(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 106412122 A
(43)申请公布日 2017.02.15

(21)申请号 201611050523.2

(22)申请日 2016.11.24

(71)申请人 美的智慧家居科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)
申请人 美的集团股份有限公司

(72)发明人 刘俊彦

(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 罗攀 肖冰滨

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 12/741(2013.01)

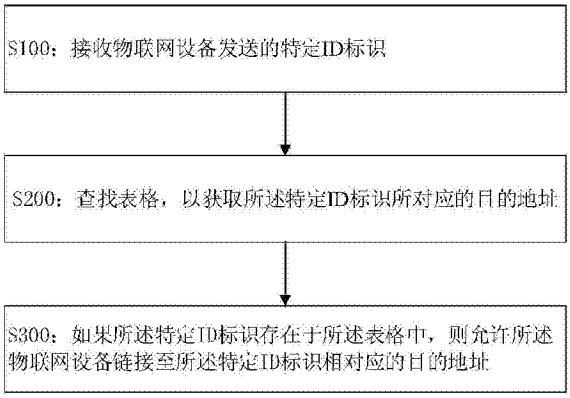
权利要求书1页 说明书4页 附图2页

(54)发明名称

物联网设备与服务器的安全链接方法和装置及无线路由器

(57)摘要

本发明涉及物联网领域,公开了一种物联网设备与服务器的安全链接方法,该方法包括:接收物联网设备发送的特定ID标识,该特定ID标识对应于所述物联网设备的链接请求所对应的目的地址;查找表格,以获取所述特定ID标识所对应的目的地址,在该表格中,每一特定ID标识与相应的目的地址相匹配;以及如果所述特定ID标识存在于所述表格中,则允许所述物联网设备链接至与所述特定ID标识相对应的目的地址。本发明的另一方面还提供一种物联网设备与服务器的安全链接装置,以及应用该装置的无线路由器。



CN 106412122 A

1.一种物联网设备与服务器的安全链接方法，其特征在于，该方法包括：

接收物联网设备发送的特定ID标识，该特定ID标识对应于所述物联网设备的链接请求所对应的目的地址；

查找表格，以获取所述特定ID标识所对应的目的地址，在该表格中，每一特定ID标识与相应的目的地址相匹配；以及

如果所述特定ID标识存在于所述表格中，则允许所述物联网设备链接至与所述特定ID标识相对应的目的地址。

2.根据权利要求1所述的物联网设备与服务器的安全链接方法，其特征在于，该方法还包括：如果所述特定ID标识不存在于所述表格中，则拦截所述物联网设备的链接请求。

3.根据权利要求1或2所述的物联网设备与服务器的安全链接方法，其特征在于，该方法还包括：实时更新所述表格。

4.根据权利要求3所述的物联网设备与服务器的安全链接方法，其特征在于，该方法还包括：对物联网设备发送的特定ID标识进行加密处理，并在接收所述特定ID标识时进行解密处理。

