(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104159225 A
(43)申请公布日 2014.11.19

(21)申请号 201410442929.X

(22)申请日 2014.09.02

(71)申请人 解芳
地址 100041 北京市石景山区北方工业大学15-8-401

(72)发明人 解芳

(74)专利代理机构 北京天奇智新知识产权代理有限公司 11340
代理人 谢磊

(51)Int.Cl.
H04W 12/06(2009.01)
H04W 24/00(2009.01)

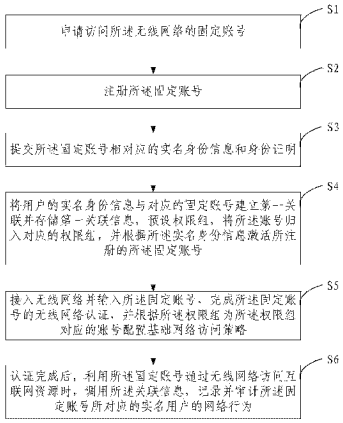
权利要求书2页 说明书8页 附图5页

(54)发明名称

一种基于无线网络的实名制管理方法及系统

(57)摘要

本发明公开了一种基于无线网络的实名制管理方法及系统，所述方法包括：申请并注册固定账号，提交所述固定账号相对应的实名身份信息和身份证明，并将用户的实名身份信息与对应的固定账号建立关联并存储关联信息，将账号归入对应的预设权限组，根据实名身份信息激活固定账号；接入无线网络并完成所述固定账号的无线网络认证；认证完成后，利用固定账号通过无线网络访问互联网资源时，调用关联信息，记录并审计所述固定账号所对应的实名用户的网络行为。本发明在实现安全、完整的实名认证安全性的基础上，对用户行为进行审计，并可为用户提供差异化服务，提高用户体验，同时具备网络安全策略相关的访问控制功能，以利于无线网络的商业模式扩展。



CN 104159225 A

1. 一种基于无线网络的实名制管理方法，其特征在于，所述方法包括：

步骤 S1，申请访问所述无线网络的固定账号；

步骤 S2，注册所述固定账号；

步骤 S3，提交所述固定账号相对应的实名身份信息和身份证明；

步骤 S4，将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的所述固定账号；

步骤 S5，接入无线网络并输入所述固定账号，完成所述固定账号的无线网络认证，并根据所述权限组为所述权限组对应的账号配置基础网络访问策略；

步骤 S6，认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述关联信息，记录并审计所述固定账号所对应的实名用户的网络行为。

2. 根据权利要求 1 所述实名制管理方法，其特征在于，所述方法还包括：

步骤 S7，认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的 IP 地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略。

3. 根据权利要求 1 或 2 所述的实名制管理方法，其特征在于，所述步骤 S4 还包括：根据用户的实名身份信息及身份证明对所对应的所述固定账号进行有效期分组，将所述固定账号分为长期用户组和短期用户组。

4. 根据权利要求 3 所述的实名制管理方法，其特征在于，所述长期用户组的用户的实名身份信息至少包括：身份证信息或户口本信息或护照信息、工作证信息或房屋产权证明；所述长期用户组用户的固定账号的有效期为工作证或房屋产权证有效期的期限；

所述短期用户组的用户的实名身份信息至少包括：身份证信息或户口本信息或护照信息、工作证信息或房屋租赁证明；所述短期用户组用户的固定账号的有效期为预先设置的有效期，所述固定账号在预先设置的有效期到期后失效或进行续期。

5. 根据权利要求 4 所述的实名制管理方法，其特征在于，所述方法还包括：

步骤 S8，通过认证成功的所述固定账号申请一个或多个临时账号；

步骤 S9，根据申请为所述临时账号开户，将申请所述临时账号的所述固定账号所对应的实名身份信息与所述临时账号建立第二关联并存储第二关联信息，并设置所述临时账号的有效期；

步骤 10，接入无线网络并输入所述临时账号，完成所述临时账号的无线网络认证，并为所述临时账号配置基础网络访问策略；

步骤 S11，认证完成后，利用所述临时账号通过无线网络访问互联网资源时，调用所述第二关联信息，记录并审计所述临时账号所对应的实名用户的网络行为。

6. 根据权利要求 5 所述实名制管理方法，其特征在于，所述方法还包括：

步骤 S12，认证完成后，利用所述临时账号通过无线网络访问网络资源时，将用户当前的 IP 地址与所述第二关联信息相对应，根据所述对应关系为所述临时账号配置用户网络访问策略。

7. 根据权利要求 5 所述实名制管理方法，其特征在于，所述方法还包括：

步骤 S13，将超过有效期的所述临时账号进行销户。

8. 一种基于无线网络的实名制管理系统，其特征在于，所述系统包括：

账号申请模块，用于提交申请访问所述无线网络的固定账号的申请，并用于提交所述固定账号相对应的实名身份信息和身份证明；

账号注册模块，与所述账号申请模块相连，用于注册所述固定账号；

账号管理模块，将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的所述固定账号；

用户登录模块，用于输入所述固定账号，并将所述固定账号发送给网络模块；

网络模块，与用户登录模块相连，用于接收所述用户登录模块所发送的固定账号，并向认证后台模块发起对所述固定账号的无线网络认证；同时用于提供接入无线网络的接口；

认证后台模块，与账号注册模块、账号管理模块、网络模块相连，用于存储所述账号注册模块所注册的固定账号，存储账号管理模块所建立的第一关联信息及所预设的权限组，并用于完成对所述固定账号的无线网络认证，并根据所述权限组、第一关系信息为所述权限组对应的账号配置基础网络访问策略；

网络行为审计模块，与认证登录模块相连，用于认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述第一关联信息，记录并审计所述固定账号所对应的实名用户的网络行为。

9. 根据权利要求 8 所述的实名制管理系统，其特征在于，所述系统还包括：

访问策略管理模块，与所述认证后台模块相连，用于认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的 IP 地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略。

