(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 101242426 B
(45)授权公告日 2010.12.08

(21)申请号 200710073234.9

(22)申请日 2007.02.06

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 潘云波

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04L 12/56(2006.01)

(56)对比文件
US 2006067340 A1,2006.03.30,
US 2006294381 A1,2006.12.28,
EP 1743449 A1,2007.01.17,

审查员 李倩

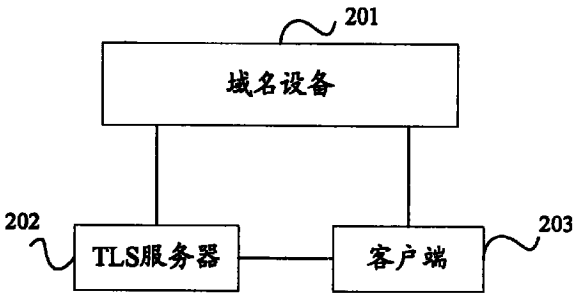
权利要求书 2 页 说明书 5 页 附图 2 页

(54)发明名称

建立传输层安全连接的方法、系统及装置

(57)摘要

本发明涉及建立传输层安全连接的方法、系统及装置，客户端向域名设备查询获取传输层安全 TLS 服务器的安全信息，根据所述安全信息与所述 TLS 服务器进行连接。由于采用诸如 DNS 服务器或者 DNS 的安全扩展服务器的域名设备存储 TLS 服务器的安全信息，只要有 Internet 的地方就有，这样 TLS 协议的应用就可以摆脱证书机构的束缚，增加了 TLS 的应用场景。



CN 101242426 B

1. 一种建立传输层安全连接的方法，其特征在于，所述方法包括：

客户端向域名设备查询获取传输层安全 TLS 服务器的安全信息，根据所述安全信息与所述 TLS 服务器进行连接，所述域名设备为域名系统 DNS 服务器或者 DNS 的安全扩展服务器，所述安全信息包括公钥的算法、公钥各个部分的长度及内容。

2. 如权利要求 1 所述的方法，其特征在于，所述客户端向域名设备查询获取传输层安全 TLS 服务器的安全信息，具体为：

客户端向域名设备查询获取传输层安全 TLS 服务器存储到所述域名设备中的安全信息。

3. 如权利要求 1 所述的方法，其特征在于，当所述域名设备为域名系统 DNS 的安全扩展服务器时，还包括：

所述 TLS 服务器将所述公钥的算法、公钥各个部分的长度及内容，以资源记录的形式存储到所述域名设备中；

所述域名设备利用所述 TLS 服务器所在区域的私钥对所述资源记录签名。

4. 如权利要求 3 所述的方法，其特征在于，所述资源记录中还包括标识业务的字段。

5. 如权利要求 3 所述的方法，其特征在于，在所述资源记录的命名格式中，服务器的 DNS 域名前包括业务名的字段。

6. 如权利要求 1 至 5 任一所述的方法，其特征在于，所述安全信息还包括所述 TLS 服务器支持的 TLS 协议的最高版本号；

在所述客户端向域名设备查询获取安全信息后，还进一步包括：

所述客户端将获取的所述最高版本号与自身所支持的最高版本号中间的较低者发送给所述 TLS 服务器，根据所述 TLS 服务器返回的包含版本号的消息，如果返回的所述版本号与发送给所述 TLS 服务器的版本号不同，则中断连接或发出警告消息。

