(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 103561044 B
(45)授权公告日 2017.06.27

(21)申请号 201310590158.4
(22)申请日 2013.11.20
(65)同一申请的已公布的文献号
申请公布号 CN 103561044 A
(43)申请公布日 2014.02.05
(73)专利权人 无锡儒安科技有限公司
地址 214135 江苏省无锡市无锡新区太科园大学科技园清源路立业楼A区501室
(72)发明人 刘慈航 司徒静弘 郭逸 杨磊
(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 胡彬
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/30(2006.01)
(56)对比文件
CN 102638585 A,2012.08.15,
CN 101201620 A,2008.06.18,
CN 102238236 A,2011.11.09,
CN 102594823 A,2012.07.18,
US 2006149962 A1,2006.07.06,
CN 101159556 A,2008.04.09,
CN 101409619 A,2009.04.15,
审查员 张春洁

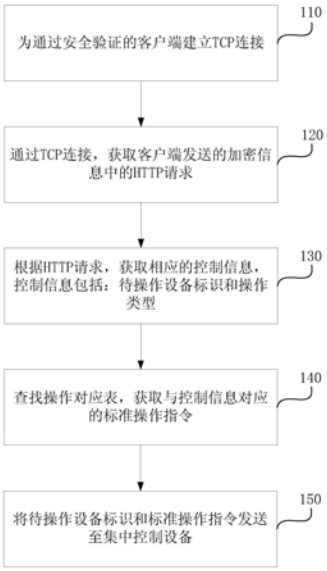
权利要求书2页 说明书8页 附图3页

(54)发明名称

数据传输方法和数据传输系统

(57)摘要

本发明公开了一种数据传输方法和数据传输系统。所述方法包括:为通过安全验证的客户端建立传输控制协议TCP连接;通过所述TCP连接,获取所述客户端发送的加密信息中的超文本传输协议HTTP请求;根据所述HTTP请求,获取相应的控制信息,其中,所述控制信息包括待操作设备标识和操作类型;查找操作对应表,获取与所述控制信息对应的标准操作指令;将所述待操作设备标识和所述标准操作指令发送至集中控制设备。本发明减少了用户与智能家居设备之间的直接交互,增强了智能家居设备使用的安全性和可靠性,减少了用户管理和使用异构型智能家居设备时的复杂度,提高了智能家居管理系统的使用有效性。



CN 103561044 B

1.一种数据传输方法,其特征在于,由服务器执行,包括:

为通过安全验证的客户端建立传输控制协议TCP连接;

其中,所述为通过安全验证的客户端建立传输控制协议TCP连接具体包括:接收客户端发送的加密后的密钥信息;根据自身的私钥和所述客户端的公钥对所述密钥信息进行解密运算,得到临时会话密钥和第一散列值;按照密码杂凑算法对所述临时会话密钥进行散列运算,当散列运算结果与所述第一散列值相同时,确定所述客户端通过安全验证;保存得到的所述临时会话密钥,为所述客户端建立TCP连接;

通过所述TCP连接,获取所述客户端发送的加密信息中的超文本传输协议HTTP请求;

根据所述HTTP请求,获取相应的控制信息,其中,所述控制信息包括待操作设备标识和操作类型;

查找操作对应表,获取与所述控制信息对应的标准操作指令;

将所述待操作设备标识和所述标准操作指令发送至集中控制设备。

2.根据权利要求1所述的数据传输方法,其特征在于,所述通过所述TCP连接,接收客户端发送的加密信息,获取所述加密信息中的HTTP请求具体包括:

通过所述TCP连接,接收所述客户端发送的加密信息;

根据所述临时会话密钥和所述客户端的公钥对接收的所述加密信息进行解密运算,得到HTTP请求和第二散列值;

按照密码杂凑算法对所述HTTP请求进行散列运算,当散列运算结果与所述第二散列值相同时,获取所述HTTP请求。

3.根据权利要求1所述的数据传输方法,其特征在于,所述根据所述HTTP请求中,获取相应的控制信息具体包括:

按照表述性状态转移REST服务原则,从所述HTTP请求中提取统一资源定位符URL信息;

获取所述URL信息中的相应的控制信息。

4.根据权利要求1所述的数据传输方法,其特征在于,所述集中控制设备为美国电气和电子工程师协会IEEE802.15.4协议ZigBee发送模块。

5.一种数据传输系统,其特征在于,包括:服务器、集中控制设备和至少两个接收设备,所述服务器与所述集中控制设备相连,所述集中控制设备分别与所述至少两个接收设备相连,其中:

所述服务器包括:

连接建立单元,用于为通过安全验证的客户端建立传输控制协议TCP连接;

其中,所述连接建立单元具体用于:接收客户端发送的加密后的密钥信息;根据自身的私钥和所述客户端的公钥对所述密钥信息进行解密运算,得到临时会话密钥和第一散列值;按照密码杂凑算法对所述临时会话密钥进行散列运算,当散列运算结果与所述第一散列值相同时,确定所述客户端通过安全验证;保存得到的所述临时会话密钥,为所述客户端建立TCP连接;

请求获取单元,用于通过所述TCP连接,获取所述客户端发送的加密信息中的超文本传输协议HTTP请求;