10. 根据权利要求 8 或 9 所述的实名制管理系统，其特征在于，

所述账号申请模块还用于利用无线网络认证成功的所述固定账号申请一个或多个临时账号；

所述账号注册模块还用于根据用户的申请为所述临时账号开户；

所述账号管理模块还用于将申请所述临时账号的所述固定账号所对应的实名身份信息与所述临时账号建立第二关联并存储第二关联信息，并设置所述临时账号的有效期；

所述用户登录模块还用于输入所述临时账号，并将所述临时账号发送给网络模块；

所述网络模块还用于接收所述用户登录模块所发送的临时账号，并向认证后台模块发起对所述临时账号的无线网络认证；同时用于提供接入无线网络的接口；

所述认证后台模块还用于完成所述临时账号的无线网络认证；

所述网络行为审计模块还用于认证完成后，利用所述临时账号通过无线网络访问互联网资源时，调用所述第二关联信息，记录并审计所述临时账号所对应的实名用户的网络行为；

所述系统还包括：临时账号销户模块，与认证后台模块相连，用于将超过有效期的所述临时账号进行销户。

一种基于无线网络的实名制管理方法及系统

技术领域

[0001] 本发明涉及无线网络技术，特别是涉及一种基于无线网络的实名制管理方法及系统。

背景技术

[0002] 随着科技的发展，无线网络技术日益完善，各种随身上网设备也日益普及，如智能手机、平板电脑等设备可以实现无线上网，因此无线上网成为了大众的需求。目前，餐厅、咖啡店、商场、酒店、机场、车站等公共场所都向公众提供无线上网服务。另外，由于无线上网无需庞大的网络线路架构，也越来越多的应用在住宅小区、企业等领域。

[0003] 通常接入无线网络时需要进行网络认证，现有的网络认证方式包括固定密码认证方式和手机短信认证方式。固定密码认证方式，适用于咖啡馆、餐厅等中小面积公共场所，是最简单和方便的认证方式，所有的用户共享一个密码，密码通常存储在网络设备本地。用户使用终端搜索到无线网络的服务集标识 (Service Set Identifier, SSID)，点击连接并输入密码后即可完成认证。手机短信密码认证方式，适用于商场、火车站等较大面积公共场所。用户使用终端接入无线网络时只有访问门户 (Portal) 认证页面权限，用户访问 portal 认证页面输入手机号码，Portal 服务器随机生成密码，并将密码发送至用户手机，用户输入密码后完成网络认证并获得 Internet 访问权限。

[0004] 以上所述的无线网络的固定密码认证方式不属于实名制认证方式，而手机短信认证方式由于我国存在大量非实名制手机号码，因此也不是完全的实名制认证方式。

[0005] 这两种无线网络认证方式都不属于网络实名认证，在实际运用过程中存在以下两点的缺陷：第一，不符合公安部 82 号令对于网络信息安全方面的有关要求，无法对用户的网络操作进行行为审计，出现信息安全事件后，网络管理责任无法落实，将造成司法证据链不完整；第二，无法对无线网络用户身份进行识别，无法对用户提供诸如网络带宽保障与限制、网络访问策略限制等差异化网络服务，无法满足不同层次用户的网络需求。

发明内容

[0006] 本发明的目的是提供一种基于无线网络的实名制管理方法及系统，对用户行为进行审计，实现安全、完整的实名认证，并可为用户提供差异化服务，提高用户体验，同时具备网络安全策略相关的访问控制功能，以利于无线网络的商业模式扩展。

[0007] 根据本发明的一个方面，提供了一种基于无线网络的实名制管理方法，所述方法包括：

[0008] 步骤 S1，申请访问所述无线网络的固定账号；

[0009] 步骤 S2，注册所述固定账号；

[0010] 步骤 S3，提交所述固定账号相对应的实名身份信息和身份证明；

[0011] 步骤 S4，将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的

所述固定账号；

[0012] 步骤 S5，接入无线网络并输入所述固定账号，完成所述固定账号的无线网络认证，并根据所述权限组为所述权限组对应的账号配置基础网络访问策略；

[0013] 步骤 S6，认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述关联信息，记录并审计所述固定账号所对应的实名用户的网络行为。

[0014] 其中，上述方案中，所述方法还包括：

[0015] 步骤 S7，认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的 IP 地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略。

[0016] 其中，上述方案中，所述步骤 S4 还包括：根据用户的实名身份信息及身份证明对所对应的所述固定账号进行有效期分组，将所述固定账号分为长期用户组和短期用户组。

[0017] 其中，上述方案中，所述长期用户组的用户的实名身份信息至少包括：、身份证信息或户口本信息或护照信息、工作证信息或房屋产权证明；所述长期用户组用户的固定账号的有效期为工作证或房屋产权证有效期的期限；

[0018] 所述短期用户组的用户的实名身份信息至少包括：身份证信息或户口本信息或护照信息、工作证信息或房屋租赁证明；所述短期用户组用户的固定账号的有效期为预先设置的有效期，所述固定账号在预先设置的有效期到期后失效或进行续期。

[0019] 其中，上述方案中，所述方法还包括：

[0020] 步骤 S8，通过认证成功的所述固定账号申请一个或多个临时账号；

[0021] 步骤 S9，根据申请为所述临时账号开户，将申请所述临时账号的所述固定账号所对应的实名身份信息与所述临时账号建立第二关联并存储第二关联信息，并设置所述临时账号的有效期；

[0022] 步骤 10，接入无线网络并输入所述临时账号，完成所述临时账号的无线网络认证，并为所述临时账号配置基础网络访问策略；

[0023] 步骤 S11，认证完成后，利用所述临时账号通过无线网络访问互联网资源时，调用所述第二关联信息，记录并审计所述临时账号所对应的实名用户的网络行为。

[0024] 其中，上述方案中，所述方法还包括：

[0025] 步骤 S12，认证完成后，利用所述临时账号通过无线网络访问网络资源时，将用户当前的 IP 地址与所述第二关联信息相对应，根据所述对应关系为所述临时账号配置用户网络访问策略。

[0026] 其中，上述方案中，所述方法还包括：

[0027] 步骤 S13，将超过有效期的所述临时账号进行销户。

[0028] 根据本发明的另一个方面，本发明还提供了一种基于无线网络的实名制管理系统，所述系统包括：

[0029] 账号申请模块，用于提交申请访问所述无线网络的固定账号的申请，并用于提交所述固定账号相对应的实名身份信息和身份证明；

[0030] 账号注册模块，与所述账号申请模块相连，用于注册所述固定账号；

[0031] 账号管理模块，将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所

注册的所述固定账号；

[0032] 用户登录模块，用于输入所述固定账号，并将所述固定账号发送给网络模块；

[0033] 网络模块，与用户登录模块相连，用于接收所述用户登录模块所发送的固定账号，并向认证后台模块发起对所述固定账号的无线网络认证；同时用于提供接入无线网络的接口；

