[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610146976.5

[43] 公开日 2008 年 6 月 4 日

[11] 公开号 CN 101193103A

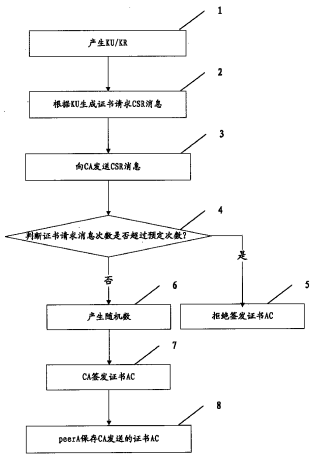
[22] 申请日 2006.11.24
[21] 申请号 200610146976.5
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 朱 贤 刘经及 符海芳 朱望斌 吕晓雨 李 朋 金洪波
[74] 专利代理机构 北京同达信恒知识产权代理有限公司
代理人 郭润湘
权利要求书 3 页 说明书 12 页 附图 6 页

[54] 发明名称

一种分配和验证身份标识的方法及系统

[57] 摘要

本发明公开了一种分配节点身份标识的方法，可解决现有技术中不能有效抵抗加入攻击、女巫攻击和 ID 欺骗攻击的问题。 所述的方法包括：节点向证书机构发送证书请求消息；所述证书机构根据所述证书请求消息生成并返回证书；所述节点根据所述证书生成节点身份标识。 本发明还公开了分配节点身份标识的系统、节点和证书机构。 根据本发明，在 AC 证书中，由于在 ID 生成的算法中引入了随机数，攻击者完全不能预知自己的 ID 和其范围；在 MC 证书中，ID 由用户的真实身份生成，攻击者不能伪造身份，生成其需要的 ID。 因此，通过 AC 证书和 MC 证书生成的 ID 可抵抗加入攻击。 AC 保证了用户的匿名性，而 MC 保证了用户身份的真实性，可以满足不同的安全需求。



1、一种分配身份标识的方法，其特征在于，包括:

节点向证书机构发送证书请求消息;

所述证书机构根据所述证书请求消息生成并返回证书;

所述节点根据所述证书生成节点身份标识。

2、根据权利要求1所述的分配节点身份标识的方法，其特征在于，所述方法具体包括:

节点向证书机构发送证书请求消息;

所述证书机构根据所述证书请求消息确定所述节点请求分配自动证书，则获得所述节点公钥，产生随机数，并根据所述节点公钥和所述随机数生成并返回自动证书;

所述节点根据所述自动证书中的随机数和节点公钥生成节点身份标识。

3、根据权利要求1所述的分配身份标识的方法，其特征在于，所述方法具体包括:

节点向证书机构发送证书请求消息;

所述证书机构根据所述证书请求消息确定所述节点请求分配手动证书，则验证所述用户身份，验证通过后根据所述手动证书请求消息生成并返回手动证书;

所述节点根据所述手动证书中的用户识别名生成节点身份标识。

4、根据权利要求1所述的分配身份标识的方法，其特征在于，所述证书请求消息包括所述节点公钥和/或所述用户识别名。

5、根据权利要求1所述的分配身份标识的方法，其特征在于，所述的方法还包括: 所述证书机构在接收到所述证书请求消息后，证书机构对用户申请证书的数量进行限制。

6、根据权利要求2所述的分配身份标识的方法，其特征在于，所述的证书机构根据所述节点公钥和所述随机数生成自动证书包括:

将随机数和节点公钥设置在自动证书的数据结构中；

利用证书机构的私钥对所述的数据结构进行签名。

7、根据权利要求1所述的分配身份标识的方法，其特征在于，所述证书机构对生成的证书进行管理，所述进行管理具体包括：限定所述证书的有效期，重发所述证书，回收所述证书；其中，