5.根据权利要求1或2所述的物联网设备与服务器的安全链接方法，其特征在于，该方法还包括：

当所述物联网设备的链接请求被拦截的次数达到预定次数时，在预定时间内不再接收所述物联网设备发送的特定ID标识。

6.一种物联网设备与服务器的安全链接装置，其特征在于，该装置包括：

接收模块，用于接收物联网设备发送的特定ID标识，该特定ID标识对应于所述物联网设备的链接请求所对应的目的地址；

查找模块，用于查找表格，以获取所述特定ID标识所对应的目的地址；以及；

链接控制模块，用于在所述特定ID标识存在于所述表格中的情况下，允许所述物联网设备链接至与所述特定ID标识相对应的目的地址；

其中，在所述表格中，每一ID标识与相应的目的地址相匹配。

7.根据权利要求6所述的物联网设备与服务器的安全链接装置，其特征在于，所述链接控制模块当所述特定ID标识不存在于所述表格中，拦截所述物联网设备的链接请求。

8.根据权利要求7所述的物联网设备与服务器的安全链接装置，其特征在于，所述查找模块实时从服务器上下载更新所述表格。

9.根据权利要求7所述的物联网设备与服务器的安全链接装置，其特征在于，该装置还包括：

解密模块，用于对被加密的所述ID标识进行解密处理。

10.根据权利要求7所述的物联网设备与服务器的安全链接装置，其特征在于，所述链接控制模块当所述物联网设备的链接请求被拦截的次数达到预定次数时，在预定时间内不再接收所述物联网设备发送的特定ID标识。

11.一种用于物联网链接控制的无线路由器，其特征在于，该无线路由器包括权利要求6-10所述的物联网设备与服务器的安全链接装置。

物联网设备与服务器的安全链接方法和装置及无线路由器

技术领域

[0001] 本发明涉及物联网领域，具体地，涉及一种物联网设备与服务器的安全链接方法和装置及用于物联网链接控制的无线路由器。

背景技术

[0002] 物联网是以计算机科学为基础，包括网络、电子、射频、感应、无线、人工智能、条码、云计算、自动化、嵌入式等技术为一体的综合性技术及应用，它要让孤立的物品(例如：冰箱、汽车、设备、家具、货品等等)接入网络世界，让它们之间能相互交流，让我们可以通过软件系统对其进行操作。

[0003] 物联网设备通常利用无线链接设备(例如，路由器)链接至相应的服务器。在现有的链接控制技术中，物联网设备链接路由器后，向路由器发送特殊标识，路由器接收该标识后，如果能够识别该特殊标识，则允许该物联网设备链接至相应的服务器。但是在现有的链接控制方式中，非法设备可能利用已被授权的物联网设备的特殊标识访问任意服务器，可能出现物联网设备滥用特殊标识的问题，并且即使是被授权的物联网设备也可能会利用该特殊标识进行在其授权功能之外的活动，从而可能超出其链接权限，因此，现有的链接控制技术存在着诸多不安全隐患。

发明内容

[0004] 本发明的目的是提供一种设备，该设备物联网设备与服务器的安全链接方法和装置，利有该方法和装置能够有效过滤物联网设备的非法连接，并能防止来自非授权设备的恶意链接从而能够保障物联网的安全。

[0005] 本发明的另一方面还提供了一种应用所述设备物联网设备与服务器的安全链接方法和装置的无线路由器，通过该无线路由器，可以保证物联网设备和服务器之间的安链接。

[0006] 为了实现上述目的，本发明提供一种物联网设备与服务器的安全链接方法，该方法包括：接收物联网设备发送的特定ID标识，该特定ID标识对应于所述物联网设备的链接请求所对应的目的地址；查找表格，以获取所述特定ID标识所对应的目的地址，在该表格中，每一特定ID标识与相应的目的地址相匹配；以及如果所述特定ID标识存在于所述表格中，则允许所述物联网设备链接至与所述特定ID标识相对应的目的地址。

[0007] 其中，每台物联网设备的特定ID标识可以在出厂时配置，并且每台物联网设备可以有多个特定ID标识，其所具有的每个特定ID标识可以代表该物联网设备需要与服务器链接的各项业务，当所述物联网设备因某种业务而需要链接至相应的服务器时，例如向服务器发送消息时，可以同时发送该特定ID标识。每台设备的特定ID标识与相应服务器相匹配，因此可以预先生成特定ID标识与服务器地址匹配的表格，在接收到物联网设备时查找该表格，从而可以判别该物联网设备是否是被授权的设备或其发送的业务是否是被授权的业务。

[0008] 其中该方法还可以包括：如果所述特定ID标识不存在于所述表格中，则拦截所述物联网设备的链接请求。如果所述特定ID标识不存在于所述表格中，则表示发送该特定ID标识的设备是权限外设备，或者该设备发送的业务是权限外业务，可以直接丢弃与该特定ID标识一同发送的业务或消息。

