的验证字符串对第二类型报文中的测试字符串进行加密,得到第二应答消息,将第二应答消息返回至智能终端。

[0116] 在本公开实施例中,第二类型报文中携带了第二设备标识。这样,智能穿戴设备根据第二设备标识,便可知道该第二类型报文由与其建立绑定关系的智能终端发起。智能穿戴设备在根据本地存储的验证字符串对第二类型报文中的测试字符串进行加密时,可采取与智能终端事先约定好的加密算法进行加密,本公开实施例对此不进行具体限定。第一应答消息中还携带了第一设备标识。这样,智能终端根据第一设备标识,便可知道该第二应答消息由与其建立绑定关系的智能穿戴设备返回。

[0117] 在步骤305b中,智能终端在接收到返回的第二应答消息后,获取本地存储的验证字符串;根据验证字符串对第二类型报文中的测试字符串进行加密,得到加密信息。

[0118] 由于智能穿戴设备事先将验证字符串发送给了智能终端,所以智能终端可直接从本地存储介质中获取验证字符串,智能终端在根据本地存储的验证字符串对第二类型报文中的测试字符串进行加密时,可采取与智能穿戴设备事先约定好的加密算法进行加密,本公开实施例对此不进行具体限定。

[0119] 在步骤306b中,若智能终端判断出第二应答消息与加密信息一致,则确定第二应答消息由已绑定智能穿戴设备返回,该触发操作合法,获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。

[0120] 若第二应答消息与加密信息一致,则证明佩戴已绑定智能穿戴设备的用户本人,位于智能设备在开启无线传输功能后可探测到范围内,确定该触发操作由用户本人发起,该触发操作合法。由于每当一个新用户A通过客户端成功登录时,服务器会创建一个新的会话标识,并将该会话标识下发至新用户A的客户端。该客户端将该会话标识存储在本地。所以,在确定该触发操作合法后,智能终端可将本地存储的与服务器通信的会话标识取出,根据该会话标识和用户操作生成操作请求,该操作请求中均会携带该会话标识。服务器在基

于携带的会话标识确定该操作请求发起者为新用户A后,再向新用户A返回该操作请求的响应结果。

[0121] 本公开实施例提供的方法,若智能终端检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险,效果更佳。

[0122] 图5是根据一示例性实施例示出的一种会话管理装置的框图。参照图5,该装置包括广播模块501,获取模块502和通信模块503。

[0123] 广播模块501,被配置为若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;

[0124] 获取模块502,被配置为若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识;

[0125] 通信模块503,被配置为根据会话标识与服务器进行通信。

[0126] 在另一个实施例中,获取模块502,还被配置为在广播第一类型报文后,若接收到已绑定智能穿戴设备返回的第一应答消息,则检测第一应答消息中是否携带验证通过标识;若第一应答消息中携带验证通过标识,则确定触发操作合法,获取本地存储的与服务器进行通信的会话标识;

[0127] 其中,验证通过标识,用于表示已绑定智能穿戴设备接收到的第一类型报文的信号强度大于预设阈值,信号强度的数值越大,已绑定智能穿戴设备与智能终端之间的距离越小。

[0128] 在另一个实施例中,获取模块502,还被配置为在广播第二类型报文后,若接收到已绑定智能穿戴设备返回的第二应答消息,则获取本地存储的验证字符串;根据验证字符串对第二类型报文中的测试字符串进行加密,得到加密信息;若第二应答消息与加密信息一致,则确定第二应答消息由已绑定智能穿戴设备返回,触发操作合法,获取本地存储的与服务器进行通信的会话标识;

[0129] 其中,验证字符串由已绑定智能穿戴设备预先发送至智能终端,已绑定智能穿戴设备用于根据验证字符串对测试字符串进行加密,得到第二应答消息。

[0130] 在另一个实施例中,参见图6,获取模块502,还被配置为获取智能穿戴设备的第一设备标识;

[0131] 建立模块504,被配置为建立第一设备标识与智能终端的第二设备标识之间的绑定关系。

[0132] 本公开实施例提供的装置,若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的

用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险,效果较佳。

[0133] 图7是根据一示例性实施例示出的一种会话管理装置的框图。参照图5,该装置包括接收模块701,获取模块702和发送模块703。

[0134] 接收模块701,被配置为在开启无线传输功能后,接收已绑定的智能终端广播的报文;

