(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 106685976 B
(45)授权公告日 2020.11.06

(21)申请号 201611264978.4

(22)申请日 2016.12.30

(65)同一申请的已公布的文献号
申请公布号 CN 106685976 A

(43)申请公布日 2017.05.17

(73)专利权人 北京国电通网络技术有限公司
地址 100085 北京市海淀区创业中路32号楼32-3-4108-4109
专利权人 国家电网有限公司
国网信息通信产业集团有限公司

(72)发明人 孙德艳 张晓枫 牟刚 汤清召 杨政巍 姜伟

(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 罗满

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04W 4/80(2018.01)
H04W 12/06(2009.01)

(56)对比文件
CN 105635174 A,2016.06.01
CN 105093948 A,2015.11.25
CN 105426796 A,2016.03.23
US 2007260635 A1,2007.11.08

审查员 白生斌

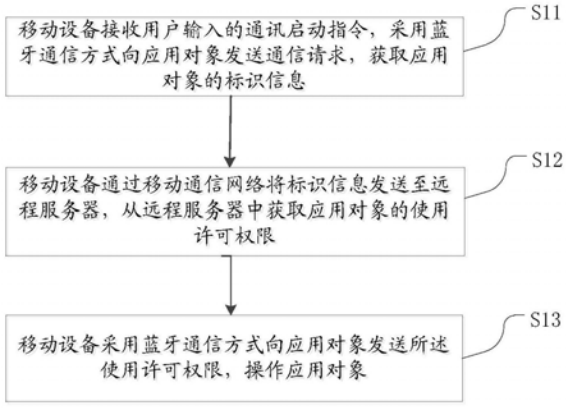
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种基于两级网络的安全管控方法

(57)摘要

本发明公开了一种基于两级网络的安全管控方法，该方法包括：移动设备接收用户输入的通讯启动指令，采用蓝牙通信方式向应用对象发送通信请求，获取应用对象的标识信息；移动设备通过移动通信网络将所述标识信息发送至远程服务器，从远程服务器中获取应用对象的使用许可权限；移动设备采用蓝牙通信方式向应用对象发送所述使用许可权限，操作应用对象。该方法实现扩大通信范围。



CN 106685976 B

1.一种基于两级网络的安全管控方法,其特征在于,包括:

移动设备接收用户输入的通讯启动指令,采用蓝牙通信方式向应用对象发送通信请求,获取应用对象的标识信息;

移动设备通过移动通信网络将所述标识信息发送至远程服务器,从远程服务器中获取应用对象的使用许可权限;

移动设备采用蓝牙通信方式向应用对象发送所述使用许可权限,操作应用对象;

其中,所述移动设备采用蓝牙通信方式向应用对象发送所述使用许可权限,操作应用对象,包括:

移动设备采用蓝牙点对点通信方式向应用对象发送所述使用许可权限;

应用对象对所述使用许可权限进行识别,识别成功后,接收移动设备对应用对象的操作。

2.如权利要求1所述的方法,其特征在于,所述移动设备接收用户输入的通讯启动指令,采用蓝牙通信方式向应用对象发送通信请求,获取应用对象的标识信息,包括:

移动设备接收用户输入的通讯启动指令,启动蓝牙通信模块;

移动设备通过蓝牙通信模块与应用对象进行蓝牙点对点通信,向应用对象发送通信请求;

应用对象接收通信请求,将应用对象的标识信息发送至移动设备。

3.如权利要求2所述的方法,其特征在于,所述移动设备通过移动通信网络将所述标识信息发送至远程服务器,从远程服务器中获取应用对象的使用许可权限,包括:

移动设备通过移动通信网络将所述标识信息发送至远程服务器;

