(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 111552215 B
(45)授权公告日 2022.02.11

(21)申请号 202010442163.0

(22)申请日 2020.05.22

(65)同一申请的已公布的文献号
申请公布号 CN 111552215 A

(43)申请公布日 2020.08.18

(73)专利权人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 黄珂

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 罗建民 杜丹丹

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/12(2022.01)
G16Y 30/10(2020.01)
G16Y 40/50(2020.01)

(56)对比文件
CN 110300102 A,2019.10.01
CN 108632293 A,2018.10.09
CN 107749848 A,2018.03.02
CN 109005220 A,2018.12.14
CN 110417567 A,2019.11.05
CN 110166411 A,2019.08.23
CN 111045690 A,2020.04.21
CN 109492380 A,2019.03.19
CN 109714173 A,2019.05.03
CN 110086821 A,2019.08.02
CN 110233868 A,2019.09.13
CN 108388806 A,2018.08.10
CN 109714174 A,2019.05.03
CN 110601844 A,2019.12.20
CN 110958123 A,2020.04.03
CN 108306887 A,2018.07.20
CN 110557384 A,2019.12.10

审查员 刘亦非

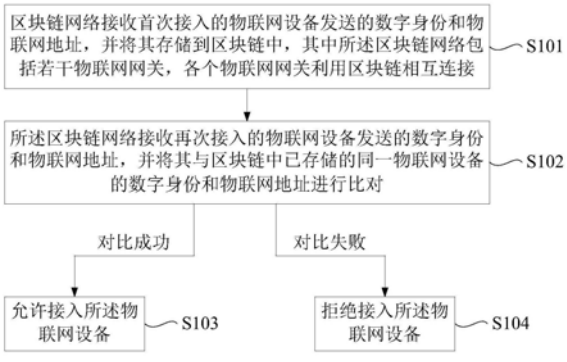
权利要求书2页 说明书8页 附图3页

(54)发明名称

物联网设备安全防护方法和系统

(57)摘要

本公开实施例提供一种物联网设备安全防护方法和系统，其中，所述方法包括：区块链网络接收首次接入的物联网设备发送的数字身份和物联网地址，并将其存储到区块链中，其中所述区块链网络包括若干物联网网关，各个物联网网关利用区块链相互连接；所述区块链网络接收再次接入的物联网设备发送的数字身份和物联网地址，并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对；以及，若比对失败，则拒绝接入所述物联网设备。本公开实施例中，通过将接入的物联网设备与之前存储的同一物联网设备的数字身份和物联网地址进行比对，并根据比对结果决定是否允许接入该物联网设备，实现了对底层各个感知节点的物联网设备的安全防护。



CN 111552215 B

1.一种物联网设备安全防护方法,其特征在于,包括:

区块链网络接收首次接入的物联网设备发送的包含第一密文的第一请求信息,其中所述区块链网络包括若干物联网网关,各个物联网网关利用区块链相互连接,所述第一密文为使用区块链公钥生成的加密后的所述物联网设备的数字身份和物联网地址;

所述区块链网络发送包含所述第一请求信息的第一广播消息至各个物联网网关,并根据区块链共识机制选出响应所述第一请求信息的第一物联网网关;

所述第一物联网网关对所述第一密文进行解密以得到包含所述物联网设备的数字身份和物联网地址的第一明文;

所述第一物联网网关将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关;以及,

所述其他各第二物联网网关对所述第一明文进行预设处理后将所述物联网设备的数字身份和物联网地址存储到区块链的区块中;

所述区块链网络接收再次接入的物联网设备发送的数字身份和物联网地址,并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对;以及,

若比对失败,则拒绝接入所述物联网设备。

2.根据权利要求1所述的方法,其特征在于,在所述第一物联网网关将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关之前,还包括:

所述第一物联网网关判断所述物联网设备的数字身份和物联网地址是否已被注册占用;以及,

若未被注册占用,再将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关。

3.根据权利要求1或2所述的方法,其特征在于,所述其他各第二物联网网关对所述第一明文进行预设处理后将所述物联网设备的数字身份和物联网地址存储到区块链的区块中,包括:

所述其他各第二物联网网关对所述第一明文进行数字签名,并返回给所述第一物联网网关;

所述第一物联网网关将第三广播消息发送给所述其他各第二物联网网关,所述第三广播消息包括所述物联网设备的数字身份、物联网地址和数字签名;以及,

所述其他各第二物联网网关基于所述第三广播消息将所述物联网设备的数字身份和物联网地址存储到区块链的区块中。

4.根据权利要求1所述的方法,其特征在于,所述区块链网络接收再次接入的物联网设备发送的数字身份和物联网地址,并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对,包括:

所述第一物联网网关接收再次接入的物联网设备发送的包含第二密文的第二请求消息,其中所述第二密文为使用区块链随机秘钥生成的加密后的再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息;

所述第一物联网网关对所述第二密文进行解密以得到包含再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息的第二明文;

所述第一物联网网关将包括所述第二明文的第四广播消息发送给所述区块链网络中

的其他各第二物联网网关;以及,

所述其他各第二物联网网关将再次接入的物联网设备的数字身份和物联网地址与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对,并对比对结果进行签名。

5.一种物联网设备安全防护系统,其特征在于,包括区块链网络,所述区块链网络包括若干物联网网关,各个物联网网关利用区块链相互连接,

所述区块链网络设置为:接收首次接入的物联网设备发送的包含第一密文的第一请求信息,其中所述第一密文为使用区块链公钥生成的加密后的所述物联网设备的数字身份和物联网地址;以及,发送包含所述第一请求信息的第一广播消息至各个物联网网关,并根据区块链共识机制选出响应所述第一请求信息的第一物联网网关;

所述第一物联网网关设置为:对所述第一密文进行解密以得到包含所述物联网设备的数字身份和物联网地址的第一明文;以及,将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关;

所述其他各第二物联网网关设置为:对所述第一明文进行预设处理后将所述物联网设备的数字身份和物联网地址存储到区块链的区块中;

所述区块链网络还设置为:接收再次接入的物联网设备发送的数字身份和物联网地址,并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对;以及,

若比对失败,则拒绝接入所述物联网设备。

6.根据权利要求5所述的系统,其特征在于,所述第一物联网网关还设置为:

判断所述物联网设备的数字身份和物联网地址是否已被注册占用;以及,

若未被注册占用,再将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关。

7.根据权利要求5或6所述的系统,其特征在于,所述其他各第二物联网网关还设置为:对所述第一明文进行数字签名,并返回给所述第一物联网网关;

所述第一物联网网关还设置为:将第三广播消息发送给所述其他各第二物联网网关,所述第三广播消息包括所述物联网设备的数字身份、物联网地址和数字签名;

所述其他各第二物联网网关还设置为:基于所述第三广播消息将所述物联网设备的数字身份和物联网地址存储到区块链的区块中。

8.根据权利要求5所述的系统,其特征在于,所述第一物联网网关还设置为:接收再次接入的物联网设备发送的包含第二密文的第二请求消息,其中所述第二密文为使用区块链随机秘钥生成的加密后的再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息;

对所述第二密文进行解密以得到包含再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息的第二明文;以及,

将包括所述第二明文的第四广播消息发送给所述区块链网络中的其他各第二物联网网关;

所述其他各第二物联网网关还设置为:将再次接入的物联网设备的数字身份和物联网地址与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对,并对比对结果进行签名。

物联网设备安全防护方法和系统

技术领域

[0001] 本公开涉及通信技术领域，尤其涉及一种物联网设备安全防护方法，以及一种物联网设备安全防护系统。

背景技术

[0002] 物联网(The Internet of Things，简称IOT)是指通过各种信息传感器、射频识别技术、全球定位系统、红外感应器、激光扫描器等各种装置与技术，实时采集任何需要监控、连接、互动的物体或过程，采集其声、光、热、电、力学、化学、生物、位置等各种需要的信息，通过各类可能的网络接入，实现物与物、物与人的泛在连接，实现对物品和过程的智能化感知、识别和管理。

[0003] 基于成本和管理等方面的因素，目前大量物联网设备，例如家庭摄像头、智能灯、路灯监视器等，缺乏有效的安全保护机制。这些物联网设备很容易被劫持，被劫持的物联网设备经常被恶意软件肆意控制，并对特定的网络服务进行分布式拒绝服务攻击(DDoS，Distributed denial of service attack)。

[0004] 因此，提出一种能够对底层各个感知节点的物联网设备进行安全防护的方案是目前亟待解决的问题。

发明内容

[0005] 为了至少部分解决现有技术中存在的技术问题而完成了本公开。

[0006] 根据本公开实施例的一方面，提供一种物联网设备安全防护方法，所述方法包括：

[0007] 区块链网络接收首次接入的物联网设备发送的数字身份和物联网地址，并将其存储到区块链中，其中所述区块链网络包括若干物联网网关，各个物联网网关利用区块链相互连接；

[0008] 所述区块链网络接收再次接入的物联网设备发送的数字身份和物联网地址，并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对；以及，

[0009] 若比对失败，则拒绝接入所述物联网设备。

[0010] 根据本公开实施例的另一方面，提供一种物联网设备安全防护系统，所述系统包括区块链网络，所述区块链网络包括若干物联网网关，各个物联网网关利用区块链相互连接，