[0135] 生成模块702,被配置为生成与报文匹配的应答消息;

[0136] 发送模块703,被配置为将应答消息返回至智能终端,应答消息用于指示智能终端与服务器进行通信的触发操作是否合法。

[0137] 在另一个实施例中,生成模块702,被配置为若报文为第一类型报文,则检测第一类型报文的信号强度,当信号强度大于预设阈值时,生成携带验证通过标识的第一应答消息,第一应答消息用于指示触发操作是否合法;若报文为第二类型报文,则根据本地存储的验证字符串,对第二类型报文中的测试字符串进行加密,得到第二应答消息,第二应答消息用于指示触发操作是否合法。

[0138] 在另一个实施例中,参见图8,获取模块704,被配置为获取智能终端的第二设备标识;

[0139] 建立模块705,被配置为建立智能穿戴设备的第一设备标识与第二设备标识之间的绑定关系。

[0140] 本公开实施例提供的装置,在开启无线传输功能后,接收已绑定的智能终端广播的报文,并生成与报文匹配的应答消息,将应答消息返回至智能终端,由智能终端在接收到已绑定智能穿戴设备返回的应答消息后,若基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识;根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险,效果较佳。

[0141] 关于上述实施例中的装置,其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述,此处将不做详细阐述说明。

[0142] 图9是根据一示例性实施例示出的一种用于会话管理的装置900的框图。例如,装置900可以是移动电话,计算机,数字广播终端,消息收发设备,游戏控制台,平板设备,医疗设备,健身设备,个人数字助理等。

[0143] 参照图9,装置900可以包括以下一个或多个组件:处理组件902,存储器904,电源组件906,多媒体组件908,音频组件910,I/O(Input/Output,输入/输出)的接口912,传感器组件914,以及通信组件916。

[0144] 处理组件902通常控制装置900的整体操作,诸如与显示,电话呼叫,数据通信,相机操作和记录操作相关联的操作。处理组件902可以包括一个或多个处理器920来执行指令,以完成上述的方法的全部或部分步骤。此外,处理组件902可以包括一个或多个模块,便

于处理组件902和其他组件之间的交互。例如,处理组件902可以包括多媒体模块,以方便多媒体组件908和处理组件902之间的交互。

[0145] 存储器904被配置为存储各种类型的数据以支持在装置900的操作。这些数据的示例包括用于在装置900上操作的任何应用程序或方法的指令,联系人数据,电话簿数据,消息,图片,视频等。存储器904可以由任何类型的易失性或非易失性存储设备或者它们的组合实现,如SRAM(Static Random Access Memory,静态随机存取存储器),EEPROM(Electrically-Erasable Programmable Read-Only Memory,电可擦除可编程只读存储器),EPROM(Erasable Programmable Read Only Memory,可擦除可编程只读存储器),PROM(Programmable Read-Only Memory,可编程只读存储器),ROM(Read-Only Memory,只读存储器),磁存储器,快闪存储器,磁盘或光盘。

[0146] 电源组件906为装置900的各种组件提供电力。电源组件906可以包括电源管理系统,一个或多个电源,及其他与为装置900生成、管理和分配电力相关联的组件。

[0147] 多媒体组件908包括在所述装置900和用户之间的提供一个输出接口的屏幕。在一些实施例中,屏幕可以包括LCD(Liquid Crystal Display,液晶显示器)和TP(Touch Panel,触摸面板)。如果屏幕包括触摸面板,屏幕可以被实现为触摸屏,以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界,而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中,多媒体组件908包括一个前置摄像头和/或后置摄像头。当装置900处于操作模式,如拍摄模式或视频模式时,前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0148] 音频组件910被配置为输出和/或输入音频信号。例如,音频组件910包括一个MIC(Microphone,麦克风),当装置900处于操作模式,如呼叫模式、记录模式和语音识别模式时,麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器904或经由通信组件916发送。在一些实施例中,音频组件910还包括一个扬声器,用于输出音频信号。

[0149] I/O接口912为处理组件902和外围接口模块之间提供接口,上述外围接口模块可以是键盘,点击轮,按钮等。这些按钮可包括但不限于:主页按钮、音量按钮、启动按钮和锁定按钮。