控制信息获取单元,用于根据所述HTTP请求,获取相应的控制信息,其中,所述控制信息包括待操作设备标识和操作类型;

标准操作代码获取单元，用于查找操作对应表，获取与所述控制信息对应的标准操作指令；

操作指令发送单元，用于将所述待操作设备标识和所述标准操作指令发送至集中控制设备；

所述集中控制设备用于向与所述待操作设备标识对应的接收设备发送所述标准操作指令；

所述接收设备用于根据接收到的所述标准操作指令，进行相应的操作。

6.根据权利要求5所述的数据传输系统，其特征在于，所述请求获取单元具体用于：

通过所述TCP连接，接收所述客户端发送的加密信息；

根据所述临时会话密钥和所述客户端的公钥对接收的所述加密信息进行解密运算，得到HTTP请求和第二散列值；

按照密码杂凑算法对所述HTTP请求进行散列运算，当散列运算结果与所述第二散列值相同时，获取所述HTTP请求。

7.根据权利要求5所述的数据传输系统，其特征在于，所述控制信息获取单元具体用于：

按照表述性状态转移REST服务原则，从所述HTTP请求中提取统一资源定位符URL信息；

获取所述URL信息中的相应的控制信息。

8.根据权利要求5所述的数据传输系统，其特征在于，所述集中控制设备为美国电气和电子工程师协会IEEE802.15.4协议ZigBee发送模块，所述接收设备为ZigBee接收模块。

数据传输方法和数据传输系统

技术领域

[0001] 本发明涉及通信技术和计算机数据处理领域，尤其涉及一种数据传输方法和数据传输系统。

背景技术

[0002] 智能家居是以住宅为平台，兼备建筑设备、网络通信、信息家电和设备自动化，集系统、结构、服务、管理为一体的智能化控制系统，该系统利用先进的计算机技术、网络通讯技术、综合布线技术、无线技术，将与家居生活有关的各种子系统有机地结合在一起，使其可以满足并实现高效、舒适、安全、遍历、环保的人文居住环境。智能家居可以提供全方位的信息交互功能，帮助家庭与外部保持信息交流畅通，优化人们的生活方式，帮助人们有效安排时间，增强家居生活的安全性。

[0003] ZigBee是IEEE802.15.4协议的代名词。根据这个协议制定的规则就被称为ZigBee技术。它是一种近距离、低复杂度、低功耗、低成本的双向无线通讯技术，主要适合于自动控制和远程控制领域，可以嵌入各种设备中，同时支持地理定位功能。ZigBee协议栈的物理层和MAC(Media Access Control，媒体访问控制)层都是由IEEE802.15.4所定义，其中物理层支持868/915MHz和2.4GHz三种频段。目前，ZigBee技术被广泛应用于智能家居系统中。

[0004] 一般来说，智能家居设备大多来自于不同的生产厂家，而不同厂家使用的协议标准不同，控制方式和控制指令也不同。因此，对于一个异构型智能家居系统来说，用户在进行家居管理和控制时，复杂度较高；另外，现有的智能家居设备在通信协议的设计上缺乏安全性方面的考虑，对数据隐私性的保护不够，一旦通信协议被破解，攻击者可以远程操纵任何家庭中的任何家居设备。

发明内容

[0005] 有鉴于此，本发明提供一种数据传输方法和数据传输系统。减少了用户与智能家居设备之间的直接交互，增强了智能家居设备使用的安全性和可靠性，减少了用户管理和使用异构型智能家居设备时的复杂度，提高了智能家居管理系统的使用有效性。

[0006] 在第一方面，本发明实施例提供了一种数据传输方法，包括：

[0007] 为通过安全验证的客户端建立传输控制协议TCP连接；

[0008] 通过所述TCP连接，获取所述客户端发送的加密信息中的超文本传输协议HTTP请求；

[0009] 根据所述HTTP请求，获取相应的控制信息，其中，所述控制信息包括待操作设备标识和操作类型；

[0010] 查找操作对应表，获取与所述控制信息对应的标准操作指令；

[0011] 将所述待操作设备标识和所述标准操作指令发送至集中控制设备。

[0012] 在第一种可能的实现方式中，所述为通过安全验证的客户端建立TCP连接具体包括：

[0013] 接收客户端发送的加密后的密钥信息；

[0014] 根据自身的私钥和所述客户端的公钥对所述密钥信息进行解密运算，得到临时会话密钥和第一散列值；

[0015] 按照密码杂凑算法对所述临时会话密钥进行散列运算，当散列运算结果与所述第一散列值相同时，确定所述客户端通过安全验证；

[0016] 保存得到的所述临时会话密钥，为所述客户端建立TCP连接。

[0017] 进一步地，所述通过所述TCP连接，接收客户端发送的加密信息，获取所述加密信息中的HTTP请求具体包括：

[0018] 通过所述TCP连接，接收所述客户端发送的加密信息；

[0019] 根据所述临时会话密钥和所述客户端的公钥对接收的所述加密信息进行解密运算，得到HTTP请求和第二散列值；

[0020] 按照密码杂凑算法对所述HTTP请求进行散列运算，当散列运算结果与所述第二散列值相同时，获取所述HTTP请求。

[0021] 在第二种可能的实现方式中，所述根据所述HTTP请求中，获取相应的控制信息具体包括：

[0022] 按照表述性状态转移REST服务原则，从所述HTTP请求中提取统一资源定位符URL信息；

[0023] 获取所述URL信息中的相应的控制信息。

[0024] 在第三种可能的实现方式中，所述集中控制设备为美国电气和电子工程师协会IEEE802.15.4协议ZigBee发送模块。

[0025] 在第二方面，本发明实施例提供了一种数据传输系统，包括：服务器、集中控制设备和至少两个接收设备，所述服务器与所述集中控制设备相连，所述集中控制设备分别与所述至少两个接收设备相连，其中：