对证书进行重发时，验证该证书是否在有效期内，若在有效期内，则进行证书重发，否则，拒绝证书重发。

8、一种验证身份的方法，其特征在于，包括：

接收消息，所述消息带有发送者的身份标识和发送者的证书；

验证发送者的身份标识与证书的一致性。

9、根据权利要求8所述的验证身份的方法，其特征在于，如果所述发送者的证书为自动证书，则所述验证发送者的身份标识与证书的一致性具体包括：

从自动证书中获得随机数和发送者节点公钥；

根据所述随机数和发送者节点公钥计算节点身份标识，并将计算的节点身份标识与发送者身份标识进行比较，若比较结果一致，则发送者身份标识与自动证书一致。

10、根据权利要求8所述的验证身份的方法，其特征在于，如果所述发送者的证书为手动证书，则所述验证发送者的身份标识与证书的一致性具体包括：

从自动证书中获得用户识别名；根据所述用户识别名计算节点身份标识，并将计算的节点身份标识与发送者身份标识进行比较，若比较结果一致，则发送者身份标识与自动证书一致。

11、根据权利要求8所述的验证身份的方法，其特征在于，所述的方法还包括：利用证书机构的公钥对所述证书进行验证，若验证通过，则该自动证书有效。

12、根据权利要求8所述的验证身份的方法，其特征在于，所述的方法还

包括：当接收者对接收的消息进行验证时，首先验证所述的证书是否在有效期内，若在有效期内，则接收者对接收的消息进行验证。

13、一种分配身份标识的系统，其特征在于，包括：

证书请求单元，用于生成证书请求消息；

证书生成单元，用于根据所述证书请求消息生成证书；

身份标识生成单元，用于根据所述证书生成节点身份标识。

14、根据权利要求13所述的分配身份标识的系统，其特征在于，所述的证书生成单元包括公钥获取单元、随机数生成单元和自动证书生成单元，

所述公钥生成单元用于获取节点公钥；所述随机数生成单元用于生成随机数；所述自动证书生成单元用于根据所述节点公钥和所述随机数生成自动证书。

15、根据权利要求13所述的分配身份标识的系统，其特征在于，所述的证书生成单元包括身份验证单元、手动证书生成单元，

所述身份验证单元用于验证节点身份；

所述手动证书生成单元用于接收所述身份验证单元输出结果，并根据所述证书请求消息生成手动证书。

16、一种证书机构，其特征在于，包括：

接收单元，用于接收证书请求消息；

证书生成单元，用于根据所述证书请求消息生成证书。

17、一种节点，其特征在于，包括：

发送单元，用于向证书机构发送证书请求消息；

接收单元，用于接收证书机构签发的证书。

18、根据权利要求17所述的节点，其特征在于，所述的节点还包括：

验证单元，用于验证发送者的节点身份标识与所述证书的一致性。

一种分配和验证身份标识的方法及系统

技术领域

本发明涉及一种通信技术，尤其涉及一种分配和验证身份标识的方法及系统。

背景技术

因对等网（P2P，Peer-to-Peer）技术提供了一种新的共享资源的方法，因而P2P已成为目前国际计算机网络技术领域研究的一个热点。在P2P网络环境中，成千上万台彼此连接的计算机都处于对等的地位，每台主机既是资源请求者（Client）又是资源提供者（Server），因此，各台计算机不仅可向其它计算机发出请求，也可对其它计算机的请求做出响应，自愿提供资源与服务，因此在P2P网络中的每一台计算机被称之为Peer对等节点。

P2P网络大致可分为结构化（Structured）网络和非结构化（Unstructured）网络两类。结构化网络相比于非结构化网络具有扩展性高和查询速度快等优势，它允许应用程序以较小的跳数定位对象，同时每个节点的路由表仅需要很少的条目。在结构化P2P中，对象的分布和路由，主要由节点的身份标识(ID)和对象的键值(key)来决定，key和ID共享一个ID空间。以Chord环为例，该环中的每个节点都有唯一的ID，通常由其IP地址进行哈希得到（即ID=Hash(IP)，其中Hash为哈希函数），而对象的key由对象的名字进行哈希得到。Hash通常采用MD5或SHA1等安全哈希函数。对象根据其key，由某个节点保存和控制，该节点的ID为系统中大于等于此key的ID中最小的ID，此时称保存和控制该对象的节点为对象的根。如图1所示，对象K10由节点N14保存，N14是对象K10的根。同理，K24、K30由节点N32保存，节点N32为K24、K30的根。

如果一个对等网络中有n个节点，那么任意两个节点之间的通信可以在O(log n)的时间内完成。每个节点通过维护一张含有⌈log n⌉条目的系统路由表，便可以完成路由工作。这⌈log n⌉个条目中的第i条记录了从当前节点的ID加上2^{i-1}后，系统中存在大于等于该ID值且最小的ID。在具体的路由过程中，当节点p与节点q进行通讯时，节点p会在自己的路由表中查找节点q，若找到则停止，否则，在自己的路由表中查找出比节点q小的最大身份标识r，并将请求转发给节点r。节点r收到请求以后会进行和p一样的操作，直至请求顺利抵达q。

由于结构化P2P网络的对象分布和路由算法与节点的ID密切相关，攻击者可以基于ID对网络发起攻击，基于ID的攻击类型可分为：加入攻击、女巫攻击和ID欺骗攻击，现分别进行介绍。

加入攻击（Join attack）：攻击者可以通过选择自己的ID，对某些节点发起攻击。例如，攻击者为了占据被攻击者路由表的第i个条目，它可以通过计算被攻击者ID1加上2i-1的值，并使其控制的节点ID的值为大于等于ID1+2i-1且在系统为最小，从而可以占据被攻击节点的某些路由表条目。图2给出了一个攻击实例，其中，节点40、55、80、100为攻击者，例如节点27的第7个条目，27+26=91，本应填入正常节点128，但由于攻击者在系统中加入了一个ID为100的节点，使第7个条目填入恶意节点节点100。当被攻击者访问网络经过这些条目时，会将请求发往攻击者。此时攻击者可以将请求包丢弃，或返回不正确的信息，使被攻击者无法正常访问部分网络。如果多个攻击者对某些节点同时发起加入攻击，可以使被攻击者路由表中绝大部分条目被污染，导致被攻击者无法访问大部分网络。例如图中的节点27的路由表条目就受到了这种攻击。另外，攻击者也可以通过这种方式取得某些对象的访问控制权。例如，攻击者如果要攻击某对象，则可以以某ID加入网络，此ID是系统中所有大于等于此key的最小ID，于是攻击者成为某对象的根。此时，攻击者可以删除、毁坏或拒绝对此对象的访问。

女巫攻击（Sybil attack）：当攻击者不能选择自己的ID时，它仍可以通过

大量申请节点ID，增大其控制的节点ID在被攻击者或整个网络路由表中出现的概率，同样可以控制被攻击者或对等网络。

ID欺骗攻击（ID spoofing attack）：攻击者可以想办法使某个节点离线，然后冒充其ID与其它节点通信。

为了对抗这些攻击，在现有技术中有两种节点ID分配方案，下面对它们分别进行介绍。

方案一、利用证书机构（Certification Authority，即CA）进行节点ID的分配。每个节点向CA申请一个ID证书，其中包含节点公钥（Public Key，即KU）与ID的绑定，ID由CA随机生成。节点需要使用证书中公钥对应的私钥（Private Key，即KR）对待发送的消息签名，证明它拥有某ID。此时，节点不能决定自己的ID，也无法假冒其它节点的ID，因此这种方法可以抵抗Join攻击和ID spoofing攻击。

然而，由于P2P系统中节点数量巨大、动态性强的特点，会加剧CA技术中的证书回收等问题，这时在该方案仅仅简单地引入CA，还会给P2P系统增加复杂性和高昂的维护成本。另外，如果用户申请证书时需要提供真实的身份证明，并在证书中绑定身份，这种方法会令很多P2P用户无法接受；如果不需用户提交身份证明，攻击者可以向CA申请大量的证书，容易发起Sybil攻击。