远程服务器对所述标识信息进行验证,验证成功后,将所述应用对象的使用许可权限发送至移动设备。

4.如权利要求1所述的方法,其特征在于,所述应用对象包括智能设备。

5.如权利要求1所述的方法,其特征在于,所述移动设备包括手机或者PAD。

6.如权利要求1至5中任意一项所述的方法,其特征在于,获取应用对象的标识信息之后,还包括:

对所述标识信息进行加密。

一种基于两级网络的安全管控方法

技术领域

[0001] 本发明涉及通信技术领域，特别是涉及一种基于两级网络的安全管控方法。

背景技术

[0002] 目前，随着电力不断发展前进的步伐，越来越多的外包队伍参与到电网建设中来，以承包形式开展设备技改、土建、电缆清退、绿化及运输吊装等工作。外包施工模式，一方面弥补了企业劳动力的不足，另一方面，由于外包队伍人员素质良莠不齐，安全意识较为淡薄。建立外包队伍管理模式，通过对外包队伍实施日常管理、教育培训、安全检查、考核奖惩等与本单位施工队伍“无差别”管理，确保外包队伍安全管理处于可控、在控、能控状态。

[0003] 从基层工作性质来说，是企业生产经营的第一线，从事具体的生产经营工作，担负急难险重、苦脏累差的工作任务，提高效率、精简机构、压缩编制是社会趋势，国家电网也是如此，招收新人的数量在逐年压缩，冀希望于大量分配年轻人员充实到基层改变这一现状是不现实的，每年新分来的人员都是杯水车薪。建立必要的作业现场与业主人员实时监督关系，是时刻防备安全隐患的重要手段。

[0004] 智能硬件是建立作业现场和现场监督的重要纽带，是简化现场实施、现场监督的重要手段。现有技术中一般采用局域网、SIM卡等实现远程管理需求。这种模式局限性大，通信范围较小，例如局域网覆盖范围小，SIM卡资源有限，既不能满足用户的快速灵活多样性需求，又增加客户端的依赖性和硬件成本。