[0026] 所述服务器包括：

[0027] 连接建立单元，用于为通过安全验证的客户端建立传输控制协议TCP连接；

[0028] 请求获取单元，用于通过所述TCP连接，获取所述客户端发送的加密信息中的超文本传输协议HTTP请求；

[0029] 控制信息获取单元，用于根据所述HTTP请求，获取相应的控制信息，其中，所述控制信息包括待操作设备标识和操作类型；

[0030] 标准操作代码获取单元，用于查找操作对应表，获取与所述控制信息对应的标准操作指令；

[0031] 操作指令发送单元，用于将所述待操作设备标识和所述标准操作指令发送至集中控制设备；

[0032] 所述集中控制设备用于向与所述待操作设备标识对应的接收设备发送所述标准操作指令；

[0033] 所述接收设备用于根据接收到的所述标准操作指令，进行相应的操作。

[0034] 在第一种可能的实现方式中，所述连接建立单元具体用于：

[0035] 接收客户端发送的加密后的密钥信息；

[0036] 根据自身的私钥和所述客户端的公钥对所述密钥信息进行解密运算，得到临时会

话密钥和第一散列值；

[0037] 按照密码杂凑算法对所述临时会话密钥进行散列运算，当散列运算结果与所述第一散列值相同时，确定所述客户端通过安全验证；

[0038] 保存得到的所述临时会话密钥，为所述客户端建立TCP连接。

[0039] 进一步地，所述请求获取单元具体用于：

[0040] 通过所述TCP连接，接收所述客户端发送的加密信息；

[0041] 根据所述临时会话密钥和所述客户端的公钥对接收的所述加密信息进行解密运算，得到HTTP请求和第二散列值；

[0042] 按照密码杂凑算法对所述HTTP请求进行散列运算，当散列运算结果与所述第二散列值相同时，获取所述HTTP请求。

[0043] 在第二种可能的实现方式中，所述控制信息获取单元具体用于：

[0044] 按照表述性状态转移REST服务原则，从所述HTTP请求中提取统一资源定位符URL信息；

[0045] 获取所述URL信息中的相应的控制信息。

[0046] 在第三种可能的实现方式中，所述集中控制设备为美国电气和电子工程师协会IEEE802.15.4协议ZigBee发送模块，所述接收设备为ZigBee接收模块。

[0047] 本发明实施例通过在智能家居系统的数据传输过程中增加了安全控制机制，将客户端的控制指令发送至集中控制设备之前，增加了对用户身份的验证步骤和对用户发送的控制指令的验证步骤，增强了智能家居设备使用的安全性；通过使用集中控制设备与智能家居系统中的各接收设备相连，实现了对各接收设备的集中控制，减少了用户与智能家居设备之间的直接交互，通过根据客户端发送的控制指令，查找并发送与待操作设备相适应的标准操作指令，减少了用户管理和使用异构型智能家居设备时的复杂度，避免了“遥控器泛滥”情况的发生，为用户提供了极大的便利。

附图说明

[0048] 图1是本发明第一实施例的一种数据传输方法的流程图；

[0049] 图2是本发明第二实施例的一种数据传输过程的系统构架图；

[0050] 图3是本发明第三实施例的一种数据传输系统的结构图。

具体实施方式

[0051] 为了使本发明的目的、技术方案和优点更加清楚，下面结合附图对本发明具体实施例作进一步的详细描述。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部内容。

[0052] 第一实施例

[0053] 图1是本发明第一实施例的一种数据传输方法的流程图，本实施例的方法可以由数据传输系统来执行，该系统可以包括服务器、集中控制设备和至少两个接收设备，与安装于移动终端内的客户端交互配合。本实施例的方法具体由服务器执行，包括如下步骤：

[0054] 步骤110、为通过安全验证的客户端建立TCP(Transmission Control Protocol，

传输控制协议)连接。

[0055] 在本实施例中,智能家居系统用户可以通过安装于移动终端(例如:智能手机、平板电脑或者计算机等)中的客户端(例如:智能家居控制软件),经由服务器和集中控制设备向家居设备发送相应的控制指令。当服务器检测到客户端的接入请求后,会为通过安全验证的客户端建立TCP连接,提供(有线或者无线)通信链路。