[0150] 传感器组件914包括一个或多个传感器,用于为装置900提供各个方面的状态评估。例如,传感器组件914可以检测到设备900的打开/关闭状态,组件的相对定位,例如组件为装置900的显示器和小键盘,传感器组件914还可以检测装置900或装置900一个组件的位置改变,用户与装置900接触的存在或不存在,装置900方位或加速/减速和装置900的温度变化。传感器组件914可以包括接近传感器,被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件914还可以包括光传感器,如CMOS(Complementary Metal Oxide Semiconductor,互补金属氧化物)或CCD(Charge-coupled Device,电荷耦合元件)图像传感器,用于在成像应用中使用。在一些实施例中,该传感器组件914还可以包括加速度传感器,陀螺仪传感器,磁传感器,压力传感器或温度传感器。

[0151] 通信组件916被配置为便于装置900和其他设备之间有线或无线方式的通信。装置

900可以接入基于通信标准的无线网络,如WiFi,2G或3G,或它们的组合。在一个示范性实施例中,通信组件916经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示范性实施例中,所述通信组件916还包括NFC(Near Field Communication,近场通信)模块,以促进短程通信。例如,在NFC模块可基于RFID(Radio Frequency Identification,射频识别)技术,IrDA(Infra-red Data Association,红外数据协会)技术,UWB(Ultra Wideband,超宽带)技术,BT(Bluetooth,蓝牙)技术和其他技术来实现。

[0152] 在示范性实施例中,装置900可以被一个或多个ASIC(Application Specific Integrated Circuit,应用专用集成电路)、DSP(Digital signal Processor,数字信号处理器)、DSPD(Digital signal Processor Device,数字信号处理设备)、PLD(Programmable Logic Device,可编程逻辑器件)、FPGA(Field Programmable Gate Array,现场可编程门阵列)、控制器、微控制器、微处理器或其他电子元件实现,用于执行上述方法。

[0153] 在示范性实施例中,还提供了一种包括指令的非临时性计算机可读存储介质,例如包括指令的存储器904,上述指令可由装置900的处理器920执行以完成上述方法。例如,所述非临时性计算机可读存储介质可以是ROM、RAM(Random Access Memory,随机存取存储器)、CD-ROM(Compact Disc Read-Only Memory,光盘只读存储器)、磁带、软盘和光数据存储设备等。

[0154] 一种非临时性计算机可读存储介质,当所述存储介质中的指令由移动终端的处理器执行时,使得移动终端能够执行一种会话管理方法,所述方法包括:

[0155] 若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文;

[0156] 若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识;

[0157] 根据会话标识与服务器进行通信。

[0158] 在另一个实施例中,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,包括:

[0159] 在广播第一类型报文后,若接收到已绑定智能穿戴设备返回的第一应答消息,则检测第一应答消息中是否携带验证通过标识;

[0160] 若第一应答消息中携带验证通过标识,则确定触发操作合法,获取本地存储的与服务器进行通信的会话标识;

[0161] 其中,验证通过标识,用于表示已绑定智能穿戴设备接收到的第一类型报文的信号强度大于预设阈值,信号强度的数值越大,已绑定智能穿戴设备与智能终端之间的距离越小。

[0162] 在另一个实施例中,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,包括:

[0163] 在广播第二类型报文后,若接收到已绑定智能穿戴设备返回的第二应答消息,则获取本地存储的验证字符串;

[0164] 根据验证字符串对第二类型报文中的测试字符串进行加密,得到加密信息;

[0165] 若第二应答消息与加密信息一致,则确定第二应答消息由已绑定智能穿戴设备返



回,触发操作合法,获取本地存储的与服务器进行通信的会话标识;

[0166] 其中,验证字符串由已绑定智能穿戴设备预先发送至智能终端,已绑定智能穿戴设备用于根据验证字符串对测试字符串进行加密,得到第二应答消息。

[0167] 在另一个实施例中,该方法还包括:

[0168] 获取智能穿戴设备的第一设备标识;