[0034] 认证后台模块，与账号注册模块、账号管理模块、网络模块相连，用于存储所述账号注册模块所注册的固定账号，存储账号管理模块所建立的第一关联信息及所预设的权限组，并用于完成对所述固定账号的无线网络认证，并根据所述权限组、第一关系信息为所述权限组对应的账号配置基础网络访问策略；

[0035] 网络行为审计模块，与认证登录模块相连，用于认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述第一关联信息，记录并审计所述固定账号所对应的实名用户的网络行为。

[0036] 其中，上述方案中，所述系统还包括：

[0037] 访问策略管理模块，与所述认证后台模块相连，用于认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的 IP 地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略。

[0038] 其中，上述方案中，所述账号申请模块还用于利用无线网络认证成功的所述固定账号申请一个或多个临时账号；

[0039] 所述账号注册模块还用于根据用户的申请为所述临时账号开户；

[0040] 所述账号管理模块还用于将申请所述临时账号的所述固定账号所对应的实名身份信息与所述临时账号建立第二关联并存储第二关联信息，并设置所述临时账号的有效期；

[0041] 所述用户登录模块还用于输入所述临时账号，并将所述临时账号发送给网络模块；

[0042] 所述网络模块还用于接收所述用户登录模块所发送的临时账号，并向认证后台模块发起对所述临时账号的无线网络认证；同时用于提供接入无线网络的接口；

[0043] 所述认证后台模块还用于完成所述临时账号的无线网络认证；

[0044] 所述网络行为审计模块还用于认证完成后，利用所述临时账号通过无线网络访问互联网资源时，调用所述第二关联信息，记录并审计所述临时账号所对应的实名用户的网络行为；

[0045] 所述系统还包括：临时账号销户模块，与认证后台相连，用于将超过有效期的所述临时账号进行销户。

[0046] 本发明所提供的基于无线网络的实名制管理方法及系统，所述方法包括：申请访问所述无线网络的固定账号；注册所述固定账号；提交所述固定账号相对应的实名身份信息和身份证明；并将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的所述固定账号；接入无线网络并输入所述固定账号，完成所述固定账号的无线网络认证，并根据所述权限组为所述权限组对应的账号配置基础网络访问策略；认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述关联信息，记录并审计所述固定账号

所对应的实名用户的网络行为。本发明在实名认证的基础上对用户行为进行审计，在实现安全、完整的实名认证安全性的基础上，并可为用户提供差异化服务，提高用户体验，同时具备网络安全策略相关的访问控制功能，以利于无线网络的商业模式扩展。

附图说明

[0047] 图 1 是本发明第一实施例的基于无线网络的实名制管理方法流程图；

[0048] 图 2 是图 1 所示的步骤 S5 的固定账号的无线网络认证流程图；

[0049] 图 3 是本发明第二实施例的基于无线网络的实名制管理方法流程图；

[0050] 图 4 是本发明第三实施例的基于无线网络的实名制管理方法流程图；

[0051] 图 5 是本发明的基于无线网络的实名制管理系统的结构示意图。

具体实施方式

[0052] 为使本发明的目的、技术方案和优点更加清楚明了，下面结合具体实施方式并参照附图，对本发明进一步详细说明。应该理解，这些描述只是示例性的，而并非要限制本发明的范围。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本发明的概念。

[0053] 图 1 是本发明第一实施例的基于无线网络的实名制管理方法流程图。

[0054] 如图 1 所示，本实施例所提供的一种基于无线网络的实名制管理方法，包括：

[0055] 步骤 S1，申请访问所述无线网络的固定账号。

[0056] 本步骤中，用户可以通过 portal 页面或移动终端应用软件 APP 来申请固定账号，固定账号信息至少包括用户名和密码，通常情况下由用户根据自己的需要进行设定，并通过通过 portal 页面或移动终端 APP 提交给 portal 服务器或 APP 服务器。

[0057] 步骤 S2，注册所述固定账号。

[0058] 本步骤中，portal 服务器或 APP 服务器接收到用户提交的需要进行注册的固定账号后，在 LDAP 服务器上对固定账号进行注册并对所注册的固定账号进行存储。这里的 LDAP 服务器与固定账号激活后进行实名认证相关联的，也就是说，进行实名认证时，可直接从 LDAP 服务器中调取与固定账号相关的已存储的信息。

[0059] LDAP 服务器可用其它数据库或 Radius 服务器替代，由于 LDAP 服务器相对其它数据库具有在大数据量的情况下查询速度快、分布式部署方便的优点，所以一般用数据库做日常管理和存储，用 LDAP 服务器做查询认证。

[0060] 步骤 S3，提交所述固定账号相对应的实名身份信息和身份证明。

[0061] 本步骤中，用户提交与所注册的固定账号相关的自身的实名身份信息和身份证明。这里的身份信息，至少包括用户的身份证信息或护照信息或户口本信息或其他可以证明用户身份的信息、工作证信息或房屋产权证信息或房屋租赁证信息，还可以包括联系方式如手机号码等，可以通过远程网络的方式或其他可信的方式提交给账号管理系统或管理员；身份证明至少包括工作证明或房屋产权证明或房屋租赁证明，可以通过远程网络的方式或邮寄或当面提交的方式将上述证明的扫描件或复印件提交给账号管理系统或管理员。

[0062] 步骤 S4，将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的

所述固定账号。

[0063] 本步骤中，账号管理系统或管理员接收到用户所提交的实名身份信息和身份证明后，将步骤S2中在LDAP服务器中所注册固定账号与用户的实名身份信息建立第一关联，并相应存储所建立的第一关联信息，这里的存储与固定账号信息的存储相类似，也是与固定账号激活后进行实名认证相关联的，也就是说，进行实名认证时，可直接从LDAP服务器中调取这里的第一关联信息。

[0064] 同时预设权限组，权限组的预设可以在固定账号申请前进行，也就是说，在用户进行固定账号的申请前，就已经存在权限组，用户申请并注册完成后，由账号管理系统或管理员，根据固定账号所对应的实名身份信息或用户的需求将固定账号分配到不同的权限组中。例如，可以预设A公司员工固定账号权限组，B小区居民固定账号权限组。另外，也可以根据用户的个性化需求，如用户根据自身需求进行购买服务方式进行分入其它的也个性化用户组。分组完成后，将所述固定账号激活，并通知申请所述固定账号的用户。