[0056] 在本实施例中,服务器可以通过对称式密钥加密算法或者非对称式密钥加密算法对客户端进行安全验证,防止非法用户对智能家居系统中的家居设备进行操作。

[0057] 其中,对称式密钥加密算法是指服务器和客户端使用同一密钥对传输信息进行加密和解密,需要提供一条安全的渠道使得通信双方在首次通信时约定好一个不为第三方所知的共同密钥;非对称密钥加密算法是指每个人都有一对唯一对应的密钥:公开密钥和私有密钥,公钥对外公开,私钥由个人秘密保存;用其中一把密钥来加密,就只能用另一把密钥来解密。发送数据的一方用另一方的公钥对发送的信息进行加密,然后由接收者用自己的私钥进行解密。

[0058] 当然,本领域技术人员可以理解,在实际应用中还可以采取其他的方式对客户端进行安全验证,例如:通过用户名、密码方式登录服务器方式等,对此并不限定。

[0059] 步骤120、通过所述TCP连接,获取所述客户端发送的加密信息中的HTTP(Hypertext transfer protocol,超文本传输协议)请求。

[0060] 在本实施例中,服务器为客户端建立一条TCP连接之后,相当于在客户端自身之间建立了一条面向连接、可靠的通信链路,客户端可以通过服务器提供的特定端口,向服务器发送相应的信息数据。

[0061] 在本实施例中,为了防止客户端发送的信息数据被非法获取并更改,客户端向服务器发送的信息数据为经过加密的信息数据。服务器将收到的加密信息进行解密后,获取用户端发送的原始的HTTP请求。

[0062] 其中,HTTP协议是一种基于请求与响应模式的、无状态的、应用层协议,常基于TCP连接。客户端通过向服务器发送请求方法和路径来请求服务。HTTP协议支持客户端/服务器模式:当客户端向服务器请求服务时,只需传送请求方法和路径。常用的请求方法有GET(获取)、POST(提交)等。每种方法规定了客户端与服务器的不同联系类型。一次HTTP操作称为一个事务,其工作流程可分为四部:1)客户端与服务器建立连接,HTTP工作开始。2)建立连接之后,客户端向服务器发送请求。3)服务器接到请求后,给予相应的响应信息。4)客户端接受服务器返回的响应信息并通过浏览器等方式显示在用户的显示屏上,之后客户端与服务器断开连接。

[0063] 步骤130、根据所述HTTP请求,获取相应的控制信息,其中,所述控制信息包括待操作设备标识和操作类型。

[0064] 在本实施例中,客户端可以以HTTP GET请求的方式或者HTTP POST请求的方式,发送相应的控制信息。其中,客户端发送的控制信息中包括待操作设备标识和操作类型。

[0065] 举例而言,一个智能家居系统中包括各种智能家居设备,如:灯泡、窗帘和插座等。在整个家居系统中,每一个智能家居设备都具有一个唯一的设备标识,如:灯泡001、窗帘002和插座003等,每一个智能家居设备都具有相应的操作类型,如:对灯泡的操作可以为打开灯泡、关闭灯泡和调整灯泡亮度;对窗帘的操作可以为升起窗帘、降下窗帘和停止窗帘移

动;对插座的操作可以为断开开关和打开开关等。客户端通过发送待操作设备标识和操作类型,可以实现对智能家居系统中的家居设备的控制。

[0066] 在本实施例的一个优选的实施方式中,客户端将上述控制信息写入发送的HTTP请求中的URL(Uniform Resource Locator,统一资源定位符)信息中。服务器按照REST(Representational State Transfer,表述性状态转移)服务原则,从所述HTTP请求中提取URL信息,进而获取所述控制信息。

[0067] 步骤140、查找操作对应表,获取与所述控制信息对应的标准操作指令。

[0068] 在本实施例中,智能家居系统中的智能家居设备可以为同一生产厂家也可以为不同生产厂家。当上述家居设备属于不同生产厂家时,不同的家居设备的操作控制指令也不尽相同。为了实现上述智能家居设备的集中控制,在服务器中需要存储有操作对象表,该操作对象表中记录了不同家居设备的不同操作类型所对应的标准操作指令。其中,所述标准操作指令为与对应的家居设备相符合的操作控制指令。

[0069] 当服务器获取待操作设备标识和操作类型,查找上述操作对象表,获取对应的标准操作指令。

[0070] 举例而言,服务器中存储的操作对象表的中数据的存储形式如表1所示:

[0071] 表1

[0072]

设备标识	操作类型	标准操作指令
001	打开灯泡	OPEN
	关闭灯泡	CLOSE
002	升起窗帘	UP
	降下窗帘	DOWN
003	打开开关	TURN ON
	关闭开关	SHUT DOWN

[0073] 当服务器收到待操作设备标识为001、操作类型为关闭灯泡的操作时,将会查找表1获取与设备001相适应的标准操作指令“CLOSE”,当设备001收到“CLOSE”指令时,将会进行关闭灯泡的操作。

[0074] 步骤150、将所述待操作设备标识和所述标准操作指令发送至集中控制设备。

[0075] 在本实施例中,当服务器根据所述控制信息获取相应的标准操作指令后,将所述待操作设备标识和所述标准操作指令发送至集中控制设备。

[0076] 在本实施例的一个优选的实施方式中,集中控制设备为一个ZigBee的发送模块,该模块将接收到的所述待操作设备标识和所述标准操作指令以无线的方式发送至与所述待操作设备标识对应的接收设备,控制接收设备进行与所述标准操作指令对应的操作。