方案二、使用自认证（Self-Certifying）技术，不需要CA参与，是一种全分布式的方案。节点自己产生一对公私钥对(KU/KR)，然后根据其公钥生成ID，可以表示为：ID=Hash(KU)。节点使用KR对待发送的消息签名，证明它拥有KU。由于采用安全Hash函数，攻击者难以产生另外一对KU_1/KR_1，使得Hash(KU1)=ID。因此节点证明了它拥有KU，也就证明了它拥有ID，从而可以抵抗ID spoofing攻击。如果对自认证不加限制，攻击节点通过大量生成ID，可以发起Sybil攻击。因此，可以采用在线验证方案，即，节点产生自认证ID后，需要向一个中心化的服务器IPR Server注册ID及其IP地址，服务器中的安全策略可以规定每个IP只能申请有限的几个(或1个)ID；其后其它节点与此节点交互

时，向服务器解析此ID，确认此ID是否经过注册。

然而，如果攻击者有较强的计算能力，它能够在一定时间内，生成大量KU，然后选择一个自己需要的KU，进而生成ID，用于攻击某些结点及路由表。攻击者虽然不能生成某个其所期望的指定的ID，不能进行ID spoofing攻击，但它生成一个与其比较接近的ID是可能的，其计算复杂性比生成一个指定的ID大大降低，这样同样可以有效地进行Join攻击。网络中节点越少，这种攻击的计算复杂性越低，即攻击越容易。另外，为了抵抗Sybil攻击，引入中心化服务器的同时也引入了单点故障，节点每次在进行验证时，都需要与此服务器进行交互。

发明内容

本发明的实施例是提供一种分配和验证节点身份标识的方法及系统，可解决不能有效抵抗加入攻击、女巫攻击和ID欺骗攻击的问题。

本发明的实施例提供了一种分配身份标识的方法，包括:

节点向证书机构发送证书请求消息;

所述证书机构根据所述证书请求消息生成并返回证书;

所述节点根据所述证书生成节点身份标识。

本发明的实施例还公开了一种验证身份的方法，包括:

接收消息，所述消息带有发送者的身份标识和发送者的证书;

验证发送者的身份标识与证书的一致性。

本发明的实施例还公开了一种分配身份标识的系统，包括:

证书请求单元，用于生成证书请求消息;

证书生成单元，用于根据所述证书请求消息生成证书;

身份标识生成单元，用于根据所述证书生成节点身份标识。

本发明的实施例还公开了一种证书机构，包括:

接收单元，用于接收证书请求消息;

证书生成单元，用于根据所述证书请求消息生成证书。

本发明的实施例还公开了一种节点，包括:

发送单元，用于向证书机构发送证书请求消息；

接收单元，用于接收证书机构签发的证书。

根据本发明，在AC证书中，由于在ID生成的算法中引入了随机数，攻击者完全不能预知自己的ID和其范围；在MC证书中，ID由用户的真实身份生成，攻击者不能伪造身份，生成其需要的ID。因此，通过AC证书和MC证书生成的ID可抵抗加入攻击。

附图说明

图1示出了Chord环结构的P2P网络；

图2示出了在Chord环结构的P2P网络中攻击实例；

图3示出了本发明实施例的AC（自动）证书的签发流程；

图4示出了本发明实施例的ID认证过程；

图5示出了本发明实施例的分配节点身份标识的系统；

图6示出了本发明实施例的证书机构；

图7示出了本发明实施例的节点。

具体实施方式

为了便于本领域一般技术人员理解和实现本发明，现结合附图描绘本发明的实施例。

本发明的实施例是采用自动证书（Automatic certificate，即AC)和手动证书(Manual certificate，即MC)这两类证书对节点的ID进行管理。这两类证书都需要CA进行签发。对于AC，不需要CA管理员手工参与证书的签发，CA程序自动签发此证书；对于MC，需要进行真实身份证明，CA才可以签发此证书。

为了便于下面的描述，首先介绍一下AC、MC和CSR的证书格式。

AC证书格式可以描述为[Version, Serial Number, Peer Public Key, Random Number, Subject Name, Issuer Name, Validity, Algorithms]KRIssuer。其中，

Version指证书的版本。Serial Number指证书的序列号，对一个CA来说，每个证书的序列号必须是唯一的（对于重发证书，认为仍然是同一个证书）。Peer Public Key指节点的公钥。Random Number指CA为此证书产生的一个随机数。Subject Name指节点的名称，即节点的DN。Issuer Name指证书发布者的名称，通常为CA的DN。Validity指此证书的有效期，它由一对起始时间和终止时间构成，在此时间之外，证书无效。Algorithms指此证书中密钥对产生所用到的公钥算法和签名算法。KRIssuer指Issuer Name所对应的私钥，通常为CA的私钥，CA使用此私钥对此证书签名。

MC证书格式可以描述为[Version, Serial Number, Peer Public Key, Subject Name, Issuer Name, Validity, Algorithms]KRIssuer。MC中的字段与AC证书中的含义相同，其中不需要Random Number字段。

CSR证书的格式可以描述为[Version, Type, Serial Number, Peer Public Key, Subject Name, Algorithms] KRIssuer。CSR中的大部分字段与AC证书中的含义基本相同。其中Type指此CSR所申请的类型，它可以是AC或MC类型。Serial Number是序列号，当CSR是一个新的证书请求时，此字段为0；当CSR是一个证书重发请求时，此字段记录旧证书的序列号。CSR是一个自签名证书，KRIssuer是CSR请求者的私钥，它与Peer Public Key构成一对公私钥对。

这些证书可以是X.509证书，也可以不是。如果是X.509证书，AC中的Random Number、CSR中的Type可以通过在X.509证书的扩展部分定义相应的扩展来实现。对于AC和MC证书，可以在X.509证书的扩展部分定义证书类型扩展来加以区别。

AC和MC这两类证书都可由用户自己产生公私钥对，然后由公钥生成证书请求（Certificate Signing Request，即CSR）消息，并通过CSR消息向CA请求证书；也可由CA代表用户产生公私钥对，将私钥分发给用户，并签发证书。下面介绍两种证书的签发及节点ID的认证流程。另外，由于对等网中节点的数量极其巨大，节点加入和退出系统频繁，证书的管理（如证书的重发和回收）也