[0065] 本步骤中，还可以根据用户的实名身份信息及身份证明对所对应的所述固定账号进行有效期分组，将所述固定账号分为长期用户组和短期用户组。所述长期用户组的用户的实名身份信息至少包括：身份证信息或户口本信息或护照信息、工作证信息或房屋产权证明；所述长期用户组用户的固定账号的有效期为工作证或房屋产权证有效期的期限；所述短期用户组的用户的实名身份信息至少包括：身份证信息或户口本信息或护照信息、工作证信息或房屋租赁证明；所述短期用户组用户的固定账号的有效期为预先设置的有效期，所述固定账号在预先设置的有效期到期后失效或进行续期。这里预先设置的有效期，可以是用户所提交的工作证或房屋租赁证明的有效期，也可以是用户根据自己的需要设定的有效期，有效期到期后固定账号即失效，若用户还需使用这一固定账号，则在规定的时间内进行续期，则所述固定账号可继续使用，直到续期的有效期到期。

[0066] 步骤S5，接入无线网络并输入所述固定账号，完成所述固定账号的无线网络认证，并根据所述权限组为所述权限组对应的账号配置基础网络访问策略；

[0067] 本步骤中，账号激活后，用户接收到账号激活的通知，接入无线网络，此时，用户对所述无线网络具有基本的访问权限，包括允许访问基本网络服务DHCP和DNS、允许授权移动终端APP接入APP服务器、允许访问Portal认证服务器等。此时，用户登录portal页面或移动终端APP，并输入固定账号，包括固定账号的用户名和密码，所述固定账号通过无线网络提交给用于无线网络认证的服务器，这里用于无线网络认证的服务器通常指的是Radius服务器，Radius服务器调用LDAP服务器中存储的所述固定账号及相关信息，完成对固定账号的网络认证。

[0068] 这里，由于LDAP服务器在账号管理方面具有更加灵活的优点，如邮件和/或其他OA系统的账号管理都可以使用LDAP，也可以实现账号的统一管理，因此，所述固定账号一般由LDAP服务器进行存储。在网络认证的过程中，Radius服务器接收到认证请求后，向LDAP服务器发出查询请求，查询与认证请求相关的固定账号及其相关信息，完成认证。

[0069] 步骤S6，认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述关联信息，记录并审计所述固定账号所对应的实名用户的网络行为。

[0070] 本步骤中，用户通过所述认证完成后的固定账号访问网络资源时，网络审计系统或设备调用认证系统的服务器如Radius服务器的设备查询接口，获取所述用户的IP地址

与用户账号、用户实名身份信息的真实对应关系，对用户的网络行为进行记录。

[0071] 图 2 是图 1 中步骤 S5 的固定账号的无线网络认证流程图。

[0072] 参见图 2，用户根据所述固定账号及所述认证前的访问权限，访问所述无线网络，完成固定账号的无线网络认证，其中，步骤 S5 中用户完成固定账号的无线网络认证步骤如下：

[0073] 步骤 S51，用户使用浏览器或使用授权移动终端 APP 访问 Portal 认证页面，输入所述固定账号的用户名和密码，启动网络认证。

[0074] 步骤 S52，Portal 服务器或 APP 服务器将所述固定账号的用户名和密码组装成认证请求报文并将所述认证请求报文发送给网络接入设备。

[0075] 步骤 S53，网络接入设备与认证后台模块之间进行 Radius 协议报文的交互并验证所述认证请求报文的用户名、密码以及网络访问期限。

[0076] 步骤 S54，网络接入设备向 Portal 服务器或 APP 服务器发送认证应答报文。

[0077] 步骤 S55，Portal 服务器或 APP 服务器向用户发送认证通过报文，通知用户网络认证成功，并向网络接入设备发送认证应答确认报文。

[0078] 步骤 S56，网络接入设备允许用户访问被管理员授权的无线网络资源。

[0079] 图 3 是本发明第二实施例的基于无线网络的实名制管理方法流程图。

[0080] 如图 3 所示，本实施例的基于无线网络的实名制管理方法，除包括图 1 所示的步骤 S1 至步骤 S6 外，还包括：

[0081] 步骤 S7，认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的 IP 地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略。

[0082] 本实施例中，通过步骤 S6 和步骤 S7，在实现安全、完整的实名认证安全性的基础上，对用户行为进行审计，并可为用户提供差异化服务，提高用户体验，同时具备网络安全策略相关的访问控制功能，以利于无线网络的商业模式扩展。

[0083] 图 4 是本发明第三实施例的基于无线网络的实名制管理方法流程图。

[0084] 如图 4 所示，本实施例的基于无线网络的实名制管理方法，除包括图 3 所示的步骤 S1 至步骤 S7，还包括：

[0085] 步骤 S8，通过认证成功的所述固定账号申请一个或多个临时账号。

[0086] 步骤 S9，根据申请为所述临时账号开户，将申请所述临时账号的所述固定账号所对应的实名身份信息与所述临时账号建立第二关联并存储第二关联信息，并设置所述临时账号的有效期。

[0087] 本步骤中，所述为临时账号开户，可以在 Radius 服务器中进行。

[0088] 步骤 10，接入无线网络并输入所述临时账号，完成所述临时账号的无线网络认证，并为所述临时账号配置基础网络访问策略。

[0089] 本步骤中，在网络认证的过程中，Radius 服务器接收到认证请求后，由于临时账户可以直接在 Radius 服务器中开户，从而不需要 Radius 服务器向 LDAP 服务器发出查询请求，而 Radius 服务器直接调用其自身存储的临时账号及相关信息，由完成认证。如此，简化了认证程序。

[0090] 由于此时的账号占用了 Radius 服务器的资源，需要对定期对临时账号进行销户，

以避免占用过多 Radius 服务器系统资源，即步骤 S13。

[0091] 步骤 S11，认证完成后，利用所述临时账号通过无线网络访问互联网资源时，调用所述第二关联信息，记录并审计所述临时账号所对应的实名用户的网络行为。

[0092] 本实施例还可以包括：

[0093] 步骤 S12，认证完成后，利用所述临时账号通过无线网络访问网络资源时，将用户当前的 IP 地址与所述第二关联信息相对应，根据所述对应关系为所述临时账号配置用户网络访问策略。