[0009] 其中，该方法还可以包括：实时更新所述表格。

[0010] 其中，该方法还可以包括：对物联网设备发送的特定ID标识进行加密处理，并在接收所述特定ID标识时进行解密处理。

[0011] 其中，该方法还可以包括：当所述物联网设备的链接请求被拦截的次数达到预定次数时，在预定时间内不再接收所述物联网设备发送的特定ID标识。

[0012] 根据本发明的另一方面，还提供一种该物联网设备与服务器的安全链接，该装置包括：接收模块，用于接收物联网设备发送的特定ID标识，该特定ID标识对应于所述物联网设备的链接请求所对应的目的地址；查找模块，用于查找表格，以获取所述特定ID标识所对应的目的地址；以及链接控制模块，用于在所述特定ID标识存在于所述表格中的情况下，允许所述物联网设备链接至与所述特定ID标识相对应的目的地址；其中，在所述表格中，每一ID标识与相应的目的地址相匹配。

[0013] 其中，所述链接控制模块可以当所述特定ID标识不存在于所述表格中，拦截所述物联网设备的链接请求。

[0014] 其中，所述查找模块可以实时从服务器上下载更新所述表格。

[0015] 其中，该装置还可以包括：解密模块，用于对被加密的所述ID标识进行解密处理。当物联网设备的特定ID标识经过加密处理时，在接收所述特定ID标识时需要对其进行解密处理。

[0016] 其中，所述链接控制模块可以当所述物联网设备的链接请求被拦截的次数达到预定次数时，在预定时间内不再接收所述物联网设备发送的特定ID标识。

[0017] 根据本发明的再一方面，还提供一种应用所述物联网设备与服务器的安全链接装置的无线路由器。

[0018] 通过上述技术方案，能够限制物联网设备的链接权限，使其只在特定的业务范围内链接到相应的服务器，防止物联网设备滥用其特定ID标识，同时，还能够限制非法物联网设备链接到服务器，从而为物联网环境提供了安全有效的链接控制方案。

[0019] 本发明的其它特征和优点将在随后的具体实施方式部分予以详细说明。

附图说明

[0020] 附图是用来提供对本发明的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本发明，但并不构成对本发明的限制。在附图中：

[0021] 图1是根据本发明的实施例一的物联网设备与服务器的安全链接方法的流程图；

[0022] 图2是是根据本发明的实施例二的物联网设备与服务器的安全链接方法的流程图；以及

[0023] 图3是根据本发明的实施例三的物联网设备与服务器的安全链接装置的结构图。

[0024] 附图标记说明

[0025] 100：接收模块 200：查找模块

[0026] 300:链接控制模块

具体实施方式

[0027] 以下结合附图对本发明的具体实施方式进行详细说明。应当理解的是,此处所描述的具体实施方式仅用于说明和解释本发明,并不用于限制本发明。

[0028] 图1是根据本发明的实施例一的物联网设备与服务器的安全链接方法的流程图。如图1所示,该方法包括以下步骤:

[0029] 在步骤S100中,接收物联网设备发送的特定ID标识,该特定ID标识对应于所述物联网设备的链接请求所对应的目的地址。物联网设备可以根据其业务需要配置多个特定ID标识,在向服务器发送相关业务请求时同时发送与该业务相应的特定ID标识。

[0030] 在步骤S200中,查找表格,以获取所述特定ID标识所对应的目的地址,在该表格中,每一特定ID标识与相应的目的地址相匹配。

[0031] 在步骤S300中,如果所述特定ID标识存在于所述表格中,则允许所述物联网设备链接至与所述特定ID标识相对应的目的地址。

[0032] 图2是是根据本发明的实施例二的物联网设备与服务器的安全链接方法的流程图。如图2所示,在实施例一的基础上,实施二的物联网设备与服务器的安全链接方法还可以包括以下步骤:

[0033] 在步骤S250中,对物联网设备发送的特定ID标识进行加密处理,同时在接收该特定ID标识时对其进行解密处理。加密可以防止非法设备滥用有权限的物联网设备的安全性,从而可以提高物联网链接的安全性。

[0034] 在步骤S400中,如果所述特定ID标识不存在于所述表格中,则拦截所述物联网设备的链接请求。如果被接收的特定ID标识不存在于所述表格中,则表示与该特定ID相应的业务不属于授权的范围,因此可以禁止该物联网设备与服务器的链接行为。

[0035] 在步骤S500中,当所述物联网设备的链接请求被拦截的次数达到预定次数时,在预定时间内不再接收所述物联网设备发送的特定ID标识。当多次接收到非法的特定ID标识时,则表明此时可能有非法设备恶意进行链接,及时禁止接收该特定ID标识可以在一定程度上防止非法设备对服务器或其它物联网设备的恶意攻击行为。

[0036] 在步骤S600中,实时更新所述表格。服务器的地址可能会发生变更,物联网设备的链接业务也有可能增加或减少,因此可以通过实时更新表格达到顺畅链接的目的。例如,可以从DNS服务器中实时更新所述表格。该步骤并不一定位于如图2所示的位置,对表格的更新操作可以在实施该方法时的任意步骤实施。

[0037] 图3是根据本发明的实施例三的物联网设备与服务器的安全链接装置的结构图。如图3所示,该装置可以包括:接收模块100,用于接收物联网设备发送的特定ID标识,该特定ID标识对应于所述物联网设备的链接请求所对应的目的地址;查找模块200,用于查找表格,以获取所述特定ID标识所对应的目的地址;以及链接控制模块300,用于在所述特定ID标识存在于所述表格中的情况下,允许所述物联网设备链接至与所述特定ID标识相对应的目的地址;其中,在所述表格中,每一ID标识与相应的目的地址相匹配。

[0038] 其中,所述链接控制模块300可以当所述特定ID标识不存在于所述表格中,拦截所述物联网设备的链接请求。此外,所述链接控制模块300还可以当所述物联网设备的链接请

求被拦截的次数达到预定次数时，在预定时间内不再接收所述物联网设备发送的特定ID标识。

[0039] 其中，所述查找模块200可以实时从服务器上下载更新所述表格。表格的更新操作可以是对每个特定ID标识所对应的服务器地址进行更新，也可以在表格中增加或减少特定ID标识与服务器的匹配，从而在保证顺畅链接的同时提高查找的效率。

[0040] 其中，该装置还可以包括：解密模块，用于对被加密的所述ID标识进行解密处理。当物联网设备的特定ID标识已经过加密处理时，在接收特定ID标识时可以利用解密模块对其进行解密。

[0041] 上述实施例中所述的物联网设备与服务器的安全链接方法及装置尤其可以应用于作为物联网链接控制装置的无线路由器。

[0042] 以上结合附图详细描述了本发明的优选实施方式，但是，本发明并不限于上述实施方式中的具体细节，在本发明的技术构思范围内，可以对本发明的技术方案进行多种简单变型，这些简单变型均属于本发明的保护范围。

[0043] 另外需要说明的是，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合，为了避免不必要的重复，本发明对各种可能的组合方式不再另行说明。