是一项十分重要的工作。因此，下面还要介绍证书的重发和回收流程。

一、AC签发流程

如图3所示，节点首先要获得CA对其签发的证书，才能正常加入和使用对等网。AC签发流程如下。

步骤1、产生KU/KR，当用户peerA希望加入对等网络时，自己产生公私钥对KU/KR(或委托CA产生，并从CA处安全地获得KR)。

步骤2、根据KU生成CSR消息，所述的CSR消息包含KU。

步骤3、向CA发送CSR消息，以便注册CSR消息，以便获得节点的ID。在CSR消息中，可以将节点的IP地址一起发送，也可以由CA自己获取节点的IP地址。

用户向CA发送CSR消息时，也可通过在线注册的形式实现。CA可以通过在线注册，获得用户端的IP地址。这种注册可以基于HTTPS，在web页面上直接粘贴CSR；也可以基于SSL，通过专用的程序上传CSR。

步骤4、CA收到CSR消息后，从CSR消息中取出IP地址（或直接获取请求者的IP地址）。然后从CA维护的IP注册数据库中，查询此IP地址对应的证书请求次数。判断证书请求消息次数是否超过预定次数，若是，则执行步骤5；否则执行步骤6。

在CA维护的IP注册数据库中，记录有一段时间区间内（例如1周）每个IP地址证书请求消息次数。当某个IP地址的证书请求消息次数达到上限后，在当前的时间区间内，CA将拒绝此IP地址发起的新的CSR注册。将证书请求消息次数上限（即，预定次数）与一个时间区间关联起来，只要时间区间不是太小，仍可有效的防止攻击者获得大量的AC。一个谨慎的CA可以将此时间区间设定为无限大。

步骤5、CA拒绝签发证书AC。

步骤6、CA首先利用一个安全随机数发生器产生一个随机数rnd。

步骤7、CA签发证书AC。

根据CSR消息和rnd签发证书AC，即从CSR消息中提取KU和其它相关字段（如：Subject Name，Algorithms），并将rnd加到准备签发的AC证书数据结构中，然后使用CA的私钥对证书数据结构签名，生成AC证书，接着将生成的AC证书发给peerA。

CA程序在启动时，直接载入CA的私钥，并在随后的运行中，使用此私钥签发证书。

步骤8、peerA保存CA发送的AC证书，以便利用AC节点与其它节点进行通信。

这样，就可根据KU和rnd生成节点ID，即ID=Hash(KU||rnd)。根据对等网的不同，Hash可采用不同的安全Hash函数。可以将ID作为证书中的一个字段，在证书中进行发布.也可以基于公式ID=Hash(KU||rnd)，在P2P网络运行时生成。对于后一种方式，可以更好的适应不同对等网底层结构的需求，使ID独立于具体的对等网结构。

如图4所示，下面以P2P网络运行时生成ID为例说明节点ID认证流程，在节点之间进行通信互发消息时，需要进行ID认证。这种消息可以是节点加入对等网时的加入请求，路由表更新消息，也可以是业务数据的发送。认证过程如下：

步骤41、在发送的P2P消息上附加发送者ID、发送者AC证书和发送者对消息的数字签名。

步骤42、消息接收者验证AC证书的有效性，验证者机器中需要预先安装CA的公钥证书。在进行验证时，使用CA的公钥证书验证AC证书是否是CA所发；同时验证AC证书是否已过期，证书是否已被回收。

步骤43、判断ID与AC证书是否一致，即，从AC证书中取出KU和rnd，计算Hash(KU||rnd)的值，判断该值是否与ID一致，若一致，则说明发送者ID与AC证书是一致的，否则，发送者ID与AC证书是非绑定的。

步骤44、验证经数字签名的消息与AC证书是否一致，即消息是否是由AC证书中公钥对应的私钥签名的。

通过步骤42和步骤43的验证，可以判断某ID是否是合法的。再通过步骤44的验证，可以确认消息是否是某合法的ID所发送的。例如，对于节点加入对等网的加入请求，通过步骤42和步骤43可以确定有一个合法的ID，通过步骤44可以知道加入请求是这个合法的ID所发出的，于是其它节点可以允许此节点加入对等网。

由于在AC中加入了随机数rnd，用户完全不能预知自己的ID和其范围，从而可防止加入攻击。另外，由于证书中的DN只是一个代名，证书中没有与用户真实身份相关的信息，保证了用户的匿名性。

二、MC证书签发流程

MC证书的签发过程按照标准的PKC（Public Key Certificate，公钥证书）进行管理，CA在签发证书的过程中需要验证用户的真实身份，如验证用户所提供的用户材料是否真实有效。

CA管理员需要手工参与证书签发。用户申请MC，需要向CA证明其真实的身份。MC是DN（用户识别名）与证书中公钥的绑定，它不保证匿名性，使通信的双方可以知道对方的真实身份，可以满足某些应用更高的安全性需求。

当使用MC证书时，节点ID由DN生成，即ID=Hash(DN）。

节点间的ID认证流程与采用AC时ID认证流程基本相同，只是在计算节点ID时采用下述公式：ID=Hash(DN)。

由于DN是用户的真实身份，所以，MC证书中不需要rnd字段，攻击者无法为了获得某个ID，或为了使其ID处于某个范围之内，而伪造身份，因此攻击者无法发起加入攻击。另外，由于ID由DN生成，用户可以通过输入DN，来实现对其它节点的查找。由于DN比KU有更好的可读性，因此它可以更好的满足即时通信类应用的安全需求。

另外，为了抵抗女巫攻击，CA针对每个用户的证书申请数量进行限制。

三、证书回收和重发

由于对等网中节点的数量极其巨大，节点加入和退出系统频繁。一种可行

的方法，使用短期证书，以降低证书回收列表(Certificate Revocation List, 即CRL)的开销。

由于采用短期证书，每个ID的生命周期也将变得很短。因此，当证书有效期快到时，用户可以使用申请证书类似的流程，请求证书的重发。

对于AC证书，节点从旧证书中取出序列号、公钥信息，在CSR消息中，包含此序列号和公钥。CA根据CSR消息中的序列号，在证书库中进行查询；如果找到此证书，且证书未被回收，则取出其中的随机数，并重新签发新的证书，且新的证书采用与旧证书相同的序列号。这种方式可以使节点的ID，不会因为证书的重发而变化。

