一种互联网主机命名和通信方法及系统

申请号：200810225793.1
申请日：2008-11-13

申请(专利权)人　中国科学院计算机网络信息中心
地址　100190 北京市海淀区中关村南4街4号
发明(设计)人　毛伟 罗万明 李晓东

主分类号　H04L9/08(2006.01)I
分类号　H04L9/08(2006.01)I H04L12/56(2006.01)I
公开(公告)号　101741545A
公开(公告)日　2010-06-16
专利代理机构　北京润泽恒知识产权代理有限公司 11319
代理人　苏培华

(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 101741545 A
(43)申请公布日 2010.06.16

(21)申请号 200810225793.1

(22)申请日 2008.11.13

(71)申请人 中国科学院计算机网络信息中心
地址 100190 北京市海淀区中关村南4街4号

(72)发明人 毛伟 罗万明 李晓东

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 12/56(2006.01)

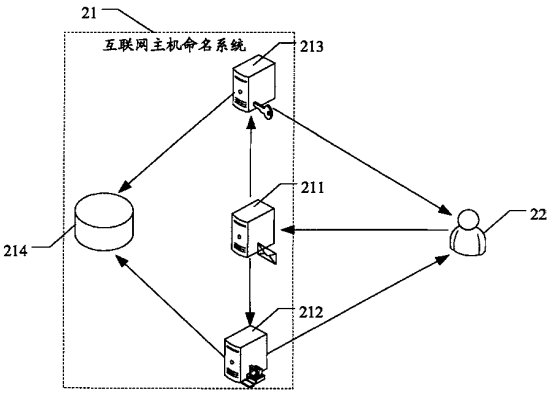
权利要求书 3 页 说明书 9 页 附图 5 页

(54)发明名称

一种互联网主机命名和通信方法及系统

(57)摘要

本发明提供了一种互联网主机命名方法，采用IPv6地址作为互联网主机的实名地址，包括：依据互联网主机的地址申请，生成一个标记符；分配IPv6地址；将分配给该主机的IPv6地址，连同所述标记符发送给该主机和密钥数据库；生成加密密钥；将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；将由相同标记符标记的所述IPv6地址和加密密钥作为一组IPv6地址/加密密钥对进行存储。采用本发明互联网主机命名方法能够实现信息溯源，有效杜绝地址假冒、垃圾信息泛滥、大量入侵和攻击别的用户主机或服务器现象的发生，有效增强互联网的安全性。



CN 101741545 A

1. 一种互联网主机命名方法，其特征在于，采用 IPv6 地址作为互联网主机的实名地址，该方法包括：

依据互联网主机的地址申请，生成一个标记符；

分配 IPv6 地址，将分配给该主机的 IPv6 地址，连同所述标记符发送给该主机和密钥数据库；

生成加密密钥，将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；

将由相同标记符标记的所述 IPv6 地址和加密密钥作为一组 IPv6 地址 / 加密密钥对进行存储。

2. 根据权利要求 1 所述的互联网主机命名方法，其特征在于，所述接收地址申请、分配 IPv6 地址和生成加密密钥分别由三个独立的服务器完成。

3. 根据权利要求 1 所述的互联网主机命名方法，其特征在于，每个所述 IPv6 地址对应一个所述加密密钥，所述加密密钥为一个 128 位的随机数。

4. 一种基于实名地址的互联网主机通信方法，其特征在于，采用 IPv6 地址作为互联网主机的实名地址，该方法包括：

依据互联网主机的地址申请，生成一个标记符；

分配 IPv6 地址，将分配给该主机的 IPv6 地址，连同所述标记符发送给该主机和密钥数据库；

生成加密密钥，将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；

将由相同标记符标记的所述 IPv6 地址和加密密钥作为一组 IPv6 地址 / 加密密钥对进行存储；

互联网主机依据所接收的所述 IPv6 地址 / 加密密钥对，生成公 / 私密钥对；

互联网主机利用所述公 / 私密钥对与其他互联网主机或服务器进行通信。

5. 根据权利要求 4 所述的互联网主机通信方法，其特征在于，每个所述 IPv6 地址对应一个所述加密密钥，所述加密密钥为一个 128 位的随机数，所述加密密钥中包括安全参数。