[0094] 步骤 S13，将超过有效期的所述临时账号进行销户。图 5 是本发明优选实施例的基于无线网络的实名制管理系统的结构示意图。

[0095] 如图 5 所示，本实施例提供了一种基于无线网络的实名制管理系统，所述系统包括：

[0096] 账号申请模块 101，用于提交申请访问所述无线网络的固定账号的申请，并用于提交所述固定账号相对应的实名身份信息和身份证明。

[0097] 这里的申请模块 101 还用于利用无线网络认证成功的所述固定账号申请一个或多个临时账号。

[0098] 账号注册模块 102，与所述账号申请模块 101 相连，用于注册所述固定账号。

[0099] 这里的账号注册模块 102 还用于根据用户的申请为所述临时账号开户。

[0100] 账号管理模块 103，将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的所述固定账号。

[0101] 这里的账号管理模块 103 还用于将申请所述临时账号的所述固定账号所对应的实名身份信息与所述临时账号建立第二关联并存储第二关联信息，并设置所述临时账号的有效期。

[0102] 用户登录模块 104，用于输入所述固定账号，并将所述固定账号发送给网络模块 105。

[0103] 这里的用户登录模块 104 还用于输入所述临时账号，并将所述临时账号发送给网络模块 105。

[0104] 网络模块 105，与用户登录模块 104 相连，用于接收所述用户登录模块 104 所发送的固定账号，并向认证后台模块 106 发起对所述固定账号的无线网络认证；同时用于提供接入无线网络的接口。

[0105] 这里的网络模块 105 还用于接收所述用户登录模块 104 所发送的临时账号，并向认证后台模块 106 发起对所述临时账号的无线网络认证；同时用于提供接入无线网络的接口。

[0106] 认证后台模块 106，与账号注册模块 102、账号管理模块 103、网络模块 105 相连，用于存储所述账号注册模块 103 所注册的固定账号，存储账号管理模块 104 所建立的第一关联信息及所预设的权限组，并用于完成对所述固定账号的无线网络认证，并根据所述权限组、第一关系信息为所述权限组对应的账号配置基础网络访问策略。

[0107] 这里的认证后台模块 106 还用于完成所述临时账号的无线网络认证。

[0108] 网络行为审计模块 107，与所述认证后台模块 106 相连，用于认证完成后，利用所

述固定账号通过无线网络访问互联网资源时，调用所述第一关联信息，记录并审计所述固定账号所对应的实名用户的网络行为。

[0109] 这里的网络行为审计模块 107，还用于临时账号的认证完成后，利用所述临时账号通过无线网络访问互联网资源时，调用所述第二关联信息，记录并审计所述临时账号所对应的实名用户的网络行为。

[0110] 访问策略管理模块 108，与所述认证后台模块 106 相连，用于认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的 IP 地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略。

[0111] 这里的访问策略管理模块 108 还用于临时账号的认证完成后，利用所述临时账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的 IP 地址与所述第二关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略。

[0112] 进一步的，所述系统还可以包括：

[0113] 临时账号销户模块 109，与认证后台模块 106 相连，用于将超过有效期的所述临时账号进行销户。

[0114] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤和系统或模块可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括存储器、磁盘或光盘等。

[0115] 应当理解的是，本发明的上述具体实施方式仅仅用于示例性说明或解释本发明的原理，而不构成对本发明的限制。因此，在不偏离本发明的精神和范围的情况下所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。此外，本发明所附权利要求旨在涵盖落入所附权利要求范围和边界、或者这种范围和边界的等同形式内的全部变化和修改例。