节点在向CA发送CSR消息时，也可以同时将旧证书一起发给CA。此时CA不用查证书库，只用验证此证书是否被回收了。

对于MC，处理流程与AC类似，只是不需要随机数。

如果一个证书A未到期时，申请证书重发，并生成一个新的证书A'，之后（在A到期之前）证书的拥有者申请作废证书A。由于A和A'有相同的序列号，因此两者同时作废。CA在维护CRL时，只有过了A'的有效期，才能在CRL中删除对A的回收记录。

为减小CA管理开销，如果还未到某证书有效期的开始时间，不能基于此证书的序列号申请重发新的证书。

证书如果已过期，不能基于它申请重发证书。否则攻击者获得某一证书后，可以对其进行长期的分析，最终获得证书中KU对应的KR，然后申请证书的重发，从而进行IP Spoofing攻击。

如图5所示，本发明的实施例还公开了一种分配节点身份标识的系统，包括：证书请求单元，用于生成证书请求消息；证书生成单元，用于根据所述证书请求消息生成证书；身份标识生成单元，用于根据所述证书生成节点身份标识。

所述的证书生成单元包括公钥获取单元、随机数生成单元和自动证书生成

单元，所述公钥生成单元用于获取节点公钥；所述随机数生成单元用于生成随机数；所述自动证书生成单元用于根据所述节点公钥和所述随机数生成自动证书。

所述的证书生成单元包括身份验证单元、手动证书生成单元，所述身份验证单元用于验证节点身份；所述手动证书生成单元用于接收所述身份验证单元输出结果，并根据所述证书请求消息生成手动证书。

如图6所示，本发明的实施例还公开了一种证书机构，包括：接收单元，用于接收证书请求消息；证书生成单元，用于根据所述证书请求消息生成证书。

如图7所示，本发明的实施例还公开了一种节点，包括：发送单元，用于向证书机构发送证书请求消息；接收单元，用于接收证书机构签发的证书；验证单元，用于验证发送者的节点身份标识与所述证书的一致性。

本发明的实施例还公开了一种节点，包括：发送单元，用于向证书机构发送包括节点公钥和节点IP地址的证书请求消息；接收单元，用于接收证书机构签发的自动证书；验证单元，用于验证自动证书的有效性；验证发送者的节点身份标识与自动证书的一致性；验证自动证书与数字签名的一致性。

根据本发明，在AC证书中，由于在ID生成的算法中引入了随机数，攻击者完全不能预知自己的ID和其范围；在MC证书中，ID由用户的真实身份生成，攻击者不能伪造身份，生成其需要的ID。因此，通过AC证书和MC证书生成的ID可抵抗加入攻击。

对于AC，由于CA记录了每个IP在一段时间内注册CSR的次数，攻击者无法大量的获得合法的ID；对于MC，CA针通过对每个用户的证书申请数量进行限制。使得攻击者也无法获得大量的ID，因此，通过AC证书和MC证书生成的ID可抵抗女巫攻击。

由于AC证书和MC证书中采用基于公钥密码学的证书机制，攻击者无法冒充拥有其它用户的证书。而ID由证书中相应字段生成，因此攻击者无法冒充其它用户的ID，从而可抵抗ID欺骗攻击。

在节点进行ID认证时，不需要向CA发起查询。对等节点拥有合法的证书，即表示对等节点没有申请大量的证书。CA只参与节点申请证书的流程，节点间的数据交互不需要CA参与。节点申请证书与节点间的数据交互次数相比，只占很小的比例，因此系统没有单点故障问题。

通过AC的引入，大大降低了CA的管理开销。由于对等网络中的节点数量往往极其巨大，对每个用户进行真实身份的认证，将给CA带来极大的负担，用户也往往不愿意参与。通过引入AC，只需要检测用户没有申请过多的证书，即可由CA程序自动进行证书的签发，用户和CA都只需要很低程度的参与。

在自认证技术中，它只提供了ID与所发消息间的认证，但并不能提供真实用户与所发消息间的认证，即可以知道消息是哪个ID所发，但不能确认消息到底是哪个人所发。这对于某些应用或通信需求，其安全性是不够的。由于不能确认对方的真实身份，节点往往难以确认对方的可信度。为了解决此问题，通常需要采用信任评估的技术，对每个ID加上一个信任值，此信任值根据用户在系统中的表现而变化。但信任评估技术目前并不成熟，容易受到一些攻击(例如共谋攻击)。本方案采用了两种证书，AC不提供真实身份的认证，可以满足匿名性的需求；MC采用真实身份的认证，它由CA来保证身份的可信度，可以满足较高级别的安全需求。例如用户可以选择与一个有AC证书的对等方通信，但当用户要与其它节点进行一些比较机密的通信时，它可以选择只与有MC证书的对等方通信。