[0169] 建立第一设备标识与智能终端的第二设备标识之间的绑定关系。

[0170] 本公开实施例提供的非临时性计算机可读存储介质,若检测到与服务器进行通信的触发操作,则在开启无线传输功能后广播报文,若接收到已绑定智能穿戴设备基于报文返回的应答消息,且基于应答消息判断出触发操作合法,则获取本地存储的与服务器进行通信的会话标识,根据会话标识与服务器进行通信。由于在会话管理过程中,基于智能穿戴设备对发起通信操作的用户进行了身份验证,仅在用户通过身份验证后方可获取到存储在智能终端上的会话标识,所以即便智能终端不在用户本人身边,或者智能终端被第三方获取到,第三方也不会拿到存储在智能终端上的会话标识,因此避免了因会话标识被第三方获取而造成用户隐私泄露的风险,效果更佳。

[0171] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本发明的真正范围和精神由下面的权利要求指出。

[0172] 应当理解的是,本发明并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限制。

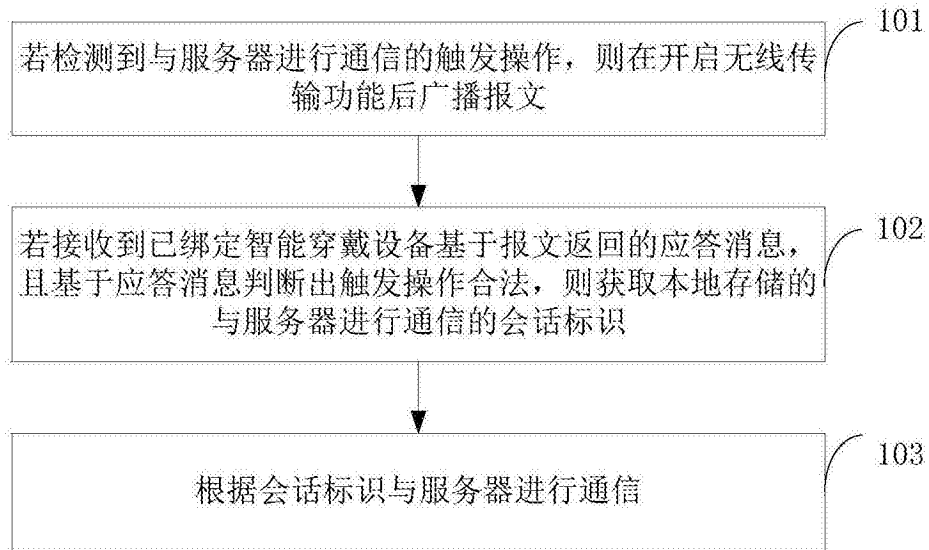


图1

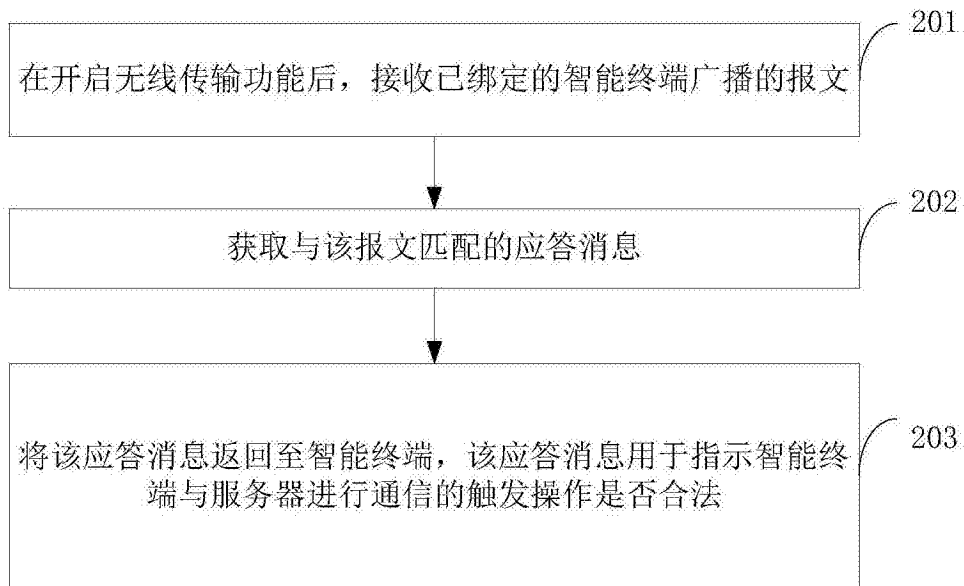


