(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 108900306 A
(43)申请公布日 2018.11.27

(21)申请号 201810709399.9

(22)申请日 2018.07.02

(71)申请人 四川斐讯信息技术有限公司
地址 610100 四川省成都市龙泉驿区龙泉街道公园路125号

(72)发明人 何山

(74)专利代理机构 成都金德联合知识产权代理事务所(特殊普通合伙) 51271
代理人 张婵婵 王晓普

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
H04W 12/06(2009.01)

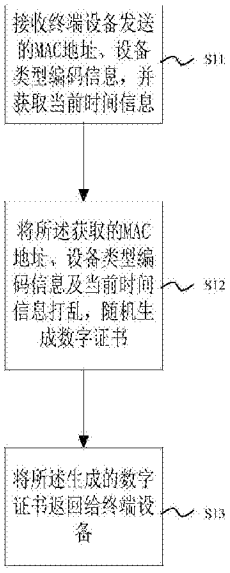
权利要求书1页 说明书6页 附图3页

(54)发明名称

一种无线路由器数字证书的产生方法及系统

(57)摘要

本发明公开了一种无线路由器数字证书的产生方法及系统，该方法包括：接收终端设备发送的MAC地址、设备类型编码信息，并获取当前时间信息；将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；将所述生成的数字证书返回给终端设备。该方法通过将终端设备的MAC地址、设备类型编码信息及当前时间信息打乱生成字符串，有效地为每一个终端设备产生一个数字证书，防止数字证书信息的泄露，提升了网络的安全性。



CN 108900306 A

1.一种无线路由器数字证书的产生方法，其特征在于，包括步骤：

S 1.接收终端设备发送的MAC地址、设备类型编码信息，并获取当前时间信息；

S2.将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

S3.将所述生成的数字证书返回给终端设备。

2.如权利要求1所述的一种无线路由器数字证书的产生方法，其特征在于，在步骤S2之前，还包括步骤：

将所述获取的MAC地址进行存储，建立MAC地址链表。

3.如权利要求1所述的一种无线路由器数字证书的产生方法，其特征在于，在步骤S2之后，还包括步骤：

将所述生成的数字证书存储到MAC地址链表里所对应的MAC地址指向的地址中。

4.如权利要求1所述的一种无线路由器数字证书的产生方法，其特征在于，步骤S3具体包括步骤：

将所述生成的数字证书通过私钥进行加密，再返回给终端设备。

5.如权利要求1所述的一种无线路由器数字证书的产生方法，其特征在于，在步骤S3之后，还包括步骤：

向终端设备发送数字证书验证请求，并对终端设备返回的数字证书信息进行验证，当数字证书信息验证通过后，对所述终端设备开放网络权限。

6.一种无线路由器数字证书的产生系统，其特征在于，包括：

接收模块，用于接收终端设备发送的MAC地址、设备类型编码信息；

获取模块，用于获取当前时间信息；

生成模块，用于将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

返回模块，用于将所述生成的数字证书返回给终端设备。

7.如权利要求6所述的一种无线路由器数字证书的产生系统，其特征在于，还包括：

存储模块，用于将所述获取的MAC地址进行存储；

建立模块，用于根据所述获取的MAC地址建立MAC地址链表。

8.如权利要求6所述的一种无线路由器数字证书的产生系统，其特征在于，还包括：

存储模块，用于将所述生成的数字证书存储到MAC地址链表所对应的MAC地址指向的地址中。

9.如权利要求6所述的一种无线路由器数字证书的产生系统，其特征在于，还包括：

加密模块，用于将所述生成的数字证书通过私钥进行加密。

10.如权利要求6所述的一种无线路由器数字证书的产生系统，其特征在于，还包括：

发送模块，用于向终端设备发送数字证书验证请求；

验证模块，用于对终端设备返回的数字证书信息进行验证。

一种无线路由器数字证书的产生方法及系统

技术领域

[0001] 本发明属于网络安全技术领域，更具体地，涉及一种无线路由器数字证书的产生方法及系统。

背景技术

[0002] 通过数字证书验证入网，可以很好地防止网络被窃取和占用。但当一个无线路由器接入多个终端设备时，如果所有终端设备都使用同一套数字证书，就容易导致数字证书的泄露，一旦被其他非认同终端设备窃用后，其他非认同终端设备也能依靠这套数字证书入网，网络安全性降低。