虽然通过实施例描绘了本发明，但本领域普通技术人员知道，在不脱离本发明的精神和实质的情况下，就可使本发明有许多变形和变化，本发明的范围由所附的权利要求来限定。

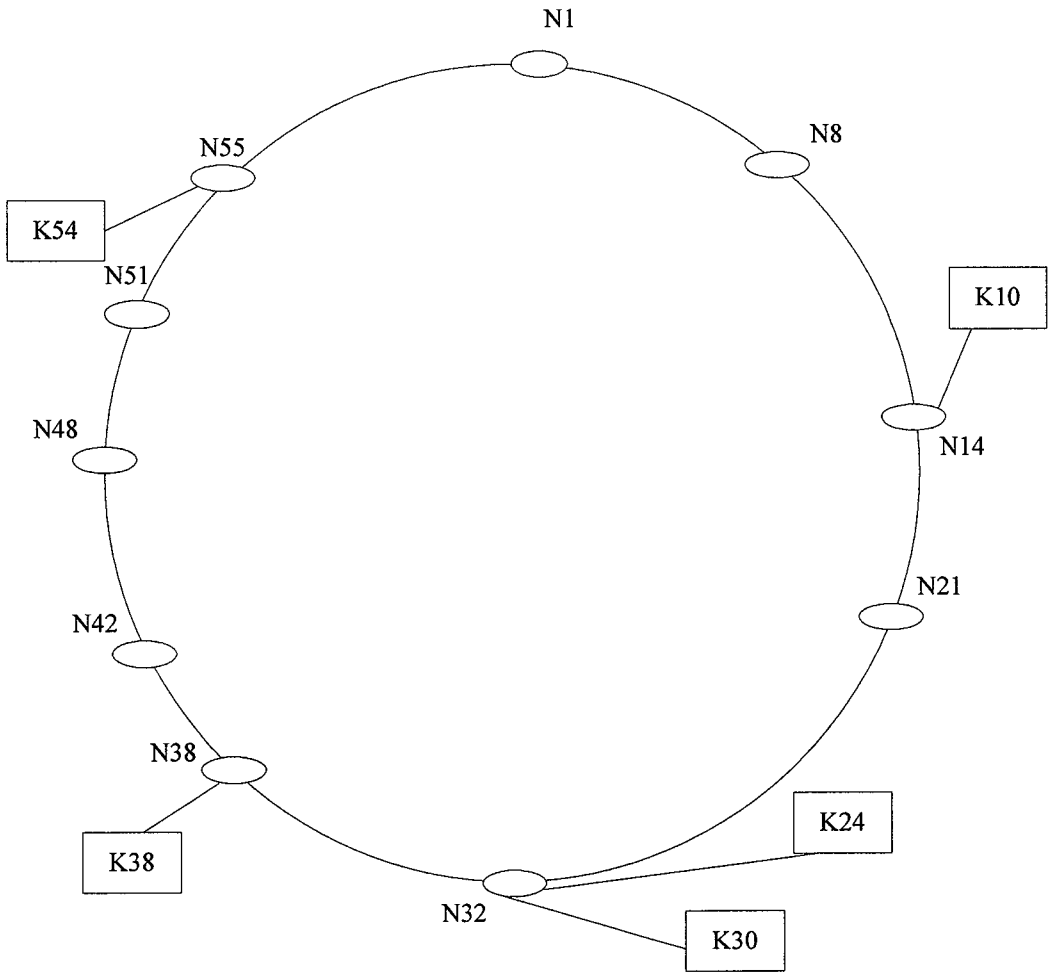
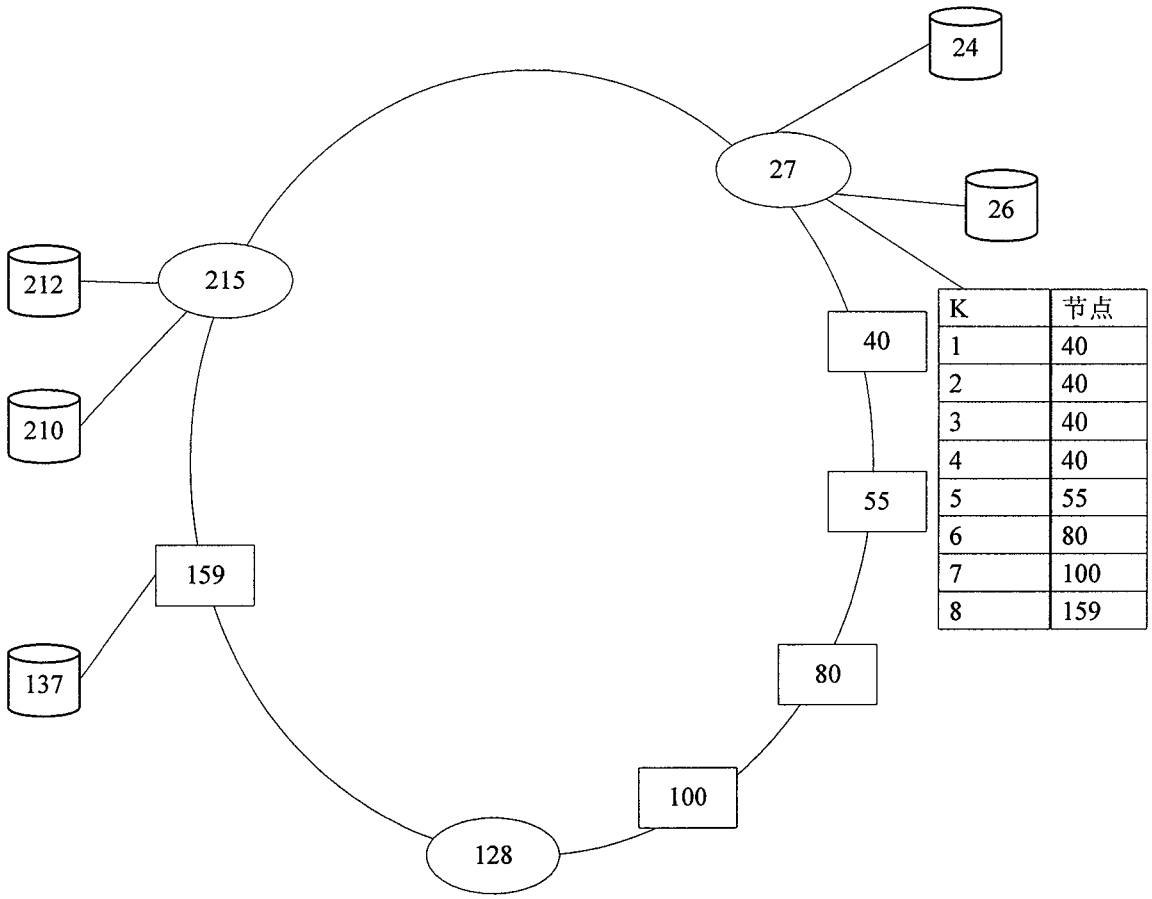