7. 一种建立传输层安全连接的系统，包括客户端和传输层安全 TLS 服务器，其特征在于，还包括域名设备，其中：

所述 TLS 服务器，用于将其安全信息存储到域名设备中，所述安全信息包括公钥的算法、公钥各个部分的长度及内容；

所述客户端，用于向域名设备查询获取所述安全信息，根据所述安全信息与所述 TLS 服务器建立连接；

所述域名设备，用于保存所述 TLS 服务器的所述安全信息，所述域名设备为域名系统 DNS 服务器或者 DNS 的安全扩展服务器。

8. 一种域名装置，其特征在于，包括：

记录模块，用于以资源记录的形式存储传输层安全 TLS 服务器的安全信息，所述安全信息包括公钥的算法、公钥各个部分的长度及内容；

输出模块，用于根据客户端的请求，向所述客户端输出所述记录模块中的相应资源记录；

所述域名装置包含在域名系统 DNS 服务器或 DNS 的安全扩展服务器中。

9. 如权利要求 8 所述的装置，其特征在于，还包括签名模块，用于根据所述 TLS 服务器所在区域的私钥对所述记录模块存储的资源记录签名。

10. 一种域名系统服务器，其特征在于，包括如权利要求 8 所述的域名装置。

11. 一种域名系统的安全扩展服务器，其特征在于，包括如权利要求 8 所述的域名装置。

建立传输层安全连接的方法、系统及装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及建立传输层安全连接的方法、系统及装置。

背景技术

[0002] DNS（域名系统，Domain Name System）实际上是一个大型的分布式数据库系统，它所执行的基本功能是网络资源（从最早的简单网络上的每个主机名到后来的域名、邮件地址等）与 IP 地址之间的翻译。由于 DNS 是一个被广泛应用的网络基础设施，所以目前的 DNS 被赋予了许多新的功能，例如，用它来进行分发 IPsec（Internet 协议安全）的公钥信息或 SSH（安全外壳，Secure Shell）的公钥指纹等。

[0003] DNSSEC 是 DNS 的安全扩展（DNS Security Extension），它通过区签名的方式来对资源记录进行数据源认证及完整性保护，所谓区签名，就是利用每个区所对应的私钥对区内的每一个资源记录集作签名，形成与资源记录集对应的签名记录。

[0004] 通过获取一个区所对应的公钥，域名解析器可以通过签名验证来判断获得的资源记录的真实性和完整性。DNSSEC 通过建立信任链来保证域名解析器所获得的公钥的可靠性，作为信任链的开端，每个域名解析器都必须预先配置一个或多个 Trust Anchor（信任锚点），Trust Anchor 为某个区的公钥或公钥的消息摘要。

[0005] TLS（传输层安全，Transport Layer Security）协议是一个能为 Internet 上的通讯双方提供安全可靠的通讯服务的协议，它允许客户端 / 服务器应用之间进行防窃听、防消息篡改及防消息伪造的安全通讯。该协议包含两个层次：上层的 握手协议和下层的记录层协议，这样做的原因是为了保证应用协议的独立性，使得低级协议对于高级协议保持透明。

[0006] 握手协议的主要功能有：

[0007] 1. 负责双方的身份验证，主要有相互认证、服务器认证、无认证三种可选方式；

[0008] 2. 协商各种算法，比如 pre-master-secret（预共享秘密）的协商算法、数据的加密算法及压缩算法、数据的完整性保护算法，以及连接的版本号等信息；

[0009] 3. 协商 pre-master-secret，并据此生成各种数据保护算法所需的密钥。

[0010] 记录层协议位于某一可靠的传输协议之上，例如 TCP 协议（传输控制协议，Transmission Control Protocol），它利用握手协议所协商好的各种算法和密钥，对数据进行分段、压缩、附上 MAC（Message Authentication Code，消息认证代码）、加密，然后将处理过的数据发送出去，接收端则进行相反的处理。

[0011] 为了验证通信双方的身份，同时保证 pre-master-secret 协商的安全性及机密性，目前应用最广泛的方法是利用证书来分发服务器公钥并进行身份验证。

[0012] 在这种方案中，需要有证书机构的支持，而这样会直接导致通信代价的增加，并且，目前还没有任何证书机构能得到所有潜在用户的信赖；在目前所存在着的诸多证书机构中，不同的证书机构可能使用不同的结构、不同的安全策略和密钥算法体系，这样会导致使用不同证书的双方无法进行通信；

[0013] 而且，目前不存在一个有效的办法来保证客户能快速、安全的获得众多证书机构的公钥。

[0014] 实体的命名也没有一个统一的标准，比方说，如果 A 拥有一个由 CA1 签发的名为 Alice 的证书，而 B 则完全可以拥有一个由 CA2 签发的同样名为 Alice 的证书，这样的话，客户端 C 就将无法辨别同为 Alice 的 A、B 的身份。