[0011] 所述区块链网络设置为：接收首次接入的物联网设备发送的数字身份和物联网地址，并将其存储到区块链中；

[0012] 所述区块链网络还设置为：接收再次接入的物联网设备发送的数字身份和物联网地址，并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对；以及，

[0013] 若比对失败，则拒绝接入所述物联网设备。

[0014] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0015] 本公开实施例提供的物联网设备安全防护方法和系统中，各个物联网网关利用区块链相互连接以构成区块链网络，通过将接入的物联网设备的数字身份和物联网地址与之前存储的同一物联网设备的数字身份和物联网地址进行比对，并根据比对结果决定是否允许接入该物联网设备，实现了对底层各个感知节点的物联网设备的安全防护。

[0016] 本公开的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本公开而了解。本公开的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0017] 附图用来提供对本公开技术方案的进一步理解，并且构成说明书的一部分，与本公开的实施例一起用于解释本公开的技术方案，并不构成对本公开技术方案的限制。

[0018] 图1为本公开实施例提供的一种物联网设备安全防护方法的流程示意图；

[0019] 图2为本公开实施例提供的另一种物联网设备安全防护方法的流程示意图；

[0020] 图3为本公开实施例提供的一种物联网设备安全防护系统的示意图；

[0021] 图4为本公开实施例提供的另一种物联网设备安全防护系统的示意图。

具体实施方式

[0022] 为使本公开实施例的目的、技术方案和优点更加清楚，以下结合附图对本公开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公开，并不用于限制本公开。

[0023] 需要说明的是，本公开的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序；并且，在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互任意组合。

[0024] 图1为本公开实施例提供的一种物联网设备安全防护方法的流程示意图。如图1所示，所述方法包括如下步骤S101至S104。

[0025] S101.区块链网络接收首次接入的物联网设备发送的数字身份和物联网地址，并将其存储到区块链中，其中所述区块链网络包括若干物联网网关，各个物联网网关利用区块链相互连接；

[0026] S102.所述区块链网络接收再次接入的物联网设备发送的数字身份和物联网地址，并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对；

[0027] S103.若比对成功，则允许接入所述物联网设备；

[0028] S104.若比对失败，则拒绝接入所述物联网设备。

[0029] 本公开实施例中，各个物联网网关利用区块链相互连接以构成区块链网络，通过将接入的物联网设备的数字身份和物联网地址与之前存储的同一物联网设备的数字身份和物联网地址进行比对，并根据比对结果决定是否允许接入该物联网设备，实现了对底层各个感知节点的物联网设备的安全防护。

[0030] 在一种实施方式中，步骤S101具体包括如下步骤S1011至S1015。

[0031] S1011.所述区块链网络接收首次接入的物联网设备发送的包含第一密文的第一请求信息，其中所述第一密文为使用区块链公钥生成的加密后的所述物联网设备的数字身

份和物联网地址；

[0032] S1012.所述区块链网络发送包含所述第一请求信息的第一广播消息至各个物联网网关，并根据区块链共识机制选出响应所述第一请求信息的第一物联网网关；

[0033] S1013.所述第一物联网网关对所述第一密文进行解密以得到包含所述物联网设备的数字身份和物联网地址的第一明文；

[0034] S1014.所述第一物联网网关将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关；

[0035] S1015.所述其他各第二物联网网关对所述第一明文进行预设处理后将所述物联网设备的数字身份和物联网地址存储到区块链的区块中。

[0036] 在一种实施方式中，在步骤S1013之后，以及步骤S1014之前，还包括如下步骤S1016：

[0037] S1016.所述第一物联网网关判断所述物联网设备的数字身份和物联网地址是否已被注册占用，若已被注册占用，则执行步骤S102；若未被注册占用，则执行步骤S1014，将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关。

[0038] 在一种实施方式中，步骤S1015具体包括如下步骤Sa至Sc。

[0039] Sa.所述其他各第二物联网网关对所述第一明文进行数字签名，并返回给所述第一物联网网关；

[0040] Sb.所述第一物联网网关将第三广播消息发送给所述其他各第二物联网网关，所述第三广播消息包括所述物联网设备的数字身份、物联网地址和数字签名；

[0041] Sc.所述其他各第二物联网网关基于所述第三广播消息将所述物联网设备的数字身份和物联网地址存储到区块链的区块中。

[0042] 在一种实施方式中，步骤S102具体包括如下步骤S1021至S1024。

[0043] S1021.所述第一物联网网关接收再次接入的物联网设备发送的包含第二密文的第二请求消息，其中所述第二密文为使用区块链随机秘钥生成的加密后的再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息(如指令、数据等)；

[0044] S1022.所述第一物联网网关对所述第二密文进行解密以得到包含再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息的第二明文；