图2

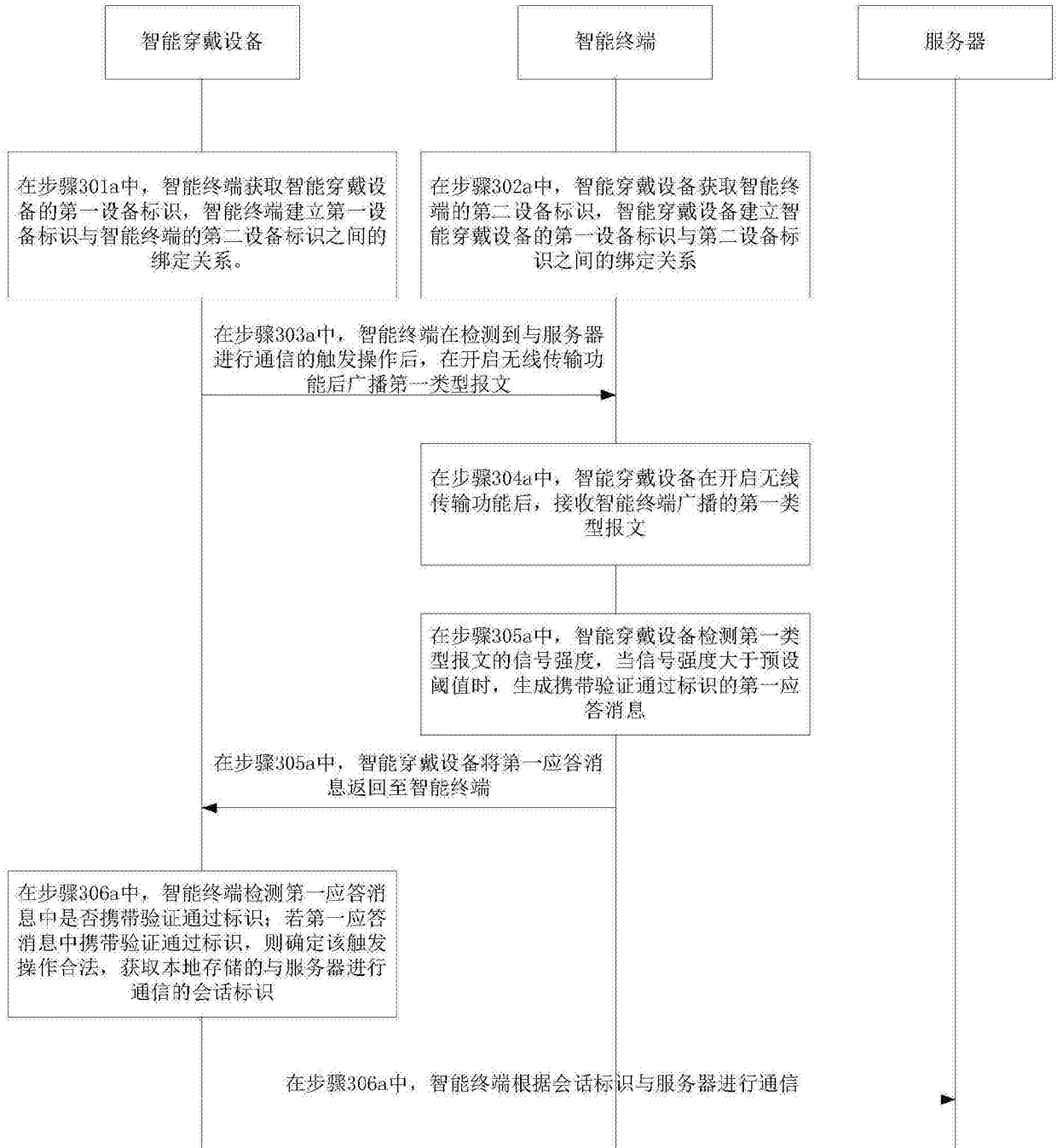


图3A

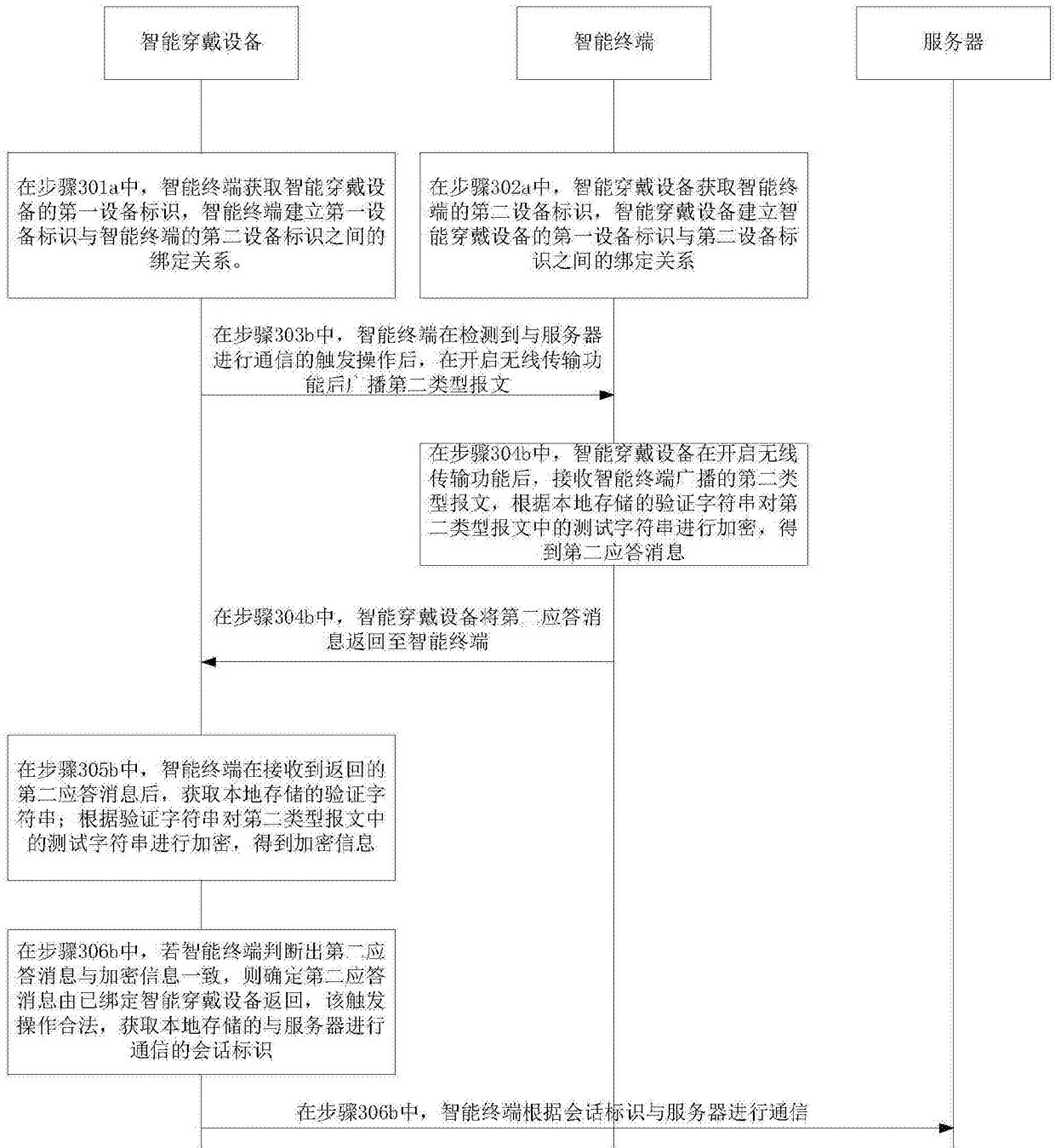


图3B

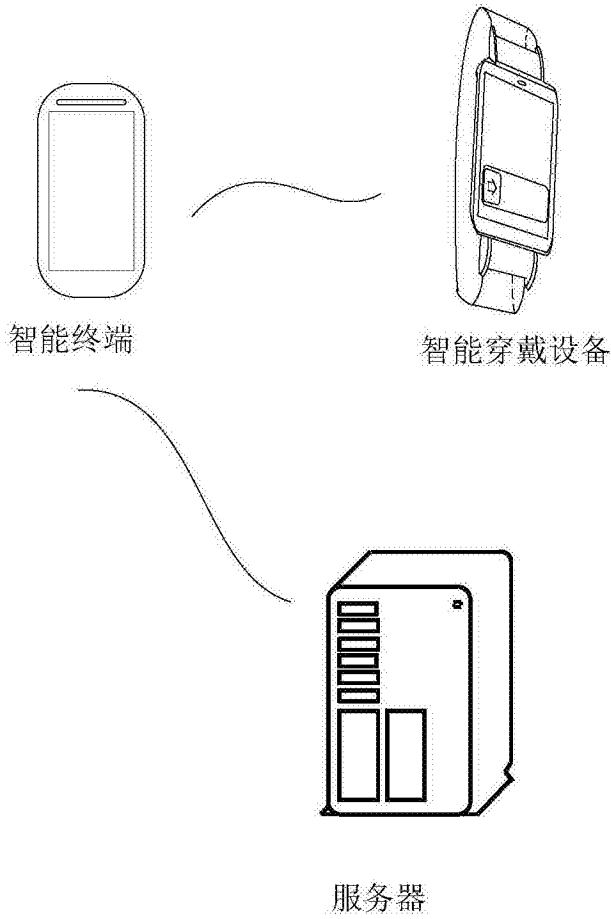


图4

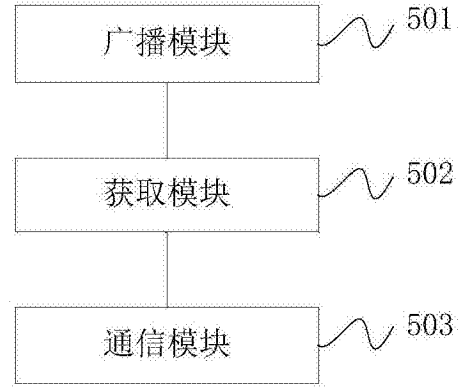