发明内容

[0015] 有鉴于此，本发明实施例的主要目的在于提供一种不使用证书机构而建立传输层安全连接的方法、系统及装置。

[0016] 为达到上述目的，本发明实施例的技术方案是这样实现的：

[0017] 本发明实施例公开了一种建立传输层安全连接的方法，包括：

[0018] 客户端向域名设备查询获取传输层安全 TLS 服务器的安全信息，根据所述安全信息与所述 TLS 服务器进行连接，所述域名设备为 DNS 服务器或者 DNS 的安全扩展服务器，所述安全信息包括公钥的算法、公钥各个部分的长度及内容。

[0019] 本发明实施例还公开了一种建立传输层安全连接的系统，包括客户端和 TLS 服务器，还包括域名设备，其中：

[0020] TLS 服务器，用于将其安全信息存储到域名设备中，所述域名设备为 DNS 服务器或者 DNS 的安全扩展服务器，所述安全信息包括公钥的算法、公钥各个部分的长度及内容；

[0021] 客户端，用于向域名设备查询获取所述安全信息，根据所述安全信息与所述 TLS 服务器建立连接；

[0022] 域名设备，用于保存所述 TLS 服务器的所述安全信息，所述域名设备为 DNS 服务器或者 DNS 的安全扩展服务器。

[0023] 另外，本发明实施例还公开了一种域名装置，包括：

[0024] 记录模块，用于以资源记录的形式存储 TLS 服务器的安全信息；

[0025] 输出模块，用于根据客户端的请求，向所述客户端输出所述记录模块中的相应资源记录，所述域名装置包含在 DHS 服务器或 DNS 的安全扩展服务器中。

[0026] 另外，本发明实施例还公开了一种包括上述域名装置的 DNS 服务器和 DNS 的安全扩展服务器。

[0027] 在本发明的实施例中，由于采用诸如 DNS 服务器或者 DNS 的安全扩展服务器的域名设备存储 TLS 服务器的安全信息，只要有 Internet 的地方就有 DNS，这样 TLS 协议的应用就可以摆脱证书机构的束缚，增加 TLS 的应用场景；

[0028] 而且 DNS 具备全球统一的规范化命名方式，每个用户都有一个明确且唯一的规范域名，可以避免出现两个不同的实体在两个不同的证书机构中拥有同样 的名字的情况；

[0029] 用户可以及时在线获得通信对端的公钥及用以验证对应签名记录的区公钥，不会出现因为用户没有证书机构的公钥而无法验证证书的情况。

[0030] 附图说明

[0031] 图 1 为本发明一实施例的流程示意图；

[0032] 图 2 为本发明另一实施例的 TLS 握手协议的消息流示意图；

[0033] 图 3 为本发明所提供的系统的一个实施例的组成示意图；

[0034] 图 4 为本发明域名装置实施例一组成示意图；

[0035] 图 5 为本发明域名装置实施例二组成示意图。

[0036] 具体实施方式

[0037] 在本发明的实施例中，将 TLS 服务器的安全信息存放在域名设备的资源记录中，方便客户端获取，从而简化交互过程，并提高了安全性能。

[0038] 为使本发明的目的、技术方案和优点更加清楚明白，以下举实施例，并参照附图，对本发明进一步详细说明。

[0039] 在如图 1 所示的本发明实施例流程图中：

[0040] 步骤 101：客户端向域名系统域名设备查询获取传输层安全 TLS 服务器的安全信息；

[0041] 在本发明的实施例中，域名设备可以是 DNS 或者 DNSSEC 权威服务器，在支持 DNSSEC 的网络环境下，究竟采用 DNS 还是 DNSSEC 来存储安全信息取决于服务器所支持的业务对通信安全及效率的权衡。

[0042] 步骤 102：客户端根据所述安全信息与 TLS 服务器进行连接。

[0043] pre-master-secret 是用来生成加密算法、消息摘要算法的密钥，客户端在获取所述 TLS 服务器的安全信息后，根据其中的相关信息进行 pre-master-secret 协商，协商完成后建立连接。

[0044] 在本发明的实施例中，域名设备可以主动存储 TLS 服务器自身的安全信息， 或者是接收 TLS 服务器发送来的自身的安全信息并加以保存，这些安全信息包括公钥的算法、公钥各个部分的长度及内容，当然，安全信息中还可以包括 TLS 服务器所支持 TLS 协议的最高版本，它们以特定的资源记录格式存入域名设备中。