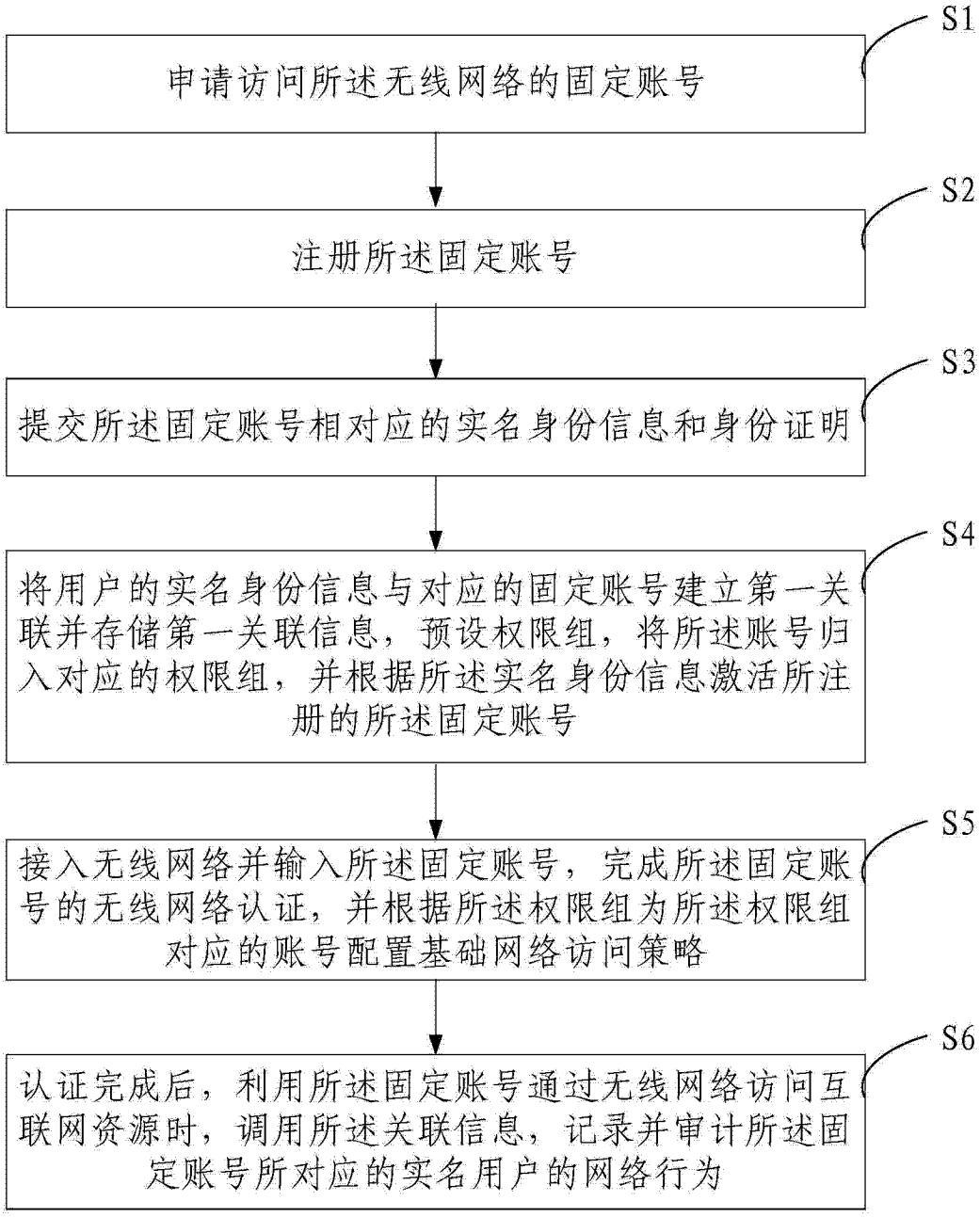

S1
申请访问所述无线网络的固定账号
S2
注册所述固定账号
S3
提交所述固定账号相对应的实名身份信息和身份证明
S4
将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的所述固定账号
S5
接入无线网络并输入所述固定账号，完成所述固定账号的无线网络认证，并根据所述权限组为所述权限组对应的账号配置基础网络访问策略
S6
认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述关联信息，记录并审计所述固定账号所对应的实名用户的网络行为

图 1

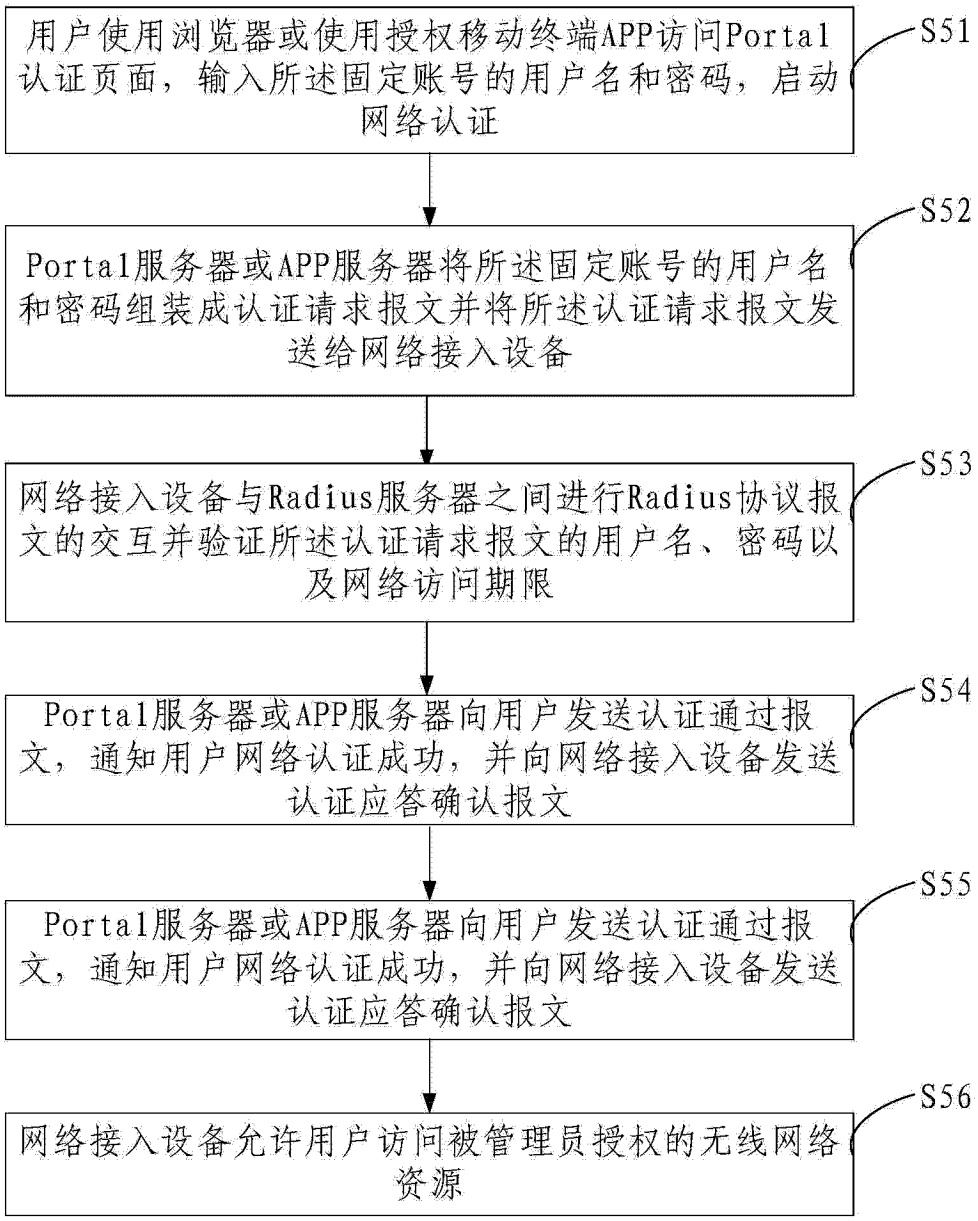

用户使用浏览器或使用授权移动终端APP访问Portal认证页面，输入所述固定账号的用户名和密码，启动网络认证
S51
Portal服务器或APP服务器将所述固定账号的用户名和密码组装成认证请求报文并将所述认证请求报文发送给网络接入设备
S52
网络接入设备与Radius服务器之间进行Radius协议报文的交互并验证所述认证请求报文的用户名、密码以及网络访问期限
S53
Portal服务器或APP服务器向用户发送认证通过报文，通知用户网络认证成功，并向网络接入设备发送认证应答确认报文
S54
Portal服务器或APP服务器向用户发送认证通过报文，通知用户网络认证成功，并向网络接入设备发送认证应答确认报文
S55
网络接入设备允许用户访问被管理员授权的无线网络资源
S56