[0003] 公开号CN108040358A的专利公开了一种无线网络连接方法、终端设备及存储介质，该方法包括：在接收到预定指令时，进行全信道扫描，获取扫描到的无线网络的参数信息，所述无线网络的参数信息包括以下至少一项：无线网络的信号强度值、无线网络所在信道的信道利用率以及无线网络所在信道接入的无线设备个数；根据扫描到的无线网络参数信息，获得扫描到的无线网络的综合性能；将所述综合性能最高的无线网络作为目标无线网络，并向所述目标无线网络发起连接请求；在密码验证正确之后，即实现无线网络连接。该方法通过向目标无线网络发起网络连接请求，在输入正确的无线网络密码后即可连接入网，尚未使用数字证书进行入网验证，更不能做到对每一个终端设备匹配专属的数字证书，安全等级较低，密码容易泄露和被盗用。

[0004] 与现有技术相比，本发明通过将终端设备的MAC地址、设备类新编码信息及当前时间信息打乱生成字符串，有效地为每一个终端设备产生一个数字证书，通过专属的数字证书进行入网的验证，同时防止了数字证书信息的泄露，提升了网络的安全性。

发明内容

[0005] 针对现有技术的以上缺陷及改进需求，本发明提供了一种无线路由器数字证书的产生方法及系统，其目的在于提供一种有效地为每一个终端设备产生一个数字证书，防止数字证书信息的泄露，提升网络的安全性的无线路由器数字证书的产生方法及系统，由此解决现有技术存在的数字证书容易泄露的技术问题。

[0006] 为实现上述目的，本发明提供了一种无线路由器数字证书的产生方法，包括步骤：

[0007] S1.接收终端设备发送的MAC地址、设备类型编码信息，并获取当前时间信息；

[0008] S2.将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

[0009] S3.将所述生成的数字证书返回给终端设备。

[0010] 进一步的，在步骤S2之前，还包括步骤：

[0011] 将所述获取的MAC地址进行存储，建立MAC地址链表。

[0012] 进一步的，在步骤S2之后，还包括步骤：

[0013] 将所述生成的数字证书存储到MAC地址链表里所对应的MAC地址指向的地址中。

[0014] 进一步的，步骤S3具体包括步骤：

[0015] 将所述生成的数字证书通过私钥进行加密，再返回给终端设备。

[0016] 进一步的，在步骤S3之后，还包括步骤：

[0017] 向终端设备发送数字证书验证请求，并对终端设备返回的数字证书信息进行验证，当数字证书信息验证通过后，对所述终端设备开放网络权限。

[0018] 相应的，还提供一种无线路由器数字证书的产生系统，包括：

[0019] 接收模块，用于接收终端设备发送的MAC地址、设备类型编码信息；

[0020] 获取模块，用于获取当前时间信息；

[0021] 生成模块，用于将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

[0022] 返回模块，用于将所述生成的数字证书返回给终端设备。

[0023] 进一步的，还包括：

[0024] 存储模块，用于将所述获取的MAC地址进行存储；

[0025] 建立模块，用于根据所述获取的MAC地址建立MAC地址链表。

[0026] 进一步的，还包括：

[0027] 存储模块，用于将所述生成的数字证书存储到MAC地址链表所对应的MAC地址指向的地址中。

[0028] 进一步的，还包括：

[0029] 加密模块，用于将所述生成的数字证书通过私钥进行加密。

[0030] 进一步的，还包括：

[0031] 发送模块，用于向终端设备发送数字证书验证请求；

[0032] 验证模块，用于对终端设备返回的数字证书信息进行验证。

[0033] 本发明与现有技术相比，有如下优点：

[0034] 通过将终端设备的MAC地址、设备类新编码信息及当前时间信息打乱生成字符串，有效地为每一个终端设备产生一个数字证书，防止数字证书信息的泄露，提升了网络的安全性。