6. 根据权利要求 4 所述的互联网主机通信方法，其特征在于，所述生成公 / 私密钥对的方法包括：

将分配 IPv6 地址 64 位的子网前缀与 64 位的全为零的场点本地地址串连，构成 128 位的明文；

将所述明文加密为密文；

对所述密文执行安全散列算法，将所得结果进行划分，得到哈希值 1 和哈希值 2；

判断所述哈希值 1 的预定位数据与所述安全参数乘积后得到的 (m×h) 位数值与零的比较，如果它们都为零或所述安全参数为零，则执行下一步；如果不为零，则密文加 1，整型变量加 1 后，返回执行上一步；其中，m 为所述预定位数值的位数，h 为所述安全参数的安全级别；

对所述哈希值 2 与整形变量串连后的数值执行所述安全散列算法，结果记为哈希值 3，将所述哈希值 3 作为私钥；

依据所述私钥，由预置的公钥密码算法生成对应的公钥。

7. 根据权利要求 6 所述的互联网主机通信方法，其特征在于，所述对密文执行安全散列算法后得到一串 160 位元的数值，最左边的 112 位记为所述哈希值 1，最右边 48 位记为所

述哈希值 2；

所述哈希值 1 的预定位数据为所述哈希值 1 的最左边 16 位数据。

8. 一种互联网主机命名系统，其特征在于，包括：

IPv6 地址 / 密钥服务器，用于处理互联网主机的地址申请、发送标记符标记的地址分配命令给 IPv6 地址服务器和所述标记符标记的加密密钥生成命令给加密密钥生成器；

IPv6 地址服务器，用于分配 IPv6 地址作为所述互联网主机的实名地址，发送所述标记符标记的所述 IPv6 地址给所述互联网主机和密钥数据库；

加密密钥生成器，用于生成加密密钥，发送所述标记符标记的所述加密密钥给主机和密钥数据库；

密钥数据库，用于存储相同标记符标记的 IPv6 地址 / 加密密钥对。

9. 根据权利要求 8 所述的互联网主机命名系统，其特征在于，每个所述 IPv6 地址对应一个所述加密密钥，所述加密密钥为一个 128 位的随机数。

10. 根据权利要求 8 所述的互联网主机命名系统，其特征在于，所述 IPv6 地址 / 密钥服务器，包括：

申请接收模块，用于接收所述互联网主机的地址申请；

标记符生成模块，用于生成一个标记符；

地址分配命令发送模块，用于向所述 IPv6 地址服务器发出一个由所述标记符标记的地址分配命令；

加密密钥命令发送模块，用于向所述加密密钥生成器发出一个由所述标记符标记的加密密钥生成命令。

11. 一种基于实名地址的互联网通信系统，其特征在于，包括互联网主机命名系统和互联网主机，其中，所述互联网主机命名系统，包括：

IPv6 地址 / 密钥服务器，用于处理互联网主机的地址申请、发送标记符标记的地址分配命令给 IPv6 地址服务器和所述标记符标记的加密密钥生成命令给加密密钥生成器；

IPv6 地址服务器，用于分配 IPv6 地址作为所述互联网主机的实名地址，发送所述标记符标记的所述 IPv6 地址给主机和密钥数据库；

加密密钥生成器，用于生成加密密钥，发送所述标记符标记的所述加密密钥给主机和密钥数据库；

密钥数据库，用于存储相同标记符标记的 IPv6 地址 / 加密密钥对；

所述互联网主机包括：

公 / 私密钥对生成模块，根据所接收的相同标记符标记的 IPv6 地址 / 加密密钥对，生成公 / 私密钥对；

通信模块，用于与其他互联网主机或服务器通过所述生成的公 / 私密钥对进行通信。

12. 根据权利要求 11 所述的互联网通信系统，其特征在于，所述公 / 私密钥对生成模块包括：

明文生成单元，用于将分配 IPv6 地址 64 位的子网前缀与 64 位的全为零的场点本地地址串连，构成 128 位的明文；

密文生成单元，用于利用加密算法将所述明文加密为密文；

哈希值划分单元，用于对所述密文执行安全散列算法，将所得结果划分为哈希值 1 和

哈希值 2；

判断单元，判断哈希值 1 的预定位数据与所述安全参数乘积后得到的 (m×h) 位数值与零的比较结果，其中，m 为所述预定位数据的位数，h 为所述安全参数的安全级别；

私钥生成单元，对所述哈希值 2 与整形变量串连后的数值执行所述安全散列算法，结果记为哈希值 3，将所述哈希值 3 作为私钥；

公钥生成单元，依据所述私钥由预置的公钥密码算法生成对应的公钥。

13. 根据权利要求 12 所述的互联网主机通信系统，其特征在于，所述对密文执行安全散列算法后得到一串 160 位元的数值，最左边的 112 位记为所述哈希值 1，最右边 48 位记为所述哈希值 2；