图 1



K	节点
1	40
2	40
3	40
4	40
5	55
6	80
7	100
8	159

图 2

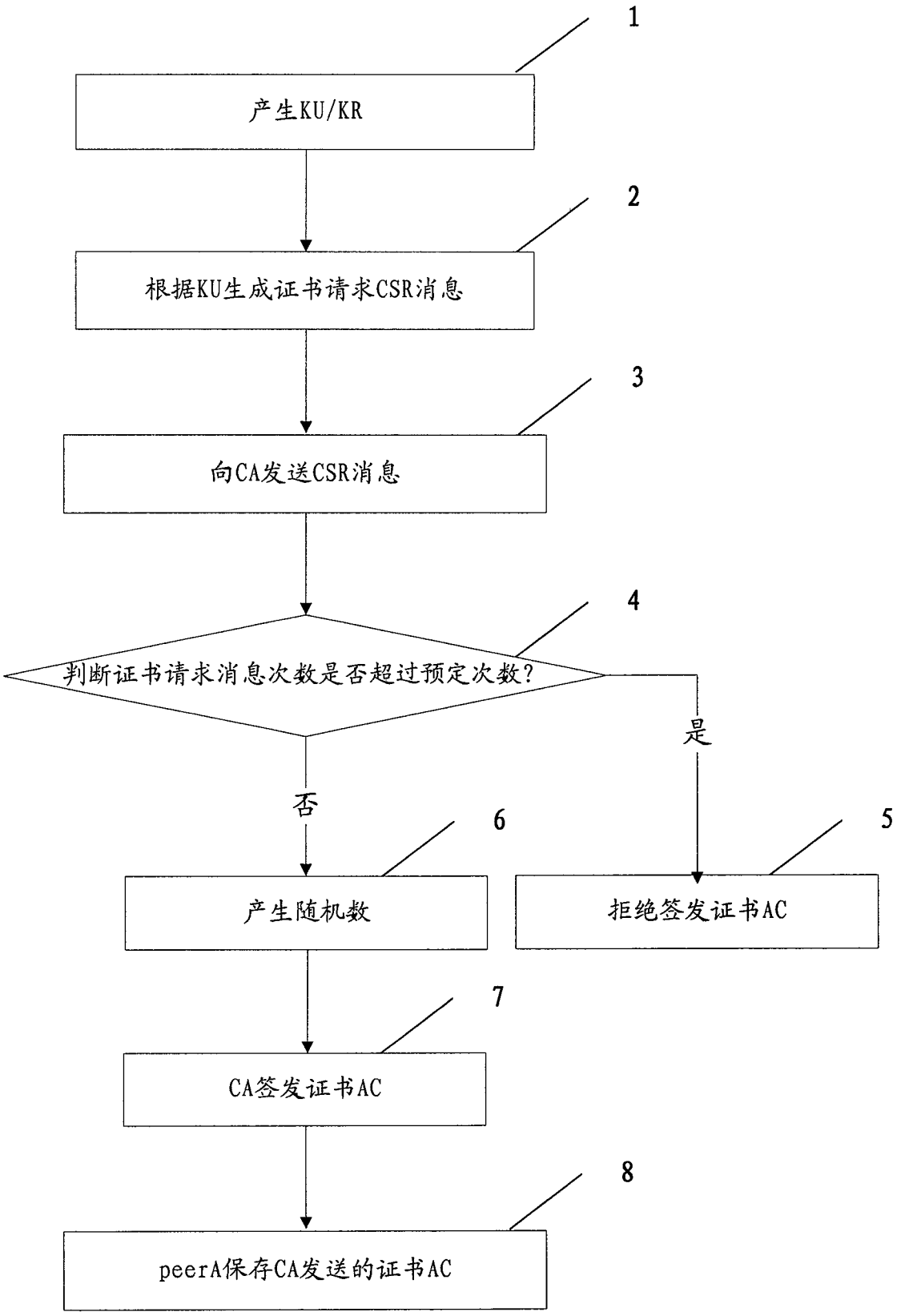

1
产生KU/KR
2
根据KU生成证书请求CSR消息
3
向CA发送CSR消息
4
判断证书请求消息次数是否超过预定次数?
是
否
5
拒绝签发证书AC
6
产生随机数
7
CA签发证书AC
8
peerA保存CA发送的证书AC

图 3

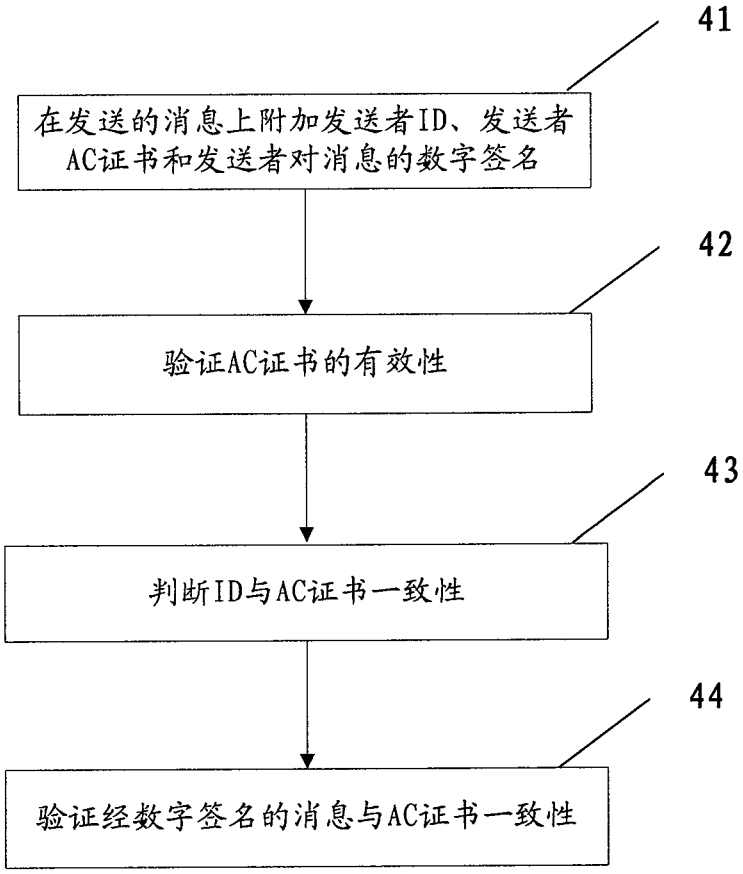

41
在发送的消息上附加发送者ID、发送者AC证书和发送者对消息的数字签名
42
验证AC证书的有效性
43
判断ID与AC证书一致性
44
验证经数字签名的消息与AC证书一致性