附图说明

[0035] 图1是实施例一提供的一种无线路由器数字证书的产生方法流程图；

[0036] 图2是实施例一提供的一种无线路由器数字证书的产生系统结构图；

[0037] 图3是实施例二提供的一种无线路由器数字证书的产生方法流程图；

[0038] 图4是实施例二提供的一种无线路由器数字证书的产生系统结构图。

具体实施方式

[0039] 以下是本发明的具体实施例并结合附图，对本发明的技术方案作进一步的描述，但本发明并不限于这些实施例。

[0040] 实施例一

[0041] 本实施例提供了一种无线路由器数字证书的产生方法，如图1所示，包括步骤：

[0042] S11.接收终端设备发送的MAC地址、设备类型编码信息，并获取当前时间信息；

[0043] S12.将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

[0044] S13.将所述生成的数字证书返回给终端设备。

[0045] 当终端设备与无线路由器第一次连接，经过无线路由器管理员的确认，终端设备向无线路由器发送终端设备的MAC地址、设备类型编码信息，无线路由器在接收终端设备发送的MAC地址、设备类型编码信息的同时，获取当前时间信息，然后利用随机函数，将获取的终端设备MAC地址、设备类型编码信息及当前时间信息字符打乱，生成一段随机字符串，该字符串则为数字证书的识别码。由于生成的数字证书是由终端设备MAC地址、设备类型编码信息及当前时间信息打乱字符顺序生成的，每个终端设备有不同的设备类型码、MAC地址，终端设备向无线路由器发送设备相关信息的时间也不同，所以对应每个终端设备生成的数字证书识别码就各不相同，避免了出现数字证书相同的情况。

[0046] 无线路由器在生成了终端设备专属的数字证书后，需要向终端设备安装这个数字证书，则将生成的数字证书返回给终端设备。

[0047] 进一步的，在步骤S12之前，还包括步骤：

[0048] 将所述获取的MAC地址进行存储，建立MAC地址链表。

[0049] 无线路由器在接收到终端设备发送的MAC地址之后，生成数字证书之前，需根据终端设备的MAC地址创建存放终端设备MAC地址的链表，以便用于存放生成的数字证书。

[0050] 进一步的，在步骤S12之后，还包括步骤：

[0051] 将所述生成的数字证书存储到MAC地址链表里所对应的MAC地址指向的地址中。

[0052] 当无线路由器将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成终端设备的专属数字证书后，则将生成的数字证书存放在已创建好的MAC地址链表里对应的终端设备的MAC地址中，这样链表的每个节点即终端设备MAC地址则指向对应的数字证书存放路径。

[0053] 进一步的，步骤S13具体包括步骤：

[0054] 将所述生成的数字证书通过私钥进行加密，再返回给终端设备。

[0055] 无线路由器与终端设备之间的通信是经过公私密钥进行加密的，这是为了保障通信安全。当发送一份保密文件时，发送方使用私钥对数据加密，而接收方使用公钥进行解密，这样，信息就可以安全无误地到达目的地了，即使被第三方截获，由于缺乏相应的公钥，无法进行解密。

[0056] 因此，无线路由器在生成了数字证书后，将生成的数字证书用私钥进行加密，再返回给终端设备，终端设备通过相应的公钥则可对无线路由器发送的信息进行解密，最终获取数字证书信息。

[0057] 相应的，还提供一种无线路由器数字证书的产生系统，如图2所示，包括：

[0058] 接收模块11，用于接收终端设备发送的MAC地址、设备类型编码信息；

[0059] 获取模块12，用于获取当前时间信息；

[0060] 生成模块13，用于将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

[0061] 返回模块14，用于将所述生成的数字证书返回给终端设备。

[0062] 接收模块11接收终端设备发送的MAC地址、设备类型编码信息并发送给生成模块

13，接收模块11接收接收终端设备发送的MAC地址、设备类型编码信息的同时，获取模块12获取当前时间信息并发送给生成模块13，生成模块13根据所述获取的MAC地址、设备类型编码信息及当前时间信息，通过随机函数打乱，随机生成数字证书，并发送给返回模块14，由返回模块14将生成的数字证书返回给终端设备。

[0063] 进一步的，还包括：

[0064] 存储模块15，用于将所述获取的MAC地址进行存储；

[0065] 建立模块16，用于根据所述获取的MAC地址建立MAC地址链表。

[0066] 接收模块11在接收到终端设备发送的MAC地址、设备类型编码信息后，将终端设备的MAC地址发送给存储模块15，由存储模块15将获取的MAC地址进行存储，再由建立模块16根据获取的MAC地址建立MAC地址链表。

[0067] 进一步的，还包括：

[0068] 存储模块15，用于将所述生成的数字证书存储到MAC地址链表所对应的MAC地址指向的地址中。

[0069] 当生成模块13根据所述获取的MAC地址、设备类型编码信息及当前时间信息，通过随机函数打乱，随机生成了数字证书后，将生成的数字证书发送给存储模块15，由存储模块15将所述生成的数字证书存储到MAC地址链表所对应的MAC地址中。