图 2

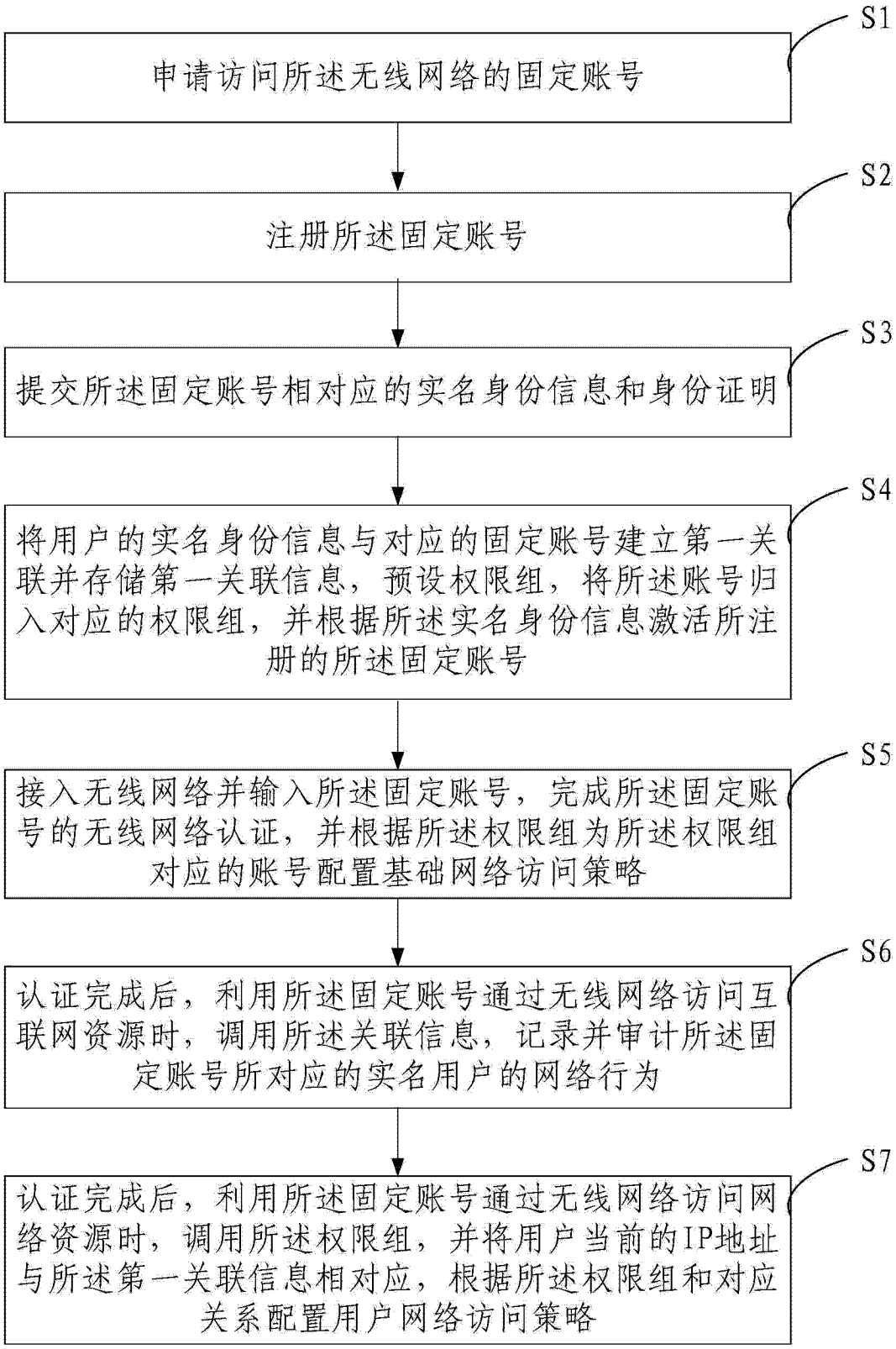

S1
申请访问所述无线网络的固定账号
S2
注册所述固定账号
S3
提交所述固定账号相对应的实名身份信息和身份证明
S4
将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的所述固定账号
S5
接入无线网络并输入所述固定账号，完成所述固定账号的无线网络认证，并根据所述权限组为所述权限组对应的账号配置基础网络访问策略
S6
认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述关联信息，记录并审计所述固定账号所对应的实名用户的网络行为
S7
认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的IP地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略