发明内容

[0005] 本发明的目的是提供一种基于两级网络的安全管控方法，以实现扩大通信范围。

[0006] 为解决上述技术问题，本发明提供一种基于两级网络的安全管控方法，该方法包括：

[0007] 移动设备接收用户输入的通讯启动指令，采用蓝牙通信方式向应用对象发送通信请求，获取应用对象的标识信息；

[0008] 移动设备通过移动通信网络将所述标识信息发送至远程服务器，从远程服务器中获取应用对象的使用许可权限；

[0009] 移动设备采用蓝牙通信方式向应用对象发送所述使用许可权限，操作应用对象。

[0010] 优选的，所述移动设备接收用户输入的通讯启动指令，采用蓝牙通信方式向应用对象发送通信请求，获取应用对象的标识信息，包括：

[0011] 移动设备接收用户输入的通讯启动指令，启动蓝牙通信模块；

[0012] 移动设备通过蓝牙通信模块与应用对象进行蓝牙点对点通信，向应用对象发送通信请求；

[0013] 应用对象接收通信请求，将应用对象的标识信息发送至移动设备。

[0014] 优选的，所述移动设备通过移动通信网络将所述标识信息发送至远程服务器，从远程服务器中获取应用对象的使用许可权限，包括：

[0015] 移动设备通过移动通信网络将所述标识信息发送至远程服务器；

[0016] 远程服务器对所述标识信息进行验证，验证成功后，将所述应用对象的使用许可权限发送至移动设备。

[0017] 优选的，所述移动设备采用蓝牙通信方式向应用对象发送所述使用许可权限，操作应用对象，包括：

[0018] 移动设备采用蓝牙点对点通信方式向应用对象发送所述使用许可权限；

[0019] 应用对象对所述使用许可权限进行识别，识别成功后，接收移动设备对应用对象的操作。

[0020] 优选的，所述应用对象包括智能设备。

[0021] 优选的，所述移动设备包括手机或者PAD。

[0022] 优选的，获取应用对象的标识信息之后，还包括：

[0023] 对所述标识信息进行加密。

[0024] 本发明所提供的一种基于两级网络的安全管控方法，移动设备接收用户输入的通讯启动指令，采用蓝牙通信方式向应用对象发送通信请求，获取应用对象的标识信息；移动设备通过移动通信网络将所述标识信息发送至远程认证服务器，从远程认证服务器中获取应用对象的使用许可权限；移动设备采用蓝牙通信方式向应用对象发送所述使用许可权限，操作应用对象本发明基于两级网络通信的智能安全管控技术释放了区域的限制性，减轻了客户端的冗余设计，快速实现用户远程管理需求的功能。可见，通过移动通信网络和蓝牙点对点网络相结合技术，采用蓝牙通信通用和移动通信网络通信的这两级网络来实现移动设备、应用对象、远程认证服务器间的通信，扩大通信范围。

附图说明

[0025] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，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，还可以根据提供的附图获得其他的附图。

[0026] 图1为本发明所提供的一种基于两级网络的安全管控方法的流程图；

[0027] 图2为基于两级网络的安全管控方法的原理图；

[0028] 图3为两级网络互相结合的原理图。

具体实施方式

[0029] 本发明的核心是提供一种基于两级网络的安全管控方法，以实现扩大通信范围。

[0030] 为了使本技术领域的人员更好地理解本发明方案，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。

[0031] 相关术语解释如下：

[0032] 移动通信网络：是相对于固定通信而言的，顾名思义是指能够在移动状态下完成信息交换的通信方式。移动通信网络包括计算机操作系统、应用软件系统、本地私有网络操

作系统、互联网协议等软件系统、物理通信信道、网络互连设备等硬件系统和系统中的数据。

[0033] 蓝牙点对点网络:是一种工作在全球通用的2.4GHz ISM(即工业、科学、医学)频段的短距离通信技术,通信距离在10m左右,其采用分散式网络结构以及快跳屏和短包技术,支持点对点及多点通信,广泛应用于智能手机及可穿戴设备领域等各个领域。

[0034] 请参考图1,图1为本发明所提供的一种基于两级网络的安全管控方法的流程图,该方法包括:

[0035] S11:移动设备接收用户输入的通讯启动指令,采用蓝牙通信方式向应用对象发送通信请求,获取应用对象的标识信息;

[0036] S12:移动设备通过移动通信网络将标识信息发送至远程服务器,从远程服务器中获取应用对象的使用许可权限;

[0037] S13:移动设备采用蓝牙通信方式向应用对象发送使用许可权限,操作应用对象。

[0038] 可见,该方法通过移动通信网络和蓝牙点对点网络相结合技术,采用蓝牙通信通用和移动通信网络通信的这两级网络来实现移动设备、应用对象、远程认证服务器间的通信,扩大通信范围。

[0039] 基于上述方法,进一步的,步骤S11具体包括以下步骤:

[0040] S1:移动设备接收用户输入的通讯启动指令,采用蓝牙通信方式向应用对象发送通信请求,获取应用对象的标识信息,包括:

[0041] S2:移动设备接收用户输入的通讯启动指令,启动蓝牙通信模块;

[0042] S3:移动设备通过蓝牙通信模块与应用对象进行蓝牙点对点通信,向应用对象发送通信请求;

[0043] S4:应用对象接收通信请求,将应用对象的标识信息发送至移动设备。

[0044] 进一步的,步骤S12的过程具体包括:移动设备通过移动通信网络将标识信息发送至远程服务器;远程服务器对标识信息进行验证,验证成功后,将应用对象的使用许可权限发送至移动设备。

[0045] 进一步的,步骤S13的过程具体包括:移动设备采用蓝牙点对点通信方式向应用对象发送使用许可权限;应用对象对使用许可权限进行识别,识别成功后,接收移动设备对应用对象的操作。