[0045] S1023.所述第一物联网网关将包括所述第二明文的第四广播消息发送给所述区块链网络中的其他各第二物联网网关；

[0046] S1024.所述其他各第二物联网网关将再次接入的物联网设备的数字身份和物联网地址与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对，并对比对结果进行签名，以确保比对结果的真实性。

[0047] 相应地，在步骤S103中，若比对成功，则所述第一物联网网关允许接入所述物联网设备；在步骤S104中，若比对失败，则所述第一物联网网关拒绝接入所述物联网设备。

[0048] 本公开实施例提供的物联网设备安全防护方法，通过各个物联网网关利用区块链相互连接以构成区块链网络，对底层各个感知节点的物联网设备进行安全防护和远程控制，共同监控、标识和处理物联网设备的网络活动，并使用加密技术和安全算法来保护物联网设备的数字身份，避免被劫持的物联网设备被恶意软件控制而对特定的网络服务进行分布式拒绝服务攻击。

[0049] 图2为本公开实施例提供的另一种物联网设备安全防护方法的流程示意图。如图2所示，所述方法包括如下步骤S201至S214。

[0050] S201.物联网设备首次接入物联网系统时，发送包含第一密文的第一请求信息至区块链网络，其中所述区块链网络包括若干物联网网关，各个物联网网关利用区块链相互连接，所述第一密文为使用区块链公钥生成的加密后的所述物联网设备的数字身份和物联网地址；

[0051] S202.所述区块链网络发送包含所述第一请求信息的第一广播消息至各个物联网网关，并根据区块链共识机制选出响应所述第一请求信息的第一物联网网关；

[0052] S203.所述第一物联网网关对所述第一密文进行解密以得到包含所述物联网设备的数字身份和物联网地址的第一明文；

[0053] S204.所述第一物联网网关判断所述物联网设备的数字身份和物联网地址是否已被注册占用，若已被注册占用，则执行步骤S209；若未被注册占用，则执行步骤S205；

[0054] S205.所述第一物联网网关将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关；

[0055] S206.所述其他各第二物联网网关对所述第一明文进行数字签名，并返回给所述第一物联网网关；

[0056] S207.所述第一物联网网关将第三广播消息发送给所述其他各第二物联网网关，所述第三广播消息包括所述物联网设备的数字身份、物联网地址和数字签名；

[0057] S208.所述其他各第二物联网网关基于所述第三广播消息将所述物联网设备的数字身份和物联网地址存储到区块链的区块中；

[0058] S209.所述物联网设备再次接入物联网系统时，发送包含第二密文的第二请求消息至所述第一物联网网关，其中所述第二密文为使用区块链随机秘钥生成的加密后的再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息(如指令、数据等)；

[0059] S210.所述第一物联网网关对所述第二密文进行解密以得到包含再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息的第二明文；

[0060] S211.所述第一物联网网关将包括所述第二明文的第四广播消息发送给所述区块链网络中的其他各第二物联网网关；

[0061] S212.所述其他各第二物联网网关将再次接入的物联网设备的数字身份和物联网地址与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对，并对比对结果进行签名，以确保比对结果的真实性；

[0062] S213.若比对成功，则所述第一物联网网关允许接入所述物联网设备；

[0063] S214.若比对失败，则所述第一物联网网关拒绝接入所述物联网设备，并在所述物联网设备访问目标服务器之前切断网络连接。

[0064] 本公开实施例提供的物联网设备安全防护方法，通过各个物联网网关利用区块链相互连接以构成区块链网络，对底层各个感知节点的物联网设备进行安全防护和远程控制，共同监控、标识和处理物联网设备的网络活动，并使用加密技术和安全算法来保护物联网设备的数字身份，避免被劫持的物联网设备被恶意软件控制而对特定的网络服务进行分布式拒绝服务攻击。

[0065] 图3为本公开实施例提供的一种物联网设备安全防护系统的示意图。如图3所示，

所述系统100包括区块链网络101，所述区块链网络101包括若干物联网网关，各个物联网网关利用区块链相互连接。

[0066] 其中，所述区块链网络101设置为：接收首次接入的物联网设备102发送的数字身份和物联网地址，并将其存储到区块链中；所述区块链网络101还设置为：接收再次接入的物联网设备102发送的数字身份和物联网地址，并将其与区块链中已存储的同一物联网设备102的数字身份和物联网地址进行比对；若比对成功，则允许接入所述物联网设备102；若比对失败，则拒绝接入所述物联网设备102。

[0067] 本公开实施例中，各个物联网网关利用区块链相互连接以构成区块链网络，通过将接入的物联网设备的数字身份和物联网地址与之前存储的同一物联网设备的数字身份和物联网地址进行比对，并根据比对结果决定是否允许接入该物联网设备，实现了对底层各个感知节点的物联网设备的安全防护。