所述哈希值 1 的预定位数据的位数 m 为所述哈希值 1 的最左边 16 位。

一种互联网主机命名和通信方法及系统

技术领域

[0001] 本发明涉及互联网技术领域，特别是涉及一种互联网主机命名系统及其公 / 私密钥对生成方法。

背景技术

[0002] 目前我们使用的互联网技术为第二代互联网 IPv4 技术，它的最大缺陷就是网络地址资源有限，从理论上讲，IPv4 技术可使用的 IP 地址有 43 亿个，基本上能够满足全世界互联网用户的需要。但是，由于 IPv4 技术的核心技术属于美国，所以存在着网络地址分配不均的问题。据统计，北美就占有 3/4，约 30 亿个，而人口最多的亚洲只有不到 4 亿个，中国只有 3 千多万个。IP 地址不足，严重地制约了我国及其他国家互联网的应用和发展。

[0003] 现在，中国互联网用户已经超过 2 亿，由于 IP 地址资源不足，需要许多用户共享一个 IP 地址。基于这种情况，当前我国的互联网主机普遍存在匿名性问题，即主机身份无法得到有效验证，用户行为无法得到审计。互联网主机的匿名性虽然促使了用户的广泛参与和信息的自由交流，但同时也导致了用户行为的随意性，引起一些负面影响甚至给社会造成危害。例如，2006 年，一些不法分子就利用互联网主机的匿名性进行网络欺骗和身份窃取，给消费者和商家带来的经济损失高达数十亿美元。此外，垃圾邮件等其它制约互联网发展的问题也同隐藏身份有关。

[0004] 这是因为由于多个用户主机共用一个 IP 地址或使用私有地址，溯源困难，导致地址假冒、垃圾信息泛滥、大量的入侵和攻击行为无法跟踪等问题，网络安全得不到保障，制约了互联网的发展。匿名已经成为了打造互联网安全的一大阻碍。

[0005] 总之，需要本领域技术人员迫切解决的一个技术问题就是：如何能够实现对互联网主机的实名制认证，提高互联网的安全性。

发明内容

[0006] 本发明所要解决的技术问题是提供一种互联网主机命名方法，能够实现互连网主机的实名制认证，解决了地址假冒信息、垃圾信息的溯源问题、大量的入侵和攻击行为的跟踪等问题，有效提高了互联网的安全性。

[0007] 为了解决上述问题，本发明公开了一种互联网主机命名方法，采用 IPv6 地址作为互联网主机的实名地址，该方法包括：

[0008] 依据互联网主机的地址申请，生成一个标记符；

[0009] 分配 IPv6 地址，将分配给该主机的 IPv6 地址，连同所述标记符发送给该主机和密钥数据库；

[0010] 生成加密密钥，将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；

[0011] 将由相同标记符标记的所述 IPv6 地址和加密密钥作为一组 IPv6 地址 / 加密密钥对进行存储。

[0012] 优选的，所述接收地址申请、分配 IPv6 地址和生成加密密钥分别由三个独立的服务器完成。

[0013] 优选的，每个所述 IPv6 地址对应一个所述加密密钥，所述加密密钥为一个 128 位的随机数。

[0014] 本发明还提供了一种基于实名地址的互联网主机通信方法，采用 IPv6 地址作为互联网主机的实名地址，该方法包括：

[0015] 依据互联网主机的地址申请，生成一个标记符；

[0016] 分配 IPv6 地址，将分配给该主机的 IPv6 地址，连同所述标记符发送给该主机和密钥数据库；

[0017] 生成加密密钥，将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；

[0018] 将由相同标记符标记的所述 IPv6 地址和加密密钥作为一组 IPv6 地址 / 加密密钥对进行存储；

[0019] 互联网主机依据所接收的所述 IPv6 地址 / 加密密钥对，生成公 / 私密钥对；

[0020] 互联网主机利用所述公 / 私密钥对与其他互联网主机或服务器进行通信。

[0021] 优选的，每个所述 IPv6 地址对应一个所述加密密钥，所述加密密钥为一个 128 位的随机数，所述加密密钥中包括安全参数。

[0022] 优选的，所述生成公 / 私密钥对的方法包括：

[0023] 将分配 IPv6 地址 64 位的子网前缀与 64 位的全为零的场点本地地址串连，构成 128 位的明文；

[0024] 将所述明文加密为密文；

[0025] 对所述密文执行安全散列算法，将所得结果进行划分，得到哈希值 1 和哈希值 2；

[0026] 判断所述哈希值 1 的预定位数据与所述安全参数乘积后得到的 (m×h) 位数值与零的比较，如果它们都为零或所述安全参数为零，则执行下一步；如果不为零，则密文加 1，整型变量加 1 后，返回执行上一步；其中，m 为所述预定位数值的位数，h 为所述安全参数的安全级别；