[0070] 进一步的，还包括：

[0071] 加密模块17，用于将所述生成的数字证书通过私钥进行加密。

[0072] 生成模块13根据所述获取的MAC地址、设备类型编码信息及当前时间信息，通过随机函数打乱，随机生成了数字证书之后，由加密模块17对生成的数字证书进行加密，再由返回模块14将经过加密处理的数字证书返回给终端设备。

[0073] 本实施例通过将终端设备的MAC地址、设备类新编码信息及当前时间信息打乱生成字符串，有效地为每一个终端设备产生一个数字证书，防止数字证书信息的泄露，提升了网络的安全性。

[0074] 实施例二

[0075] 本实施例提供了一种无线路由器数字证书的产生方法，如图3所示，包括步骤：

[0076] S21.接收终端设备发送的MAC地址、设备类型编码信息，并获取当前时间信息；

[0077] S22.将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

[0078] S23.将所述生成的数字证书返回给终端设备。

[0079] 进一步的，在步骤S22之前，还包括步骤：

[0080] 将所述获取的MAC地址进行存储，建立MAC地址链表。

[0081] 进一步的，在步骤S22之后，还包括步骤：

[0082] 将所述生成的数字证书存储到MAC地址链表里所对应的MAC地址指向的地址中。

[0083] 进一步的，步骤S23具体包括步骤：

[0084] 将所述生成的数字证书通过私钥进行加密，再返回给终端设备。

[0085] 进一步的，在步骤S23之后，还包括步骤：

[0086] 向终端设备发送数字证书验证请求，并对终端设备返回的数字证书信息进行验证，当数字证书信息验证通过后，对所述终端设备开放网络权限。

[0087] 与实施例一不同的是，在步骤S23之后，还包括步骤：

[0088] 向终端设备发送数字证书验证请求，并对终端设备返回的数字证书信息进行验证，当数字证书信息验证通过后，对所述终端设备开放网络权限。

[0089] 在日后的连接中，当终端设备通过SSID及相应的密码与无线路由器建立连接之后，无线路由器会向终端设备发送数字证书验证请求，终端设备根据无线路由器发送的数字证书验证请求回复相应的验证信息，无线路由器根据终端设备回复的验证信息，由系统根据MAC地址链表中的MAC地址找到相应的数字证书对验证信息进行验证，验证通过后，对通过验证的终端设备开放网络权限。

[0090] 例如，数字证书是由48位字符组成，无线路由器可以向终端设备发送验证请求，要求随机验证数字证书的某些位的字符，如要求终端设备返回数字证书的第10-16位字符码，当返回字符经无线路由器验证与存储的数字证书对应位的字符一致时，标明验证正确，无线路由器即向终端设备开放网络权限。

[0091] 本实施例相较于实施例一，其优点在于：

[0092] 通过数字证书信息对请求入网的终端设备进行验证，只有通过验证的终端设备才享有开放的网络权限，这进一步的提高网络连接的安全性。

[0093] 相应的，还提供一种无线路由器数字证书的产生系统，如图4所示，包括：

[0094] 接收模块21，用于接收终端设备发送的MAC地址、设备类型编码信息；

[0095] 获取模块22，用于获取当前时间信息；

[0096] 生成模块23，用于将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书；

[0097] 返回模块24，用于将所述生成的数字证书返回给终端设备。

[0098] 进一步的，还包括：

[0099] 存储模块25，用于将所述获取的MAC地址进行存储；

[0100] 建立模块26，用于根据所述获取的MAC地址建立MAC地址链表。

[0101] 进一步的，还包括：

[0102] 存储模块25，用于将所述生成的数字证书存储到MAC地址链表所对应的MAC地址指向的地址中。

[0103] 进一步的，还包括：

[0104] 加密模块27，用于将所述生成的数字证书通过私钥进行加密。

[0105] 进一步的，还包括：

[0106] 发送模块28，用于向终端设备发送数字证书验证请求；

[0107] 验证模块29，用于对终端设备返回的数字证书信息进行验证。

[0108] 与实施例一不同的是，还包括发送模块28、验证模块29。

[0109] 发送模块28向终端设备发送数字证书验证请求，终端设备回复验证信息后，由验证模块29对终端设备返回的数字证书信息进行验证，验证通过后，则向该终端设备开放网络权限。

[0110] 通过数字证书信息对请求入网的终端设备进行验证，只有通过验证的终端设备才享有开放的网络权限，这进一步的提高网络连接的安全性。

[0111] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明。本发明所属技术领

域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代，但并不会偏离本发明的精神或者超越所附权利要求书所定义的范围。