[0068] 在一种实施方式中，所述区块链网络101具体设置为：

[0069] 接收首次接入的物联网设备102发送的包含第一密文的第一请求信息，其中所述第一密文为使用区块链公钥生成的加密后的所述物联网设备102的数字身份和物联网地址；以及，发送包含所述第一请求信息的第一广播消息至各个物联网网关，并根据区块链共识机制选出响应所述第一请求信息的第一物联网网关1011。

[0070] 所述第一物联网网关1011设置为：对所述第一密文进行解密以得到包含所述物联网设备102的数字身份和物联网地址的第一明文；以及，将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关1012。

[0071] 所述其他各第二物联网网关1012设置为：对所述第一明文进行预设处理后将所述物联网设备102的数字身份和物联网地址存储到区块链的区块中。

[0072] 在一种实施方式中，所述第一物联网网关1011还设置为：判断所述物联网设备102的数字身份和物联网地址是否已被注册占用；以及，若未被注册占用，再将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关1012。

[0073] 在一种实施方式中，所述其他各第二物联网网关1012还设置为：对所述第一明文进行数字签名，并返回给所述第一物联网网关1011；

[0074] 所述第一物联网网关1011还设置为：将第三广播消息发送给所述其他各第二物联网网关1012，所述第三广播消息包括所述物联网设备102的数字身份、物联网地址和数字签名；

[0075] 所述其他各第二物联网网关1012还设置为：基于所述第三广播消息将所述物联网设备102的数字身份和物联网地址存储到区块链的区块中。

[0076] 在一种实施方式中，所述第一物联网网关1011还设置为：接收再次接入的物联网设备102发送的包含第二密文的第二请求消息，其中所述第二密文为使用区块链随机秘钥生成的加密后的再次接入的物联网设备102的数字身份、物联网地址以及需要交互的信息(如指令、数据等)；对所述第二密文进行解密以得到包含再次接入的物联网设备102的数字身份、物联网地址以及需要交互的信息的第二明文；以及，将包括所述第二明文的第四广播消息发送给所述区块链网络中的其他各第二物联网网关1012。

[0077] 所述其他各第二物联网网关1012还设置为：将再次接入的物联网设备102的数字身份和物联网地址与区块链中已存储的同一物联网设备102的数字身份和物联网地址进行

比对，并对比对结果进行签名。

[0078] 相应地，所述第一物联网网关1011还设置为：若所述其他各第二物联网网关1012的比对结果为比对成功，则允许接入所述物联网设备；若所述其他各第二物联网网关1012的比对结果为比对失败，则拒绝接入所述物联网设备。

[0079] 本公开实施例提供的物联网设备安全防护系统，通过各个物联网网关利用区块链相互连接以构成区块链网络，对底层各个感知节点的物联网设备进行安全防护和远程控制，共同监控、标识和处理物联网设备的网络活动，并使用加密技术和安全算法来保护物联网设备的数字身份，避免被劫持的物联网设备被恶意软件控制而对特定的网络服务进行分布式拒绝服务攻击，从而构建出物联网环境下更加安全便捷的设备安全防护系统。

[0080] 图4为本公开实施例提供的另一种物联网设备安全防护系统的示意图。如图4所示，所述系统100包括区块链网络101、物联网设备102和物联网平台103。其中，所述区块链网络101包括第一物联网网关1011、若干第二物联网网关1012和若干数据服务器1013，各个物联网网关利用区块链相互连接，每个物联网网关均与一个数据服务器1013连接。

[0081] 本公开实施例中，每个物联网网关和与之连接的数据服务器1013构成一个工作单元，而物联网系统至少包含一个由物联网网关和数据服务器组建的工作单元。工作单元中的物联网网关可通过物联网无线通信网络或互联网无线通信网络与物联网平台103和物联网设备102连接。

[0082] 本公开实施例中，数据服务器1013包括：注册模块、认证模块、加密模块、数据处理模块、数据存储模块及数据检索模块。其中，注册模块设置为对待接入的物联网设备进行注册服务；认证模块设置为对物联网设备的接入请求进行合法性认证；加密模块设置为对区块链网络的各个节点或设备交互的指令和数据进行加密和解密处理；数据处理模块、数据存储模块和数据检索模块设置为对物联网网关或物联网设备提供数据处理、存储和检索的服务。

[0083] 物联网设备102首次接入物联网系统时，设置为发送包含第一密文的第一请求信息至区块链网络101，其中所述第一密文为使用区块链公钥生成的加密后的所述物联网设备102的数字身份和物联网地址；

[0084] 所述区块链网络101设置为发送包含所述第一请求信息的第一广播消息至各个物联网网关，并根据区块链共识机制选出响应所述第一请求信息的第一物联网网关1011；