图5

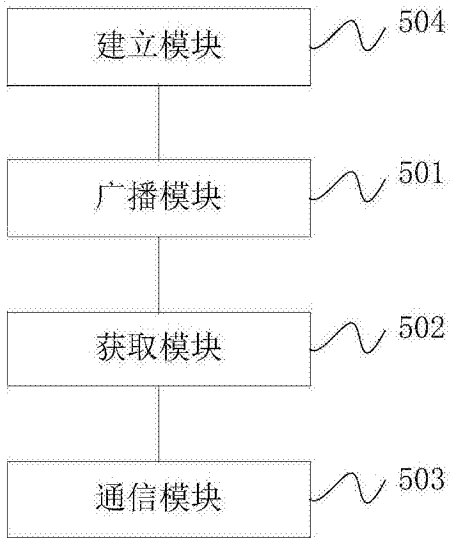


图6

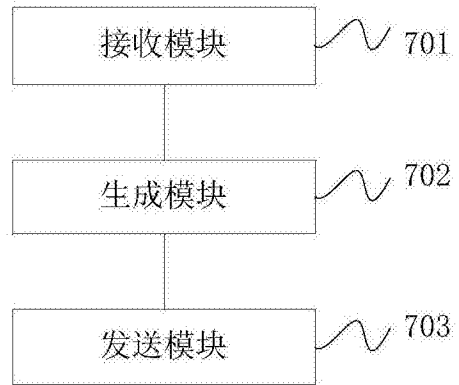


图7

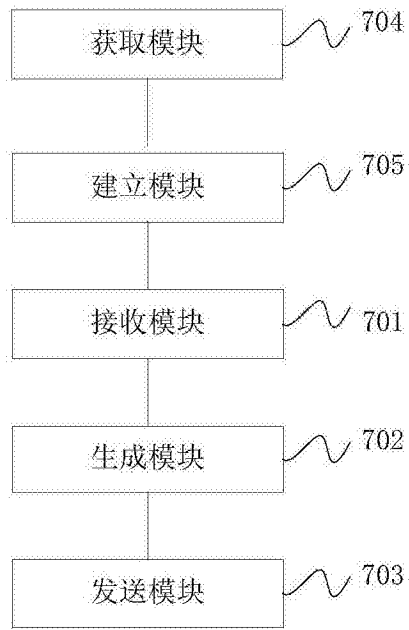


图8

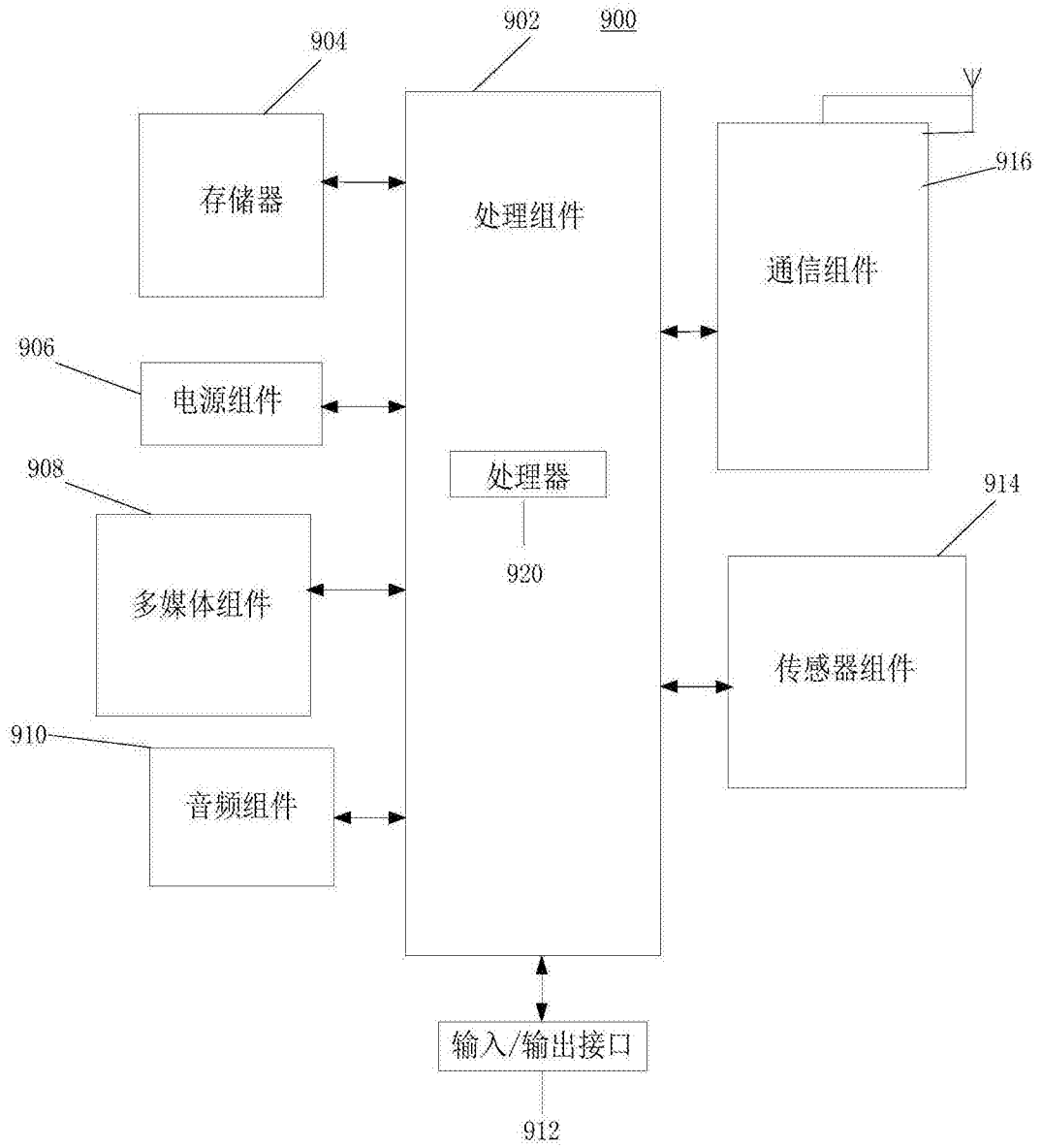


图9