[0045] 资源记录是 DNS 中的数据格式，所有 DNS 中的数据都可以以资源记录的形式存储，资源记录有很多种，其格式如下：

[0046] 资源记录名 网络类别 资源记录类型 生存时间 数据

[0047] 其中对于资源记录类型代表不同种类资源记录的外在表现，而数据则标识不同种类的资源记录不同的数据格式。

[0048] 而且，在支持 DNSSEC 的情况下，设备需要利用 TLS 服务器所在区域的私钥对此资源记录签名，生成签名记录。如果同一个网址下的 TLS 服务器针对不同的业务采用不同的安全保护方式，那么在资源记录中还可以加入用以辨别业务的字段，或者修改资源记录的命名格式，在资源记录名前加上业务名的前缀。

[0049] 在如图 2 所示的 TLS 握手协议的消息流示意图中：

[0050] 在建立 TLS 连接时，客户端通过查询域名设备获得特定业务所对应的安全信息。如果安全信息中包括 TLS 服务器所支持 TLS 协议的最高版本，客户端可以在获知 TLS 服务器所支持的最高版本号后，将之与自身支持的最高版本号比较，取其中较低的一个作为本次连接所采用协议的版本号，并将该版本号写入 ClientHello 消息中发送至 TLS 服务器，在收到 TLS 服务器返回的 ServerHello 消息后，将 ServerHello 中的版本信息与 ClientHello 中的版本信息比较，如果两个不一致，则可能出现了传输错误或受到了攻击，此时客户端可以选择中断连接或发出警告消息。

[0051] 在客户端接收到 HelloDone 报文后，如果没有 ServerKeyExchange 报文，则客户端

可以根据资源记录中所存储的密钥格式获知密钥协商算法 ：

[0052] 如果资源记录中存储有服务器的 RSA 公钥，客户端在获取该公钥后，选择一个 pre-master-secret，利用 TLS 服务器的公钥，对 pre-master-secret 进行加密， 用 ClientKeyExchange 消息将它发给 TLS 服务器，TLS 服务器利用对应的私钥解密得出 pre-master-secret，这样可以保证双方知道该 pre-master-secret ；

[0053] 如果 TLS 服务器将进行 Diffie-Hellman 交换所需的公钥中的 p、g 及 server 的交换参数存储在资源记录中，客户端根据 p、g 产生自己的交换参数，根据两个交换参数即可生成 pre-master-secret ；

[0054] 产生 pre-master-secret 的过程可以是 ：客户端获知 g、p 后，随机选取 x，则客户端生成自己的交换参数 ：g^x mod p，而 TLS 服务器的交换参数为 g^y mod

[0055] p，由于只有客户端知道 x，只有 TLS 服务器知道 y，因此客户端可以根据 TLS 服务器的交换参数和 x 计算 (g^y mod p)^x ＝ g^xy mod p，TLS 服务器计算 (g^xmod p)^y ＝ g^xy mod p，从而双方得到同样的 pre-master-secret，他人即使知道了双方的交换参数，如果不知道 x、y 的话还是无法计算出 g^xy mod p 的。

[0056] 如果客户端收到 ServerKeyExchange 报文，则协商算法为 DHE，TLS 服务器存储在资源记录中的公钥则是用来验证签名的，而非用来进行直接密钥交换的。DHE 密钥交换算法和 DH 交换的区别在于 ：TLS 服务器和客户端利用 DH 算法来协商密钥时，每次协商所用的 g、p 是固定的，而 DHE 算法中所采用的 g、p 是可变的。在 DHE 算法中，对于每次协商 TLS 服务器都将产生一个新的 p、g 组合，并以此产生自身的交换参数，TLS 服务器通过 ServerKeyExchange 消息来通知客户端此次密钥协商的 p、g 以及 TLS 服务器的交换参数，为了保证 serverkeyexchange 消息中的内容的源认证及数据完整性，TLS 服务器需要对 p、g 及交换参数等内容进行签名，而资源记录中的公钥的作用就是由客户端用来验证签名。