[0085] 所述第一物联网网关1011设置为对所述第一密文进行解密以得到包含所述物联网设备102的数字身份和物联网地址的第一明文；

[0086] 所述第一物联网网关1011还设置为判断所述物联网设备102的数字身份和物联网地址是否已被注册占用，若未被注册占用，则将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关1012；

[0087] 所述其他各第二物联网网关1012设置为对所述第一明文进行数字签名，并返回给所述第一物联网网关1011；

[0088] 所述第一物联网网关1011还设置为将第三广播消息发送给所述其他各第二物联网网关1012，所述第三广播消息包括所述物联网设备102的数字身份、物联网地址和数字签名；

[0089] 所述其他各第二物联网网关1012还设置为基于所述第三广播消息将所述物联网

设备102的数字身份和物联网地址存储到区块链的区块中；

[0090] 所述物联网设备102再次接入物联网系统时，还设置为发送包含第二密文的第二请求消息至所述第一物联网网关1011，其中所述第二密文为使用区块链随机秘钥生成的加密后的再次接入的物联网设备102的数字身份、物联网地址以及需要交互的信息(如指令、数据等)；

[0091] 所述第一物联网网关1011还设置为对所述第二密文进行解密以得到包含再次接入的物联网设备102的数字身份、物联网地址以及需要交互的信息的第二明文；

[0092] 所述第一物联网网关1011还设置为将包括所述第二明文的第四广播消息发送给所述区块链网络中的其他各第二物联网网关；

[0093] 所述其他各第二物联网网关1012还设置为将再次接入的物联网设备102的数字身份和物联网地址与区块链中已存储的同一物联网设备102的数字身份和物联网地址进行比对，并对比对结果进行签名，以确保比对结果的真实性；

[0094] 所述第一物联网网关1011还设置为若比对成功，则允许接入所述物联网设备102；若比对失败，则拒绝接入所述物联网设备102，并在所述物联网设备102访问目标服务器之前切断网络连接。

[0095] 本公开实施例提供的物联网设备安全防护系统，通过各个物联网网关利用区块链相互连接以构成区块链网络，对底层各个感知节点的物联网设备进行安全防护和远程控制，共同监控、标识和处理物联网设备的网络活动，并使用加密技术和安全算法来保护物联网设备的数字身份，避免被劫持的物联网设备被恶意软件控制而对特定的网络服务进行分布式拒绝服务攻击，从而构建出物联网环境下更加安全便捷的设备安全防护系统。

[0096] 综上所述，本公开实施例提供的物联网设备安全防护方法和系统，在现有物联网技术、区块链技术、物联网无线通信网络和互联网无线通信网络的基础上，升级物联网网关，并将物联网网关用区块链相互连接以构成区块链网络，对底层各个感知节点的物联网设备进行安全防护和远程控制，共同监控、标识和处理物联网设备的网络活动，并使用加密技术和安全算法来保护物联网设备的数字身份，构建了物联网环境下更加安全便捷的物联网设备安全防护体系。

[0097] 本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读

指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

[0098] 最后应说明的是：以上各实施例仅用以说明本公开的技术方案，而非对其限制；尽管参照前述各实施例对本公开进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本公开各实施例技术方案的范围。