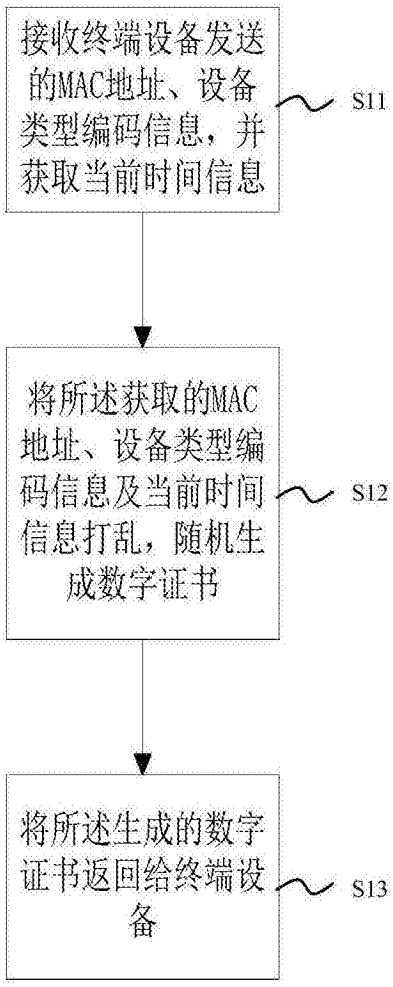

接收终端设备发送的MAC地址、设备类型编码信息，并获取当前时间信息
S11
将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书
S12
将所述生成的数字证书返回给终端设备
S13