[0057] 如图 3 所示的建立传输层安全连接的系统实施例中，包括客户端 203、域名设备 201 和 TLS 服务器 202，其中 ：

[0058] TLS 服务器 202，用于将其安全信息存储到域名设备 201 中 ；

[0059] 客户端 203，用于向域名设备 201 查询获取所述安全信息，根据所述安全信息与 TLS 服务器 202 进行 pre-master-secret 协商 ；

[0060] 域名设备 201，用于保存所述 TLS 服务器 202 的所述安全信息，在所述 客户端 203 查询时，将所述安全信息发送给所述客户端 203 ；

[0061] 一般而言，域名设备可以是 DNS 服务器或者 DNS 的安全扩展服务器。

[0062] 在如图 4 所示的域名装置实施例中，包括记录模块 2011 和输出模块 2012，其中 ：

[0063] 记录模块 2011，用于以资源记录的形式存储 TLS 服务器的安全信息 ；

[0064] 输出模块 2012，用于根据客户端的请求，向所述客户端输出所述记录模块中的相应资源记录。

[0065] 一般情况下，这样的域名装置可以包含在DNS服务器或DNS的安全扩展服务器中。

[0066] 当然，在域名装置包含在 DNS 的安全扩展服务器中时，还可以如图 5 所示，包括一个签名模块 2013，用于根据所述 TLS 服务器所在区域的私钥对所述记录模块存储的资源记录签名。

[0067] 可以理解的是，本发明实施例还可以计算机可读介质的形式独立存在，而这样的

计算机可读介质可以是包含、存储、传达、传播或者传输计算机程序的介质，所述计算机程序为使用指令以运行本发明实施例所提供的系统装置、系统或者设备的程序，或者是与该指令有关的程序。该计算机可读介质可以是电子、磁、电磁、光学、红外或者半导体的系统、装置、设备、传播介质或者计算机存储器。

[0068] 可以看出，由于采用诸如DNS服务器或DNS的安全扩展服务器的域名设备存储TLS服务器的安全信息，只要有 Internet 的地方就有，这样 TLS 协议的应用就可以摆脱证书机构的束缚，增加 TLS 的应用场景；

[0069] 而且 DNS 具备全球统一的规范化命名方式，每个用户都有一个明确且唯一的规范域名，可以避免出现两个不同的实体在两个不同的证书机构中拥有同样的名字的情况；

[0070] 用户可以及时在线获得通信对端的公钥及用以验证对应签名记录的区公钥，不会出现因为用户没有证书机构的公钥而无法验证证书的情况。

[0071] 以上所述仅是本发明的优选实施方式，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，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