[0046] 其中,应用对象包括智能设备。

[0047] 其中,移动设备包括手机或者PAD。

[0048] 进一步的,步骤S11中,获取应用对象的标识信息之后,还包括:对标识信息进行加密。具体的,采用安全加密模块对标识信息进行加密。

[0049] 本方法基于稳定的移动通信网络,结合蓝牙点对点通信实现复杂环境下“互联网+”的应用功能,方便地域广、应用环境复杂、远程管理精度高的“互联网+”应用的推广实现复杂环境下范围广、适应性强、设备耦合性强的“互联网+”智能应用。

[0050] 图2为基于两级网络的安全管控方法的原理图。本发明基于稳定的移动通信网络,结合蓝牙点对点通信实现复杂环境下“互联网+”的应用功能,方便地域广、应用环境复杂、远程管理精度高的“互联网+”应用的推广。

[0051] 详细的,基于本方法,具体实现分为三个步骤:

[0052] 1、用户采用移动设备(例如:手机、PDA)依据自己的需求通过蓝牙点对点通信向应用对象发出通信要求,并获取通信对象的唯一标识。

[0053] 2、用户采用移动设备通过移动通信网络应用对象标识和当前用户信息,并从远程服务器获取应用对象信息、对象使用许可权限。

[0054] 3、用户采用移动设备通过蓝牙点对点通信向应用对象提交权限识别认证后,操作应用对象。

[0055] 另外,现在的时代是一个无不网络的时代,家庭网、企业网、政府网无不充斥生活的角角落落,手机、电脑、路由器、交换机、服务器、智能家居、智能穿戴、智能工具等网络设备密密麻麻。庞大的客户端、中转站和高度依赖性的产品设计都让设备必须处于运行状态,造成许多有限资源的无效浪费。本方法基于移动通信网络,结合蓝牙点对点通信建立的移动分支通信网络,也能有效利用移动客户端的中转路由资源,节省资源,在广范围条件下,实现了远程管理的需求。

[0056] 图3为两级网络互相结合的原理图。进一步的,移动设备从远程服务器中获取应用对象的使用许可权限的过程中,远程服务器将标识信息推送给另一个移动设备,由另一个移动设备在审核用户的操作指令下对标识信息进行审核,审核完成后这个移动设备向远程服务器发送认证信息,远程服务器接收认证信息。

[0057] 其中,在通过蓝牙点对点通信和移动通信网络进行信息传递的过程中,需要对传递的数据进行分析转换,具体的,选择想要分析的物理模型文件,系统自动将物理模型文件转化成XML文件的形式,然后通过DOM方式解析XML,DOM是一种基于树解析的方法,物理模型文档转化的XML文档的主要构成的元素有文档根节点、若干个表格元素、表格元素下的列集合元素、列集合下的属性元素、属性中的文本元素等,自上而下呈树形包含关系,层次结构清晰分明,通过遍历整个XML文件中的节点信息可以实现具体的功能,保证了数据的完整性和持久性。

[0058] 本发明基于移动通信网络、蓝牙点对点通信的两级网络叠加通信的形式,有别于现有的数据传输方式,提高产品的耦合性和实用性。另外本发明除了以上阐述的通讯功能外,还整合了数据通讯过程的安全加密模块,保证安全稳定可靠的数据通讯。通过本发明,可以明确智能硬件的网络部署方式,建立稳定的通讯交互模块,保证智能硬件的安全稳定应用和维护。

[0059] 综上,本发明所提供的一种基于两级网络的安全管控方法,移动设备接收用户输入的通讯启动指令,采用蓝牙通信方式向应用对象发送通信请求,获取应用对象的标识信息;移动设备通过移动通信网络将标识信息发送至远程认证服务器,从远程认证服务器中获取应用对象的使用许可权限;移动设备采用蓝牙通信方式向应用对象发送使用许可权限,操作应用对象本发明基于两级网络通信的智能安全管控技术释放了区域的限制性,减轻了客户端的冗余设计,快速实现用户远程管理需求的功能。可见,该方法通过移动通信网络和蓝牙点对点网络相结合技术,采用蓝牙通信通用和移动通信网络通信的这两级网络来实现移动设备、应用对象、远程认证服务器间的通信,扩大通信范围。