[0077] 本发明实施例通过在智能家居系统的数据传输过程中增加了安全控制机制,将客

户端的控制指令发送至集中控制设备之前，增加了对用户身份的验证步骤和对用户发送的控制指令的验证步骤，增强了智能家居设备使用的安全性；通过使用集中控制设备与智能家居系统中的各接收设备相连，实现了对各接收设备的集中控制，减少了用户与智能家居设备之间的直接交互，通过根据客户端发送的控制指令，查找并发送与待操作设备相适应的标准操作指令，减少了用户管理和使用异构型智能家居设备时的复杂度，避免了“遥控器泛滥”情况的发生，为用户提供了极大的便利。

[0078] 在上述技术方案的基础上，所述为通过安全验证的客户端建立TCP连接可以优化为：接收客户端发送的加密后的密钥信息；根据自身的私钥和所述客户端的公钥对所述密钥信息进行解密运算，得到临时会话密钥和第一散列值；按照SM3(码杂凑算法)对所述临时会话密钥进行散列运算，当散列运算结果与所述第一散列值相同时，确定所述客户端通过安全验证；保存得到的所述临时会话密钥，为所述客户端建立TCP连接。

[0079] 在本优选实施方式中，客户端和服务器使用SM2(椭圆曲线公钥密码算法)作为公钥密码算法，SM3算法进行散列运算，SM4(分组密码算法)生成临时会话密钥。其中，服务器中存储有SM2私钥k_s，同时公开SM2公钥k_p，每个客户端在购买或者加入智能家居系统时，会得到授权，系统将为用户生成一份SM2密钥对，分别是私钥k_s'和公钥k_p'，由服务器存储k_p'，客户端存储k_s'。

[0080] 在建立TCP连接之前，客户端通过SM4算法生成临时会话密钥k。由客户端对其进行签名，签名过程如下：

[0081] 使用SM3算法对k进行散列，得到散列结果f(k)；

[0082] 使用自身的私钥k_s'对k和f(k)进行签名，得到$k_s'(k,f(k))$；

[0083] 使用服务器的公钥k_p进行加密，得到$k_p(k_s'(k,f(k)))$，将加密结果发送至服务器；

[0084] 服务器使用自身私钥k_s和客户端公钥k_p'对加密结果进行解密，得到(k,f(k))；

[0085] 服务器使用SM3算法对得到k进行散列，验证散列结果是否与f(k)的值相同。

[0086] 其中，如果计算得到的散列值与用户发来f(k)一致，则认为在之前的传输过程中，会话密钥没有被截取和篡改过，进而将k作为此次通信的会话密钥，为该客户端建立TCP连接；如果计算得到的散列值与用户发来f(k)不一致，则报告错误并终止通信。

[0087] 在上述各技术方案的基础上，所述通过所述TCP连接，接收客户端发送的加密信息，获取所述加密信息中的HTTP请求可以优化为：通过所述TCP连接，接收所述客户端发送的加密信息；根据所述临时会话密钥和所述客户端的公钥对接收的所述加密信息进行解密运算，得到HTTP请求和第二散列值；按照密码杂凑SM3算法对所述HTTP请求进行散列运算，当散列运算结果与所述第二散列值相同时，获取所述HTTP请求。

[0088] 在本优选实施方式中，一旦会话密钥k产生并且TCP连接建立之后，客户端与服务器就可以通过临时会话密钥传输控制信息，步骤如下：

[0089] 客户端使用SM3算法对消息x进行散列，得到散列值f(x)；

[0090] 客户端使用自身私钥k_s'对f(x)进行签名得到$k_s'(x,f(x))$；

[0091] 客户端使用临时会话密钥k对签名结果进行加密得到$k(k_s'(x,f(x)))$；

[0092] 客户端将加密结果发送给服务器；

[0093] 服务器使用临时会话密钥k解密得到$k_s'(x,f(x))$；

[0094] 服务器使用客户端公钥k_p'解密$k_s'(x,f(x))$得到(x,f(x))；

[0095] 服务器使用SM3算法验证控制信息是否被修改:如果对x进行散列运算得到的结果与f(x)相同,则证明在传输过程中,没有被更改过,是合法的,则可以继续获取消息x中的控制信息;否则,则证明消息x是不合法的,丢弃该消息。

[0096] 第二实施例

[0097] 在图2中示出了本发明第二实施例的一种数据传输过程的系统构架图,本实施例以上述各实施例为基础,将上述各实施例的数据传输方法按照逻辑分层的方式分层执行。如图2所示,所述系统包括:用户层210、支持层220、网络层230、控制层240和设备层250。用户层210负责以应用层HTTP请求的形式发送控制指令,支持层220负责对指令进行权限验证、解密并提交给网络层230,网络层230负责获取控制指令中的设备标识和标准操作指令,将其提交给控制层240,最后由控制层240完成对设备层250设备的直接控制。