图1

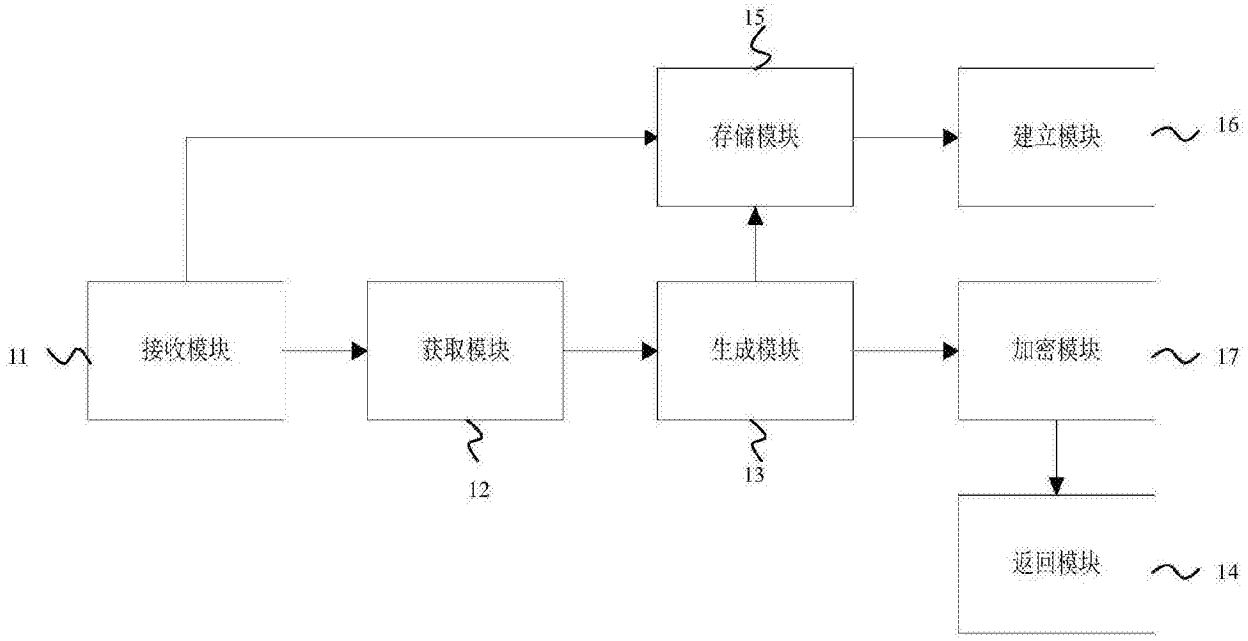

15
存储模块
建立模块
16
11
接收模块
获取模块
生成模块
加密模块
17
12
13
返回模块
14

图2

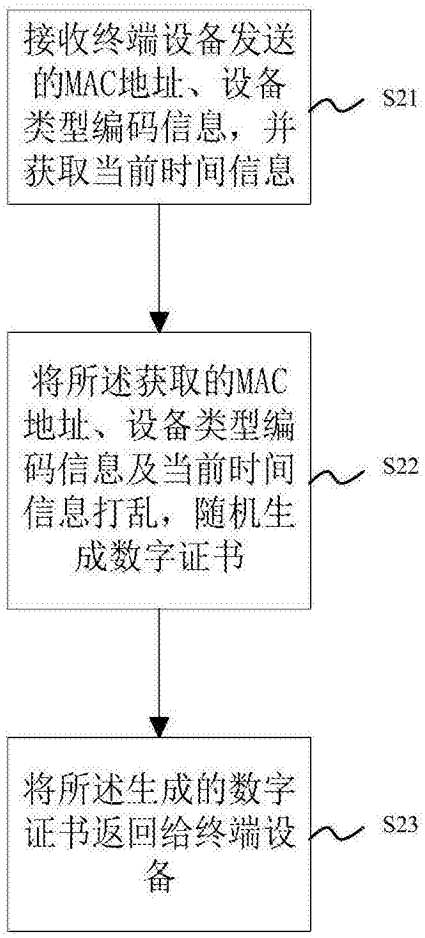

接收终端设备发送的MAC地址、设备类型编码信息，并获取当前时间信息
S21
将所述获取的MAC地址、设备类型编码信息及当前时间信息打乱，随机生成数字证书
S22
将所述生成的数字证书返回给终端设备
S23

图3

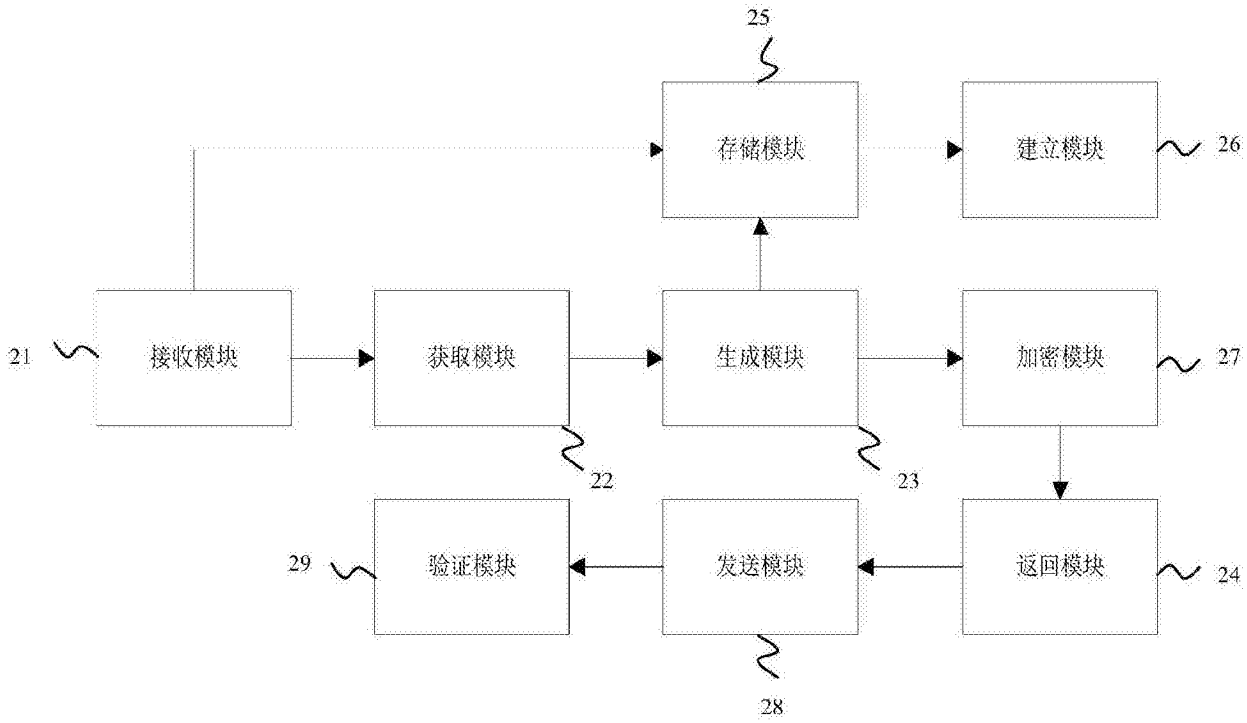

25
存储模块
建立模块
26
21
接收模块
获取模块
生成模块
加密模块
27
22
23
29
验证模块
发送模块
返回模块
24
28

图4