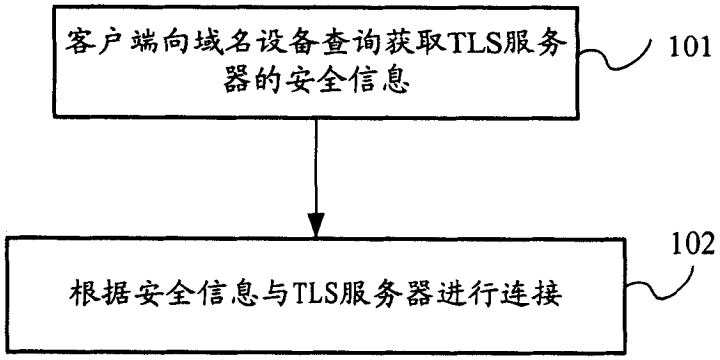

客户端向域名设备查询获取TLS服务器的安全信息
101
根据安全信息与TLS服务器进行连接
102

图 1

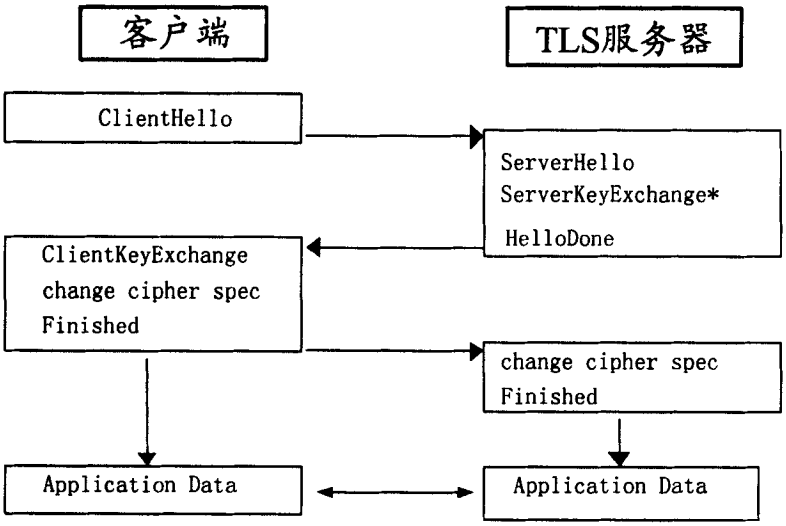

客户端
TLS服务器
ClientHello
ServerHello
ServerKeyExchange*
HelloDone
ClientKeyExchange
change cipher spec
Finished
change cipher spec
Finished
Application Data
Application Data

图 2

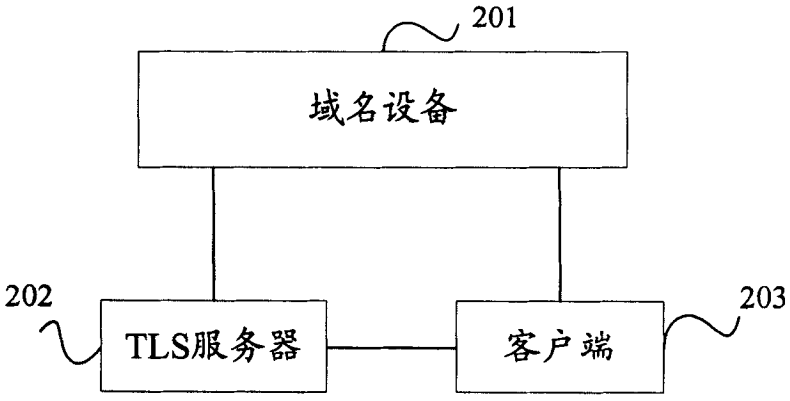

201
域名设备
202
TLS服务器
客户端
203

图 3

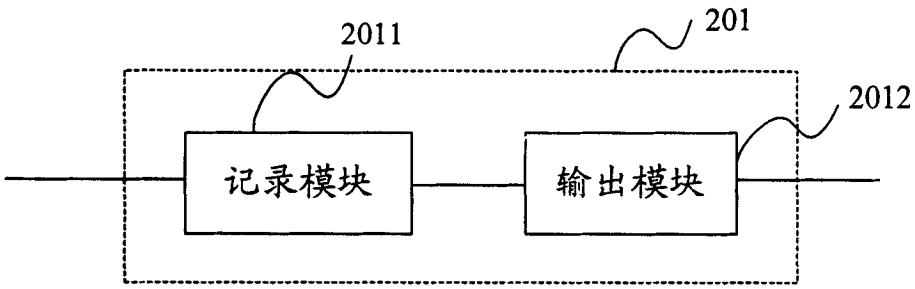


图 4

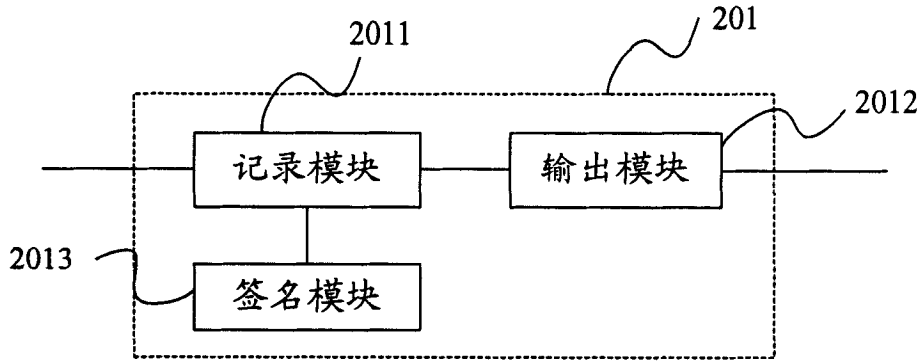


图 5