[0098] 本发明实施例通过在智能家居系统的数据传输过程中增加了安全控制机制,将客户端的控制指令发送至集中控制设备之前,增加了对用户身份的验证步骤和对用户发送的控制指令的验证步骤,增强了智能家居设备使用的安全性;通过使用集中控制设备与智能家居系统中的各接收设备相连,实现了对各接收设备的集中控制,减少了用户与智能家居设备之间的直接交互,通过根据客户端发送的控制指令,查找并发送与待操作设备相适应的标准操作指令,减少了用户管理和使用异构型智能家居设备时的复杂度,避免了“遥控器泛滥”情况的发生,为用户提供了极大的便利。

[0099] 第三实施例

[0100] 在图3中示出了本发明第三实施例的一种数据传输系统的结构图。如图3所示,所述系统包括:

[0101] 服务器31、集中控制设备32和至少两个接收设备,服务器31与集中控制设备相连32,集中控制设备分别与至少两个接收设备相连,其中:

[0102] 服务器31包括:

[0103] 连接建立单元311,用于为通过安全验证的客户端建立TCP连接;

[0104] 请求获取单元312,用于通过所述TCP连接,获取所述客户端发送的加密信息中的HTTP请求;

[0105] 控制信息获取单元313,用于根据所述HTTP请求,获取相应的控制信息,其中,所述控制信息包括待操作设备标识和操作类型;

[0106] 标准操作代码获取单元314,用于查找操作对应表,获取与所述控制信息对应的标准操作指令;

[0107] 操作指令发送单元315,用于将所述待操作设备标识和所述标准操作指令发送至集中控制设备;

[0108] 集中控制设备32用于向与所述待操作设备标识对应的接收设备发送所述标准操作指令;

[0109] 所述接收设备用于根据接收到的所述标准操作指令,进行相应的操作。

[0110] 本发明实施例通过在智能家居系统的数据传输过程中增加了安全控制机制,将客户端的控制指令发送至集中控制设备之前,增加了对用户身份的验证步骤和对用户发送的控制指令的验证步骤,增强了智能家居设备使用的安全性;通过使用集中控制设备与智能家居系统中的各接收设备相连,实现了对各接收设备的集中控制,减少了用户与智能家居

设备之间的直接交互，通过根据客户端发送的控制指令，查找并发送与待操作设备相适应的标准操作指令，减少了用户管理和使用异构型智能家居设备时的复杂度，避免了“遥控器泛滥”情况的发生，为用户提供了极大的便利。

[0111] 在上述各实施例的基础上，连接建立单元311具体用于：

[0112] 接收客户端发送的加密后的密钥信息；

[0113] 根据自身的私钥和所述客户端的公钥对所述密钥信息进行解密运算，得到临时会话密钥和第一散列值；

[0114] 按照密码杂凑算法对所述临时会话密钥进行散列运算，当散列运算结果与所述第一散列值相同时，确定所述客户端通过安全验证；

[0115] 保存得到的所述临时会话密钥，为所述客户端建立TCP连接。

[0116] 在上述各实施例的基础上，请求获取单元312具体用于：

[0117] 通过所述TCP连接，接收所述客户端发送的加密信息；

[0118] 根据所述临时会话密钥和所述客户端的公钥对接收的所述加密信息进行解密运算，得到HTTP请求和第二散列值；

[0119] 按照密码杂凑算法对所述HTTP请求进行散列运算，当散列运算结果与所述第二散列值相同时，获取所述HTTP请求。

[0120] 在上述各实施例的基础上，控制信息获取单元313具体用于：

[0121] 按照REST服务原则，从所述HTTP请求中URL信息；

[0122] 获取所述URL信息中的相应的控制信息。

[0123] 在上述各实施例的基础上，集中控制设备32为ZigBee发送模块，接收设备为ZigBee接收模块。

[0124] 本发明实施例所提供的数据传输系统可以用于执行本发明任意实施例提供的数据传输方法，具备相应的功能模块，达到同样的技术效果。

[0125] 显然，本领域技术人员应该明白，上述的本发明的各模块或各步骤可以通过如上所述的服务器实施。可选地，本发明实施例可以用计算机装置可执行的程序来实现，从而可以将它们存储在存储装置中由处理器来执行，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等；或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件的结合。

[0126] 以上所述仅为本发明的优选实施例，并不用于限制本发明，对于本领域技术人员而言，本发明可以有各种改动和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