[0044] 此外，本发明的各种不同的实施方式之间也可以进行任意组合，只要其不违背本发明的思想，其同样应当视为本发明所公开的内容。

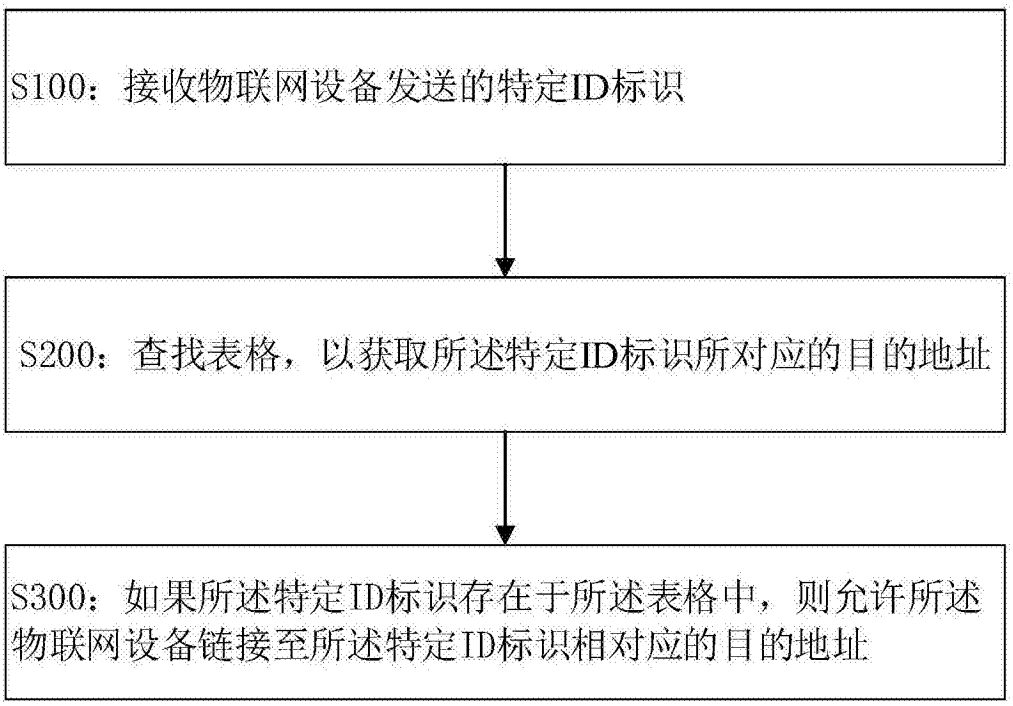

S100：接收物联网设备发送的特定ID标识
S200：查找表格，以获取所述特定ID标识所对应的目的地址
S300：如果所述特定ID标识存在于所述表格中，则允许所述物联网设备链接至所述特定ID标识相对应的目的地址