图 4

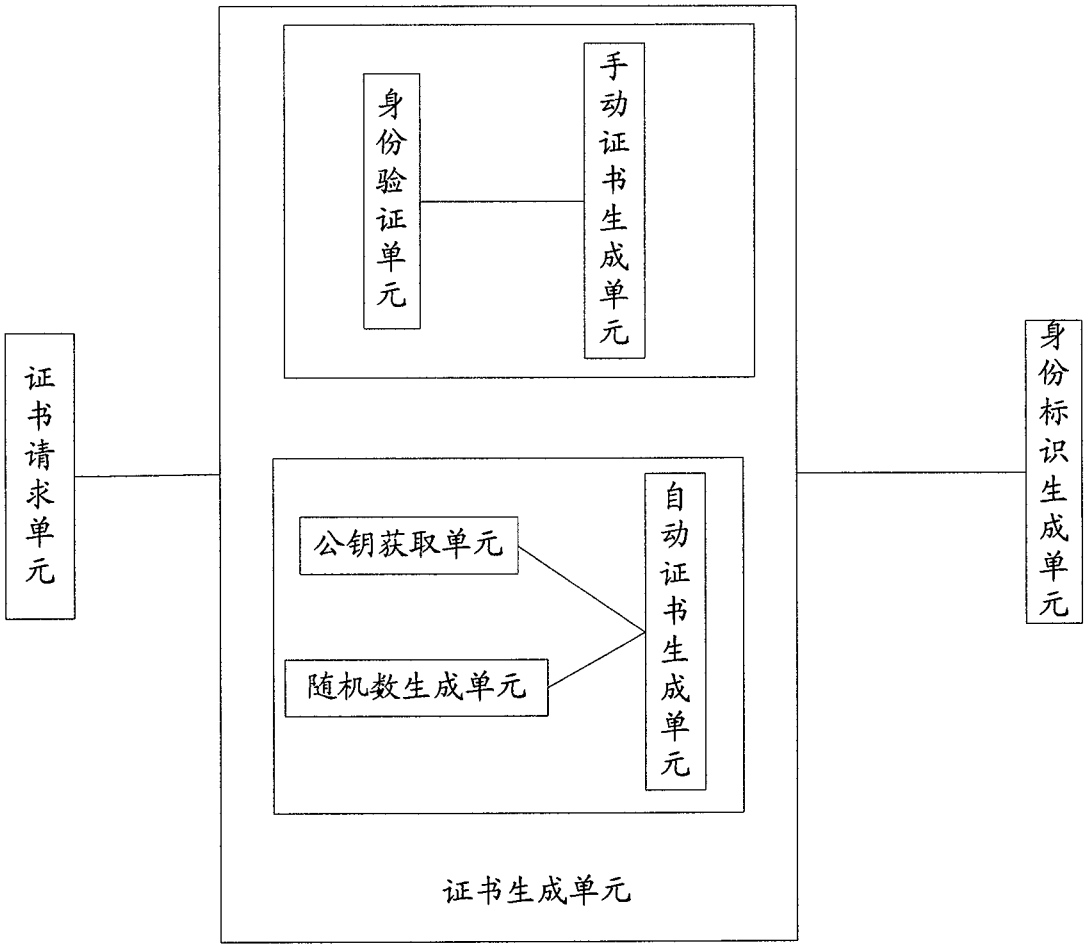

证书请求单元
身份验证单元
手动证书生成单元
公钥获取单元
随机数生成单元
自动证书生成单元
证书生成单元
身份标识生成单元

图 5

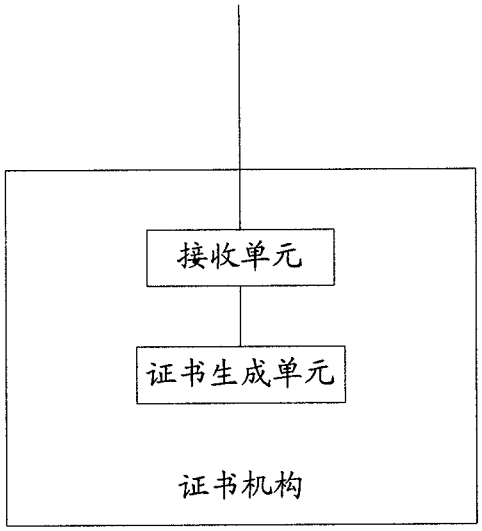


图 6

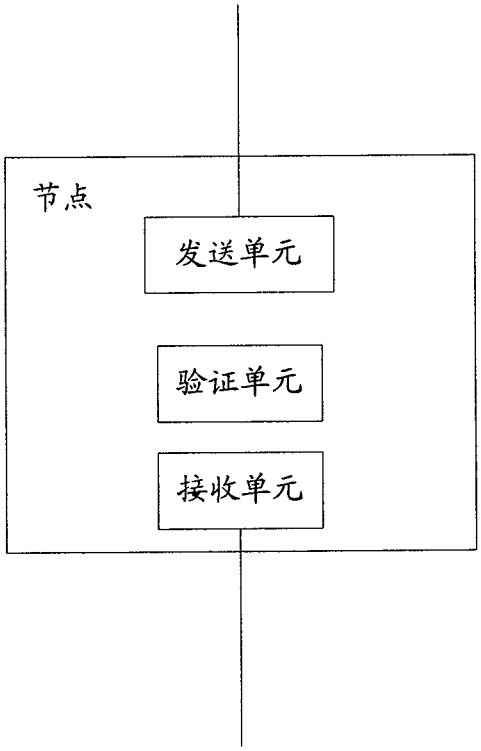


图 7