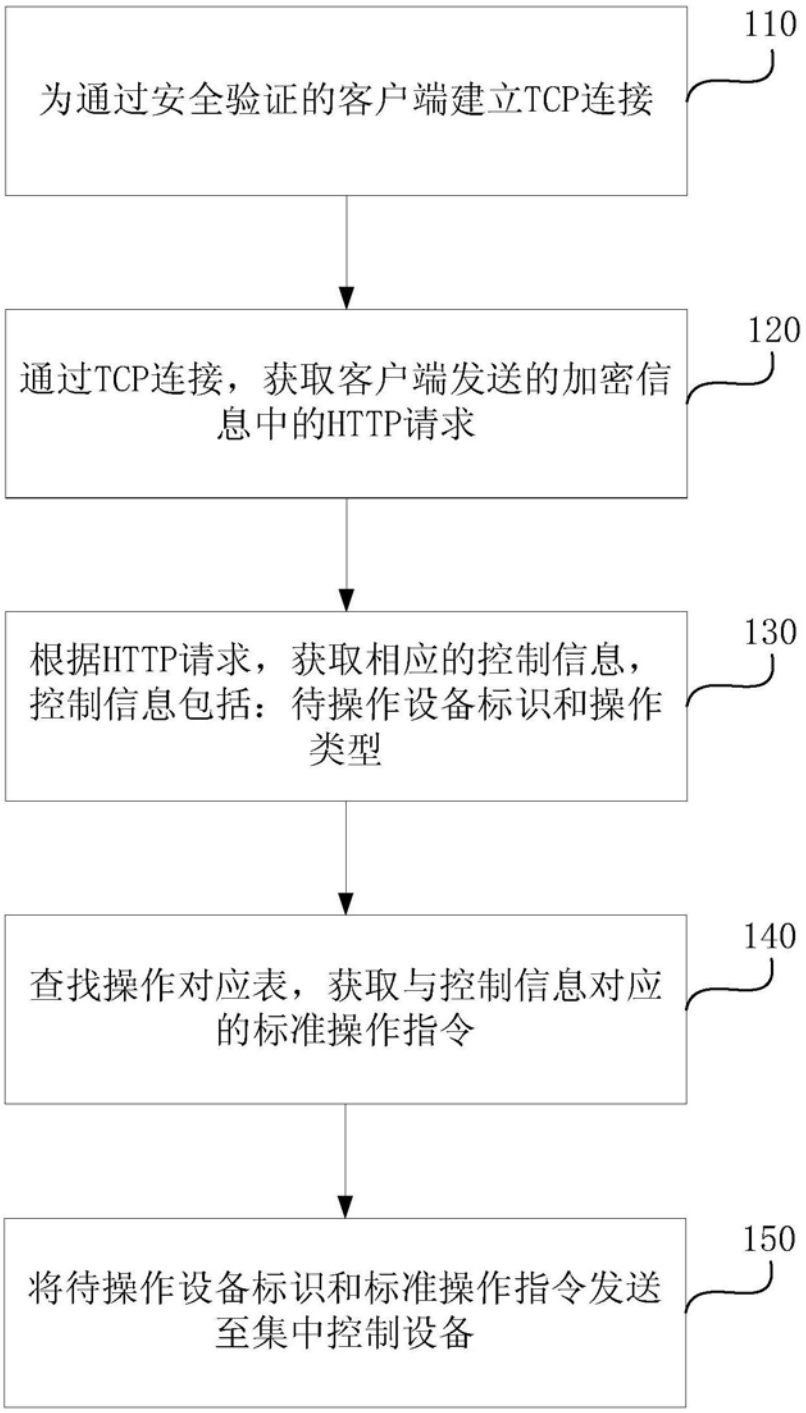

110
为通过安全验证的客户端建立TCP连接
120
通过TCP连接，获取客户端发送的加密信息中的HTTP请求
130
根据HTTP请求，获取相应的控制信息，控制信息包括：待操作设备标识和操作类型
140
查找操作对应表，获取与控制信息对应的标准操作指令
150
将待操作设备标识和标准操作指令发送至集中控制设备