图1

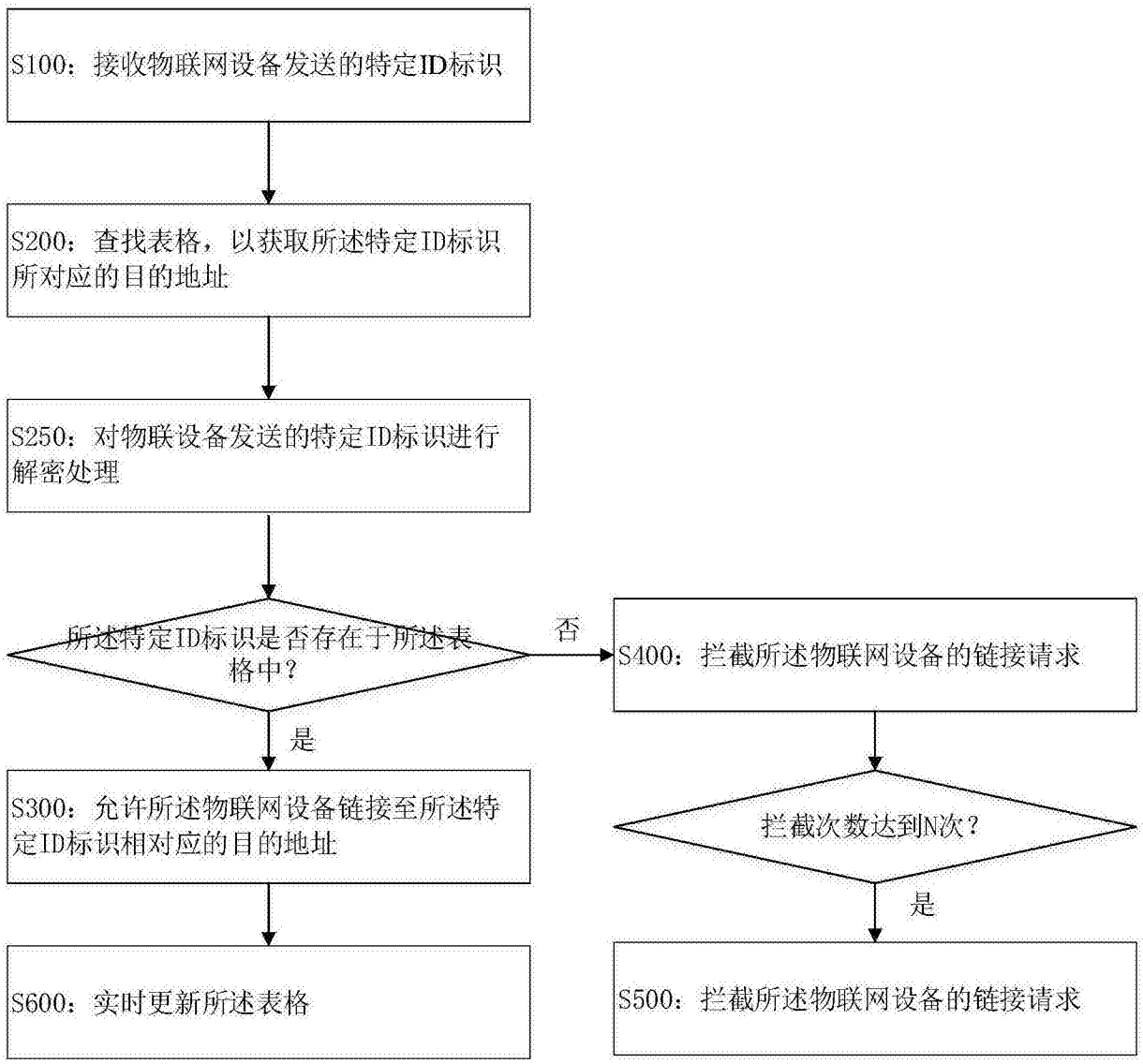

S100：接收物联网设备发送的特定ID标识
S200：查找表格，以获取所述特定ID标识所对应的目的地址
S250：对物联设备发送的特定ID标识进行解密处理
所述特定ID标识是否存在于所述表格中？
否
是
S400：拦截所述物联网设备的链接请求
拦截次数达到N次？
是
S300：允许所述物联网设备链接至所述特定ID标识相对应的目的地址
S600：实时更新所述表格
S500：拦截所述物联网设备的链接请求

图2

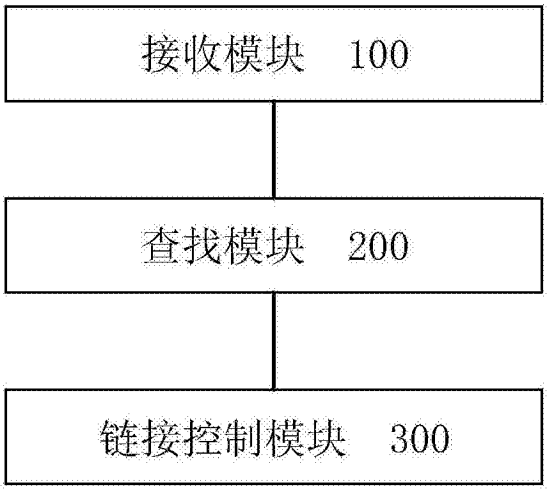

接收模块 100
查找模块 200
链接控制模块 300

图3