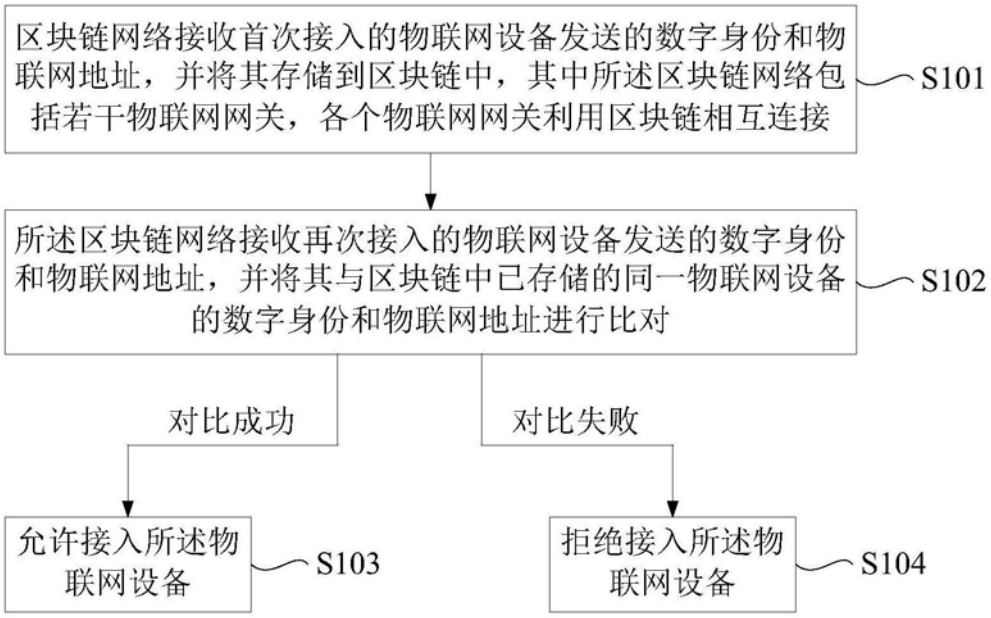

区块链网络接收首次接入的物联网设备发送的数字身份和物联网地址，并将其存储到区块链中，其中所述区块链网络包括若干物联网网关，各个物联网网关利用区块链相互连接
S101
所述区块链网络接收再次接入的物联网设备发送的数字身份和物联网地址，并将其与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对
S102
对比成功
对比失败
允许接入所述物联网设备
S103
拒绝接入所述物联网设备
S104