[0060] 并且,本方法基于稳定的移动通信网络,结合蓝牙点对点通信实现复杂环境下“互联网+”的应用功能,方便地域广、应用环境复杂、远程管理精度高的“互联网+”应用的推广实现复杂环境下范围广、适应性强、设备耦合性强的“互联网+”智能应用。

[0061] 以上对本发明所提供的的一种基于两级网络的安全管控方法进行了详细介绍。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。应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以对本发明进行若干改进和修饰，这些改进和修饰也落入本发明权利要求的保护范围内。

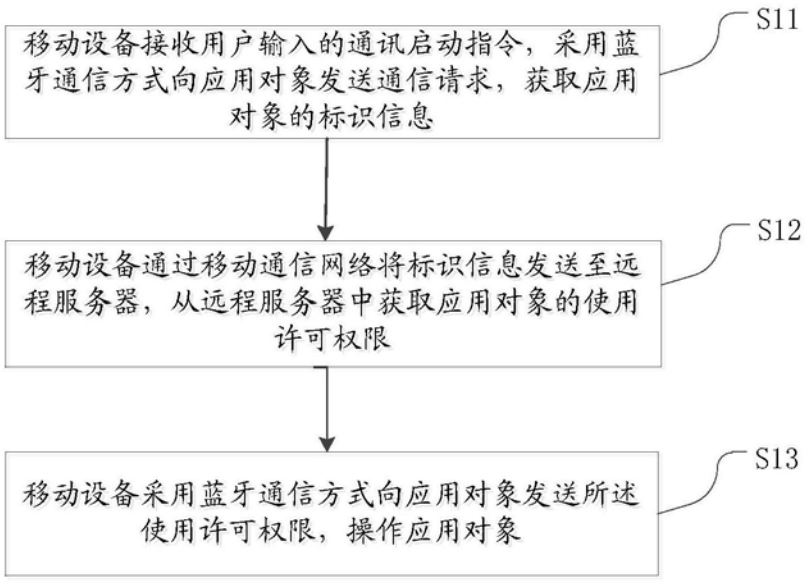

移动设备接收用户输入的通讯启动指令，采用蓝牙通信方式向应用对象发送通信请求，获取应用对象的标识信息
S11
移动设备通过移动通信网络将标识信息发送至远程服务器，从远程服务器中获取应用对象的使用许可权限
S12
移动设备采用蓝牙通信方式向应用对象发送所述使用许可权限，操作应用对象
S13