图1

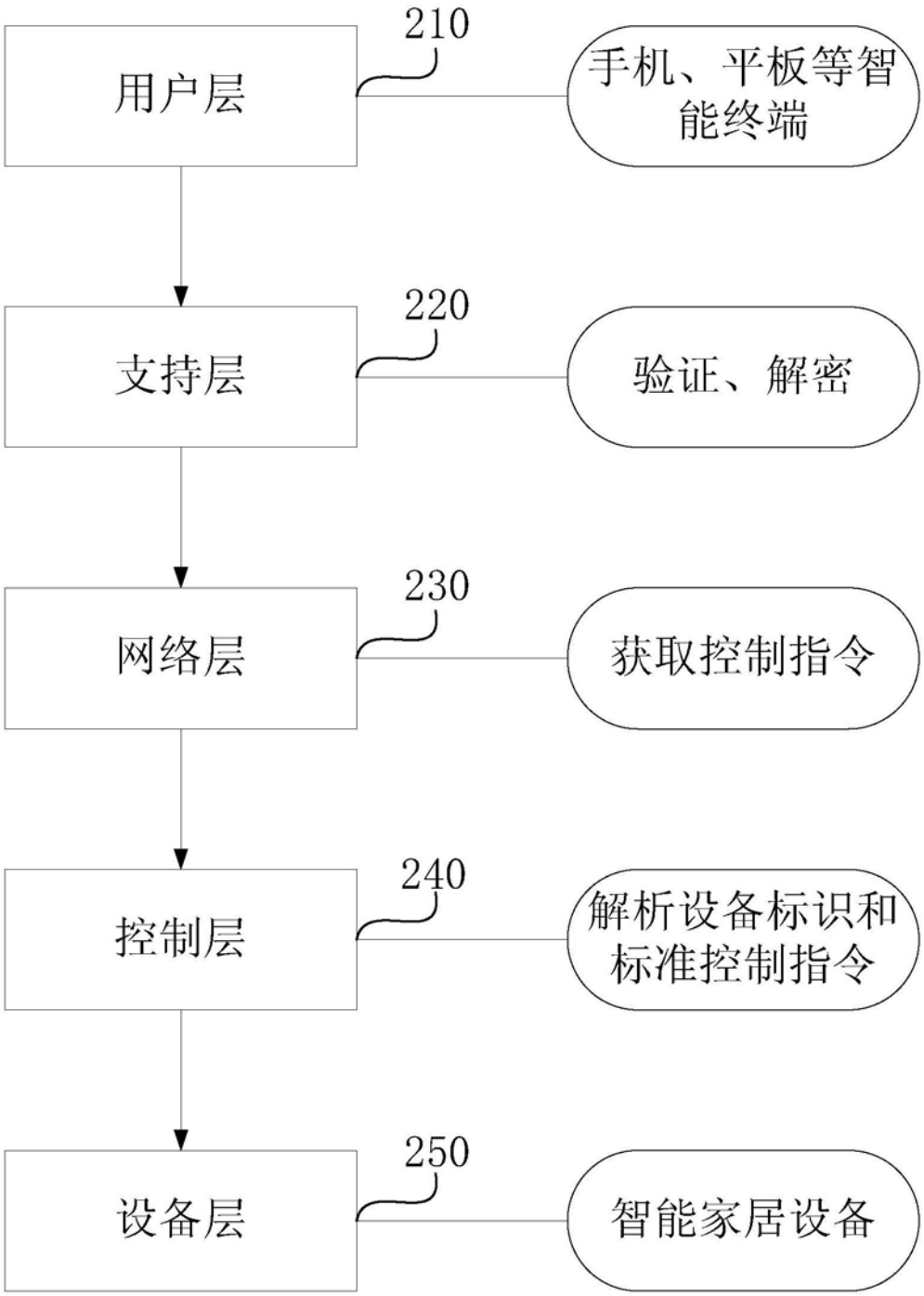

用户层
210
手机、平板等智能终端
支持层
220
验证、解密
网络层
230
获取控制指令
控制层
240
解析设备标识和标准控制指令
设备层
250
智能家居设备

图2

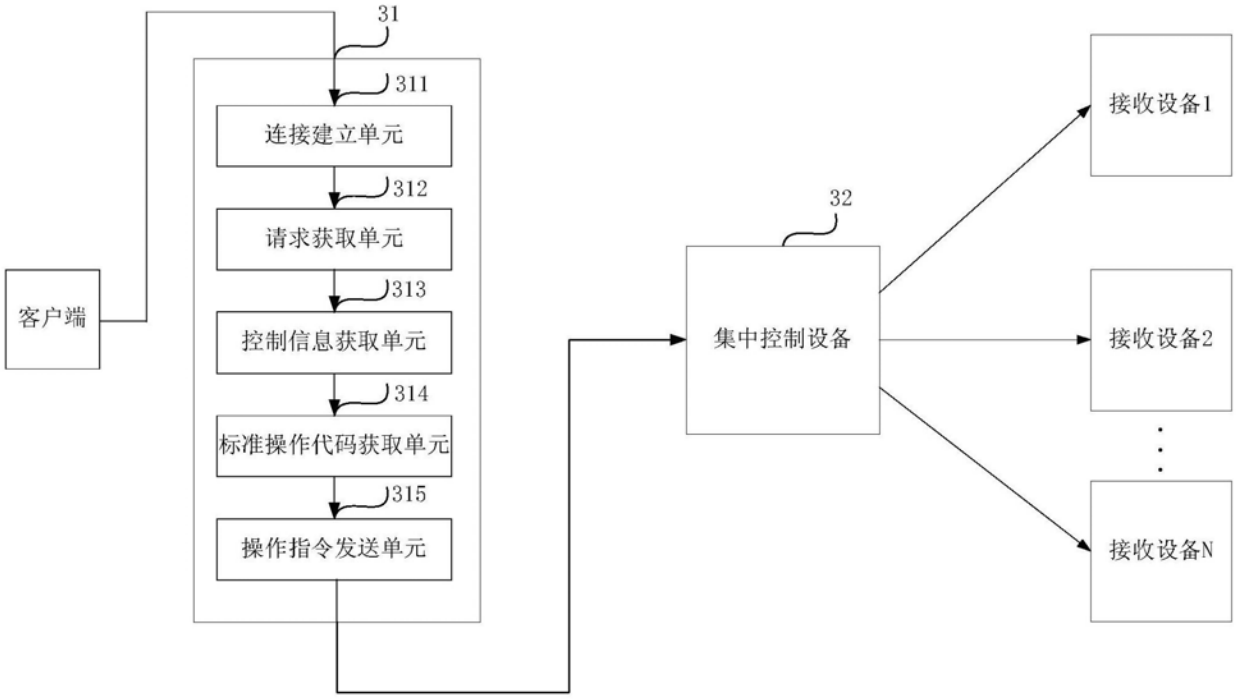

31
311
连接建立单元
312
请求获取单元
313
控制信息获取单元
314
标准操作代码获取单元
315
操作指令发送单元
客户端
32
集中控制设备
接收设备1
接收设备2
接收设备N

图3