图1

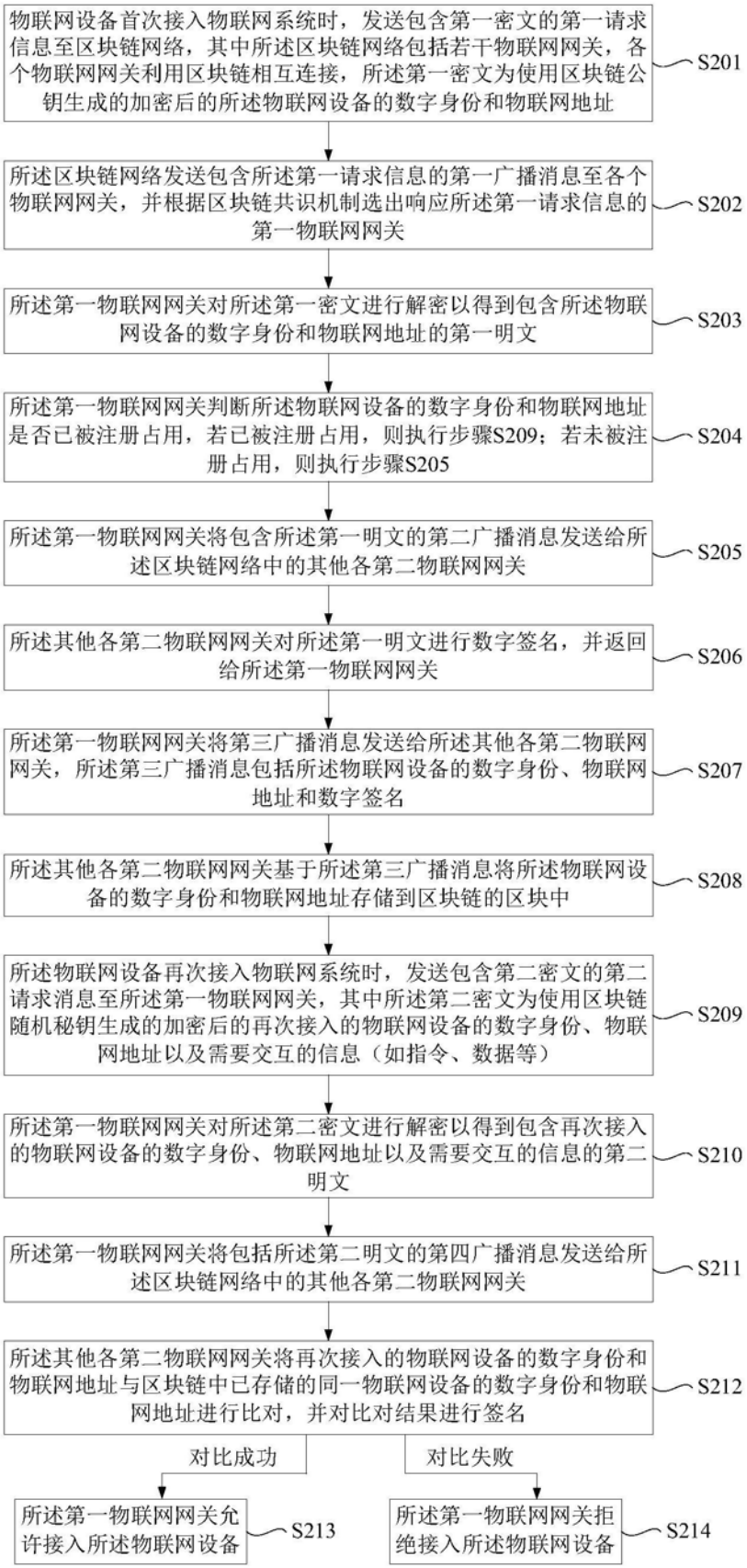

物联网设备首次接入物联网系统时，发送包含第一密文的第一请求信息至区块链网络，其中所述区块链网络包括若干物联网网关，各个物联网网关利用区块链相互连接，所述第一密文为使用区块链公钥生成的加密后的所述物联网设备的数字身份和物联网地址
S201
所述区块链网络发送包含所述第一请求信息的第一广播消息至各个物联网网关，并根据区块链共识机制选出响应所述第一请求信息的第一物联网网关
S202
所述第一物联网网关对所述第一密文进行解密以得到包含所述物联网设备的数字身份和物联网地址的第一明文
S203
所述第一物联网网关判断所述物联网设备的数字身份和物联网地址是否已被注册占用，若已被注册占用，则执行步骤S209；若未被注册占用，则执行步骤S205
S204
所述第一物联网网关将包含所述第一明文的第二广播消息发送给所述区块链网络中的其他各第二物联网网关
S205
所述其他各第二物联网网关对所述第一明文进行数字签名，并返回给所述第一物联网网关
S206
所述第一物联网网关将第三广播消息发送给所述其他各第二物联网网关，所述第三广播消息包括所述物联网设备的数字身份、物联网地址和数字签名
S207
所述其他各第二物联网网关基于所述第三广播消息将所述物联网设备的数字身份和物联网地址存储到区块链的区块中
S208
所述物联网设备再次接入物联网系统时，发送包含第二密文的第二请求消息至所述第一物联网网关，其中所述第二密文为使用区块链随机秘钥生成的加密后的再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息（如指令、数据等）
S209
所述第一物联网网关对所述第二密文进行解密以得到包含再次接入的物联网设备的数字身份、物联网地址以及需要交互的信息的第二明文
S210
所述第一物联网网关将包括所述第二明文的第四广播消息发送给所述区块链网络中的其他各第二物联网网关
S211
所述其他各第二物联网网关将再次接入的物联网设备的数字身份和物联网地址与区块链中已存储的同一物联网设备的数字身份和物联网地址进行比对，并对比对结果进行签名
S212
对比成功
对比失败
所述第一物联网网关允许接入所述物联网设备
S213
所述第一物联网网关拒绝接入所述物联网设备
S214

图2

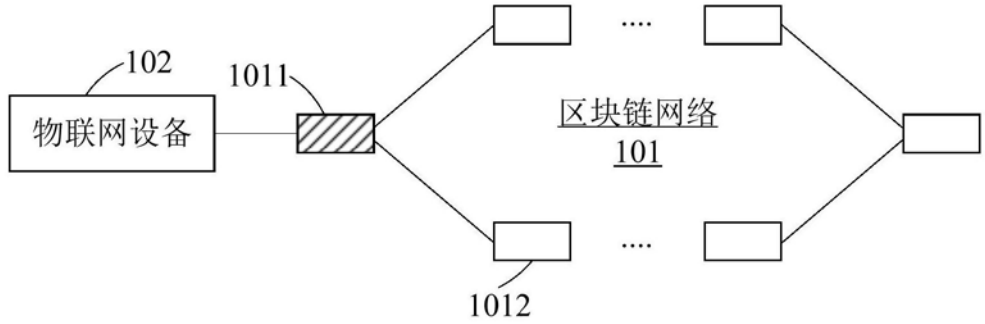

102
物联网设备
1011
区块链网络
101
1012

图3

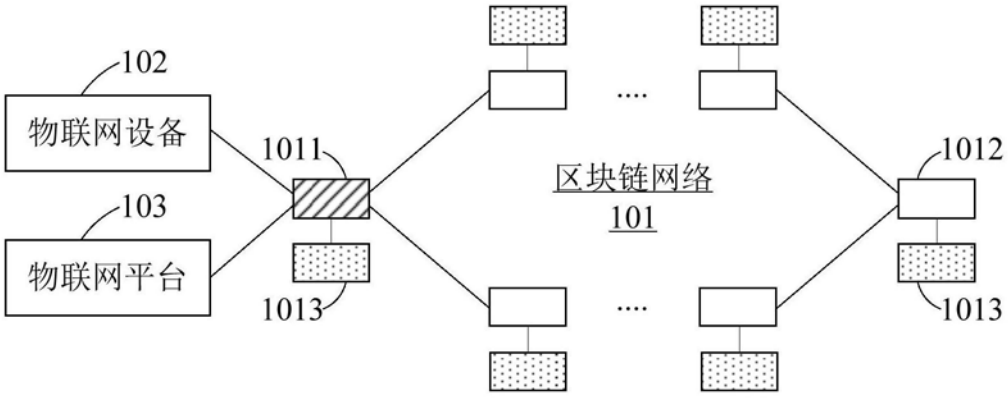

102
物联网设备
103
物联网平台
1011
1013
区块链网络
101
1012
1013

图4