图1

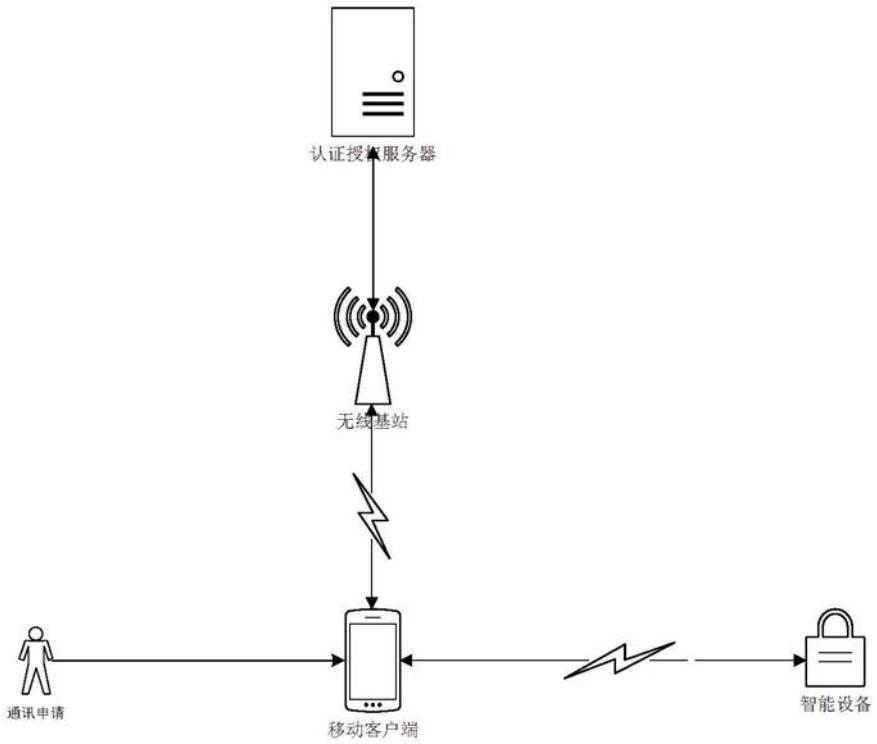

认证授权服务器
无线基站
通讯申请
移动客户端
智能设备

图2

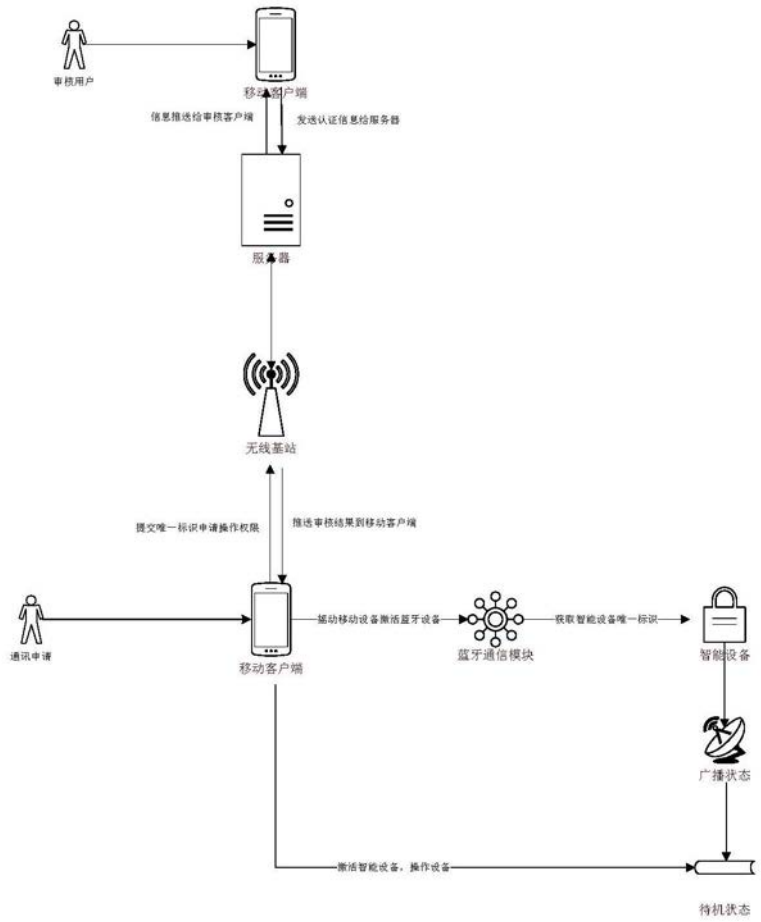

审核用户
移动客户端
信息推送给审核客户端
发送认证信息给服务器
服务器
无线基站
提交唯一标识申请操作权限
推送审核结果到移动客户端
通讯申请
移动客户端
驱动移动设备激活蓝牙设备
蓝牙通信模块
获取智能设备唯一标识
智能设备
广播状态
激活智能设备，操作设备
待机状态

图3