图 3

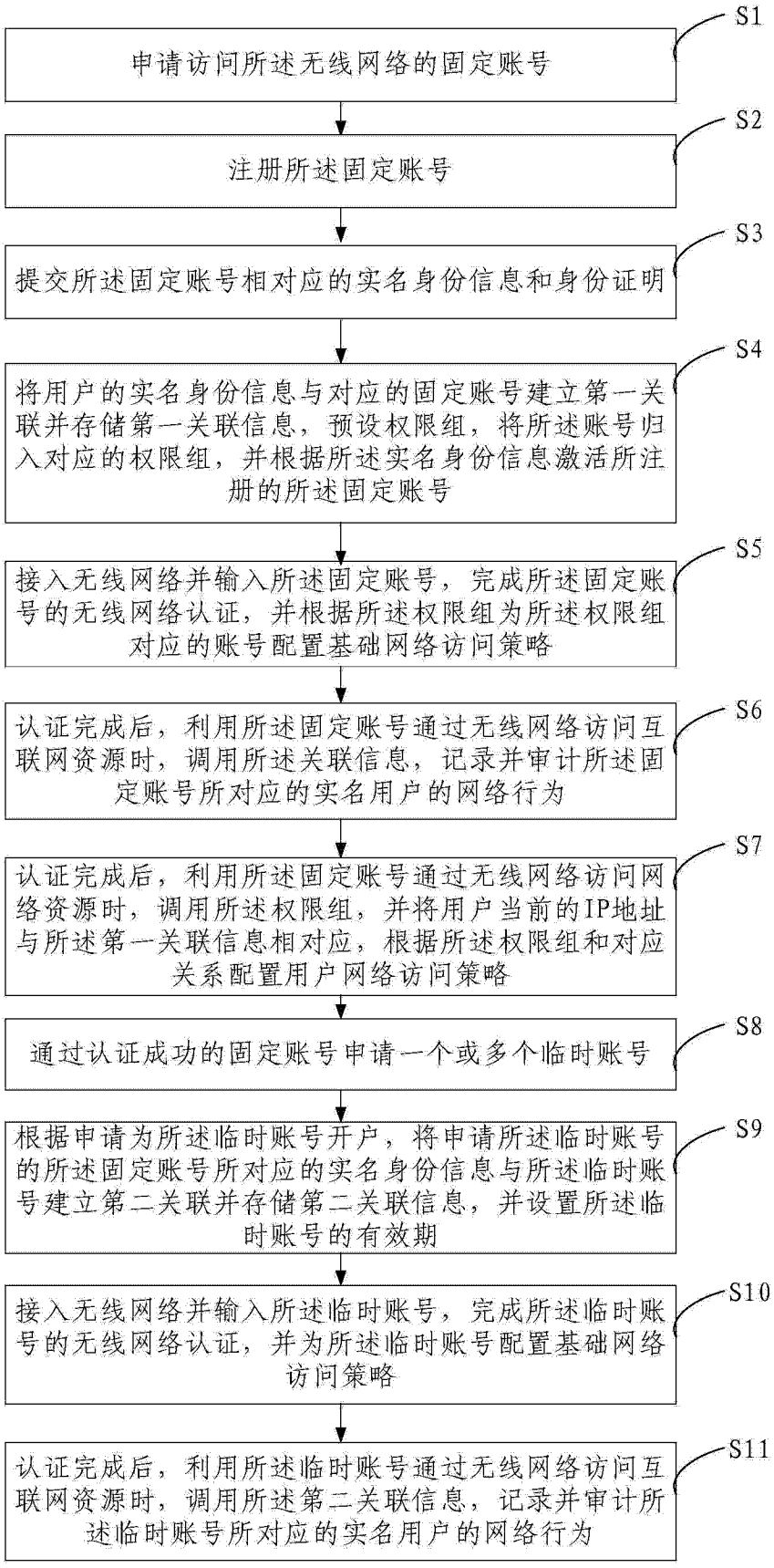

S1
申请访问所述无线网络的固定账号
S2
注册所述固定账号
S3
提交所述固定账号相对应的实名身份信息和身份证明
S4
将用户的实名身份信息与对应的固定账号建立第一关联并存储第一关联信息，预设权限组，将所述账号归入对应的权限组，并根据所述实名身份信息激活所注册的所述固定账号
S5
接入无线网络并输入所述固定账号，完成所述固定账号的无线网络认证，并根据所述权限组为所述权限组对应的账号配置基础网络访问策略
S6
认证完成后，利用所述固定账号通过无线网络访问互联网资源时，调用所述关联信息，记录并审计所述固定账号所对应的实名用户的网络行为
S7
认证完成后，利用所述固定账号通过无线网络访问网络资源时，调用所述权限组，并将用户当前的IP地址与所述第一关联信息相对应，根据所述权限组和对应关系配置用户网络访问策略
S8
通过认证成功的固定账号申请一个或多个临时账号
S9
根据申请为所述临时账号开户，将申请所述临时账号的所述固定账号所对应的实名身份信息与所述临时账号建立第二关联并存储第二关联信息，并设置所述临时账号的有效期
S10
接入无线网络并输入所述临时账号，完成所述临时账号的无线网络认证，并为所述临时账号配置基础网络访问策略
S11
认证完成后，利用所述临时账号通过无线网络访问互联网资源时，调用所述第二关联信息，记录并审计所述临时账号所对应的实名用户的网络行为

图 4

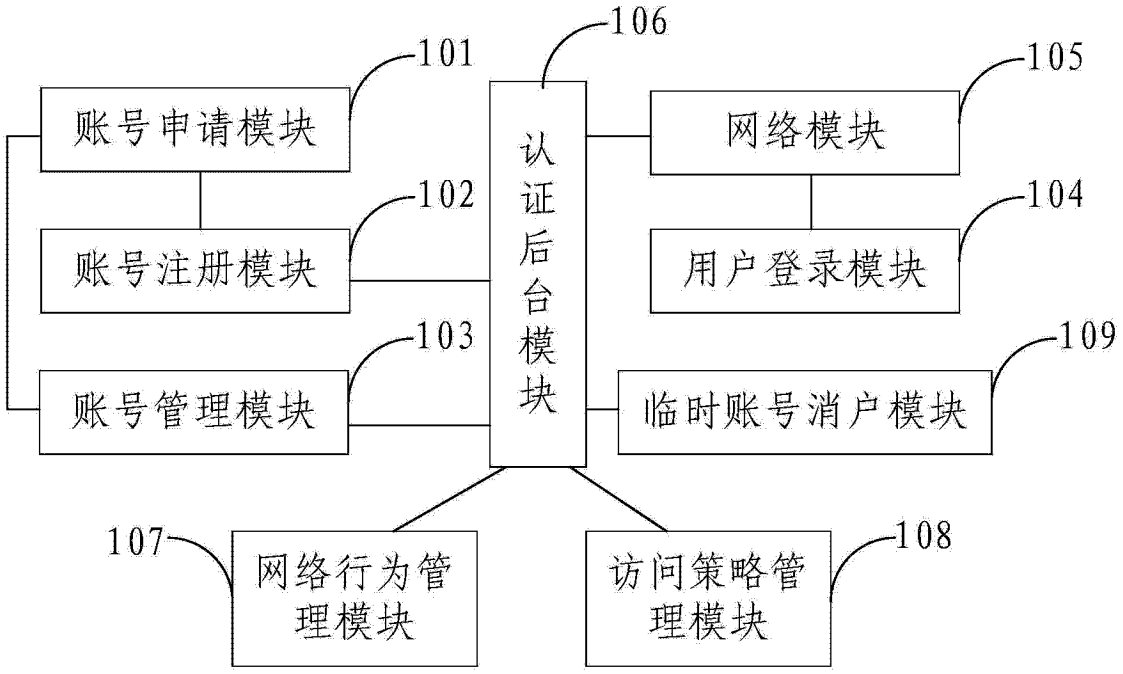

106
101
105
账号申请模块
认证后台模块
网络模块
102
104
账号注册模块
用户登录模块
103
109
账号管理模块
临时账号消户模块
107
网络行为管理模块
访问策略管理模块
108

图 5