[0027] 对所述哈希值 2 与整形变量串连后的数值执行所述安全散列算法，结果记为哈希值 3，将所述哈希值 3 作为私钥；

[0028] 依据所述私钥，由预置的公钥密码算法生成对应的公钥。

[0029] 优选的，所述对密文执行安全散列算法后得到一串 160 位元的数值，最左边的 112 位记为所述哈希值 1，最右边 48 位记为所述哈希值 2；

[0030] 所述哈希值 1 的预定位数据为所述哈希值 1 的最左边 16 位数据。

[0031] 相应的，本发明还提供了一种互联网主机命名系统，包括：

[0032] IPv6 地址 / 密钥服务器，用于处理互联网主机的地址申请、发送标记符标记的地址分配命令给 IPv6 地址服务器和所述标记符标记的加密密钥生成命令给加密密钥生成器；

[0033] IPv6 地址服务器，用于分配 IPv6 地址作为所述互联网主机的实名地址，发送所述标记符标记的所述 IPv6 地址给所述互联网主机和密钥数据库；

[0034] 加密密钥生成器，用于生成加密密钥，发送所述标记符标记的所述加密密钥给主

机和密钥数据库；

[0035] 密钥数据库，用于存储相同标记符标记的 IPv6 地址 / 加密密钥对。

[0036] 优选的，每个所述 IPv6 地址对应一个所述加密密钥，所述加密密钥为一个 128 位的随机数。

[0037] 优选的，所述 IPv6 地址 / 密钥服务器，包括：

[0038] 申请接收模块，用于接收所述互联网主机的地址申请；

[0039] 标记符生成模块，用于生成一个标记符；

[0040] 地址分配命令发送模块，用于向所述 IPv6 地址服务器发出一个由所述标记符标记的地址分配命令；

[0041] 加密密钥命令发送模块，用于向所述加密密钥生成器发出一个由所述标记符标记的加密密钥生成命令。

[0042] 最后，本发明还提供了一种基于实名地址的互联网通信系统，包括互联网主机命名系统和互联网主机，其中，所述互联网主机命名系统，包括：

[0043] IPv6 地址 / 密钥服务器，用于处理互联网主机的地址申请、发送标记符标记的地址分配命令给 IPv6 地址服务器和所述标记符标记的加密密钥生成命令给加密密钥生成器；

[0044] IPv6 地址服务器，用于分配 IPv6 地址作为所述互联网主机的实名地址，发送所述标记符标记的所述 IPv6 地址给主机和密钥数据库；

[0045] 加密密钥生成器，用于生成加密密钥，发送所述标记符标记的所述加密密钥给主机和密钥数据库；

[0046] 密钥数据库，用于存储相同标记符标记的 IPv6 地址 / 加密密钥对；

[0047] 所述互联网主机包括：

[0048] 公 / 私密钥对生成模块，根据所接收的相同标记符标记的 IPv6 地址 / 加密密钥对，生成公 / 私密钥对；

[0049] 通信模块，用于与其他互联网主机或服务器通过所述生成的公 / 私密钥对进行通信。

[0050] 优选的，所述公 / 私密钥对生成模块包括：

[0051] 明文生成单元，用于将分配 IPv6 地址 64 位的子网前缀与 64 位的全为零的场点本地地址串连，构成 128 位的明文；

[0052] 密文生成单元，用于利用加密算法将所述明文加密为密文；

[0053] 哈希值划分单元，用于对所述密文执行安全散列算法，将所得结果划分为哈希值 1 和哈希值 2；

[0054] 判断单元，判断哈希值 1 的预定位数据与所述安全参数乘积后得到的 (m×h) 位数值与零的比较结果，其中，m 为所述预定位数据的位数，h 为所述安全参数的安全级别；

[0055] 私钥生成单元，对所述哈希值 2 与整形变量串连后的数值执行所述安全散列算法，结果记为哈希值 3，将所述哈希值 3 作为私钥；

[0056] 公钥生成单元，依据所述私钥由预置的公钥密码算法生成对应的公钥。

[0057] 优选的，所述对密文执行安全散列算法后得到一串 160 位元的数值，最左边的 112 位记为所述哈希值 1，最右边 48 位记为所述哈希值 2；所述哈希值 1 的预定位数据的位数 m

为所述哈希值 1 的最左边 16 位。

[0058] 与现有技术相比，本发明具有以下优点：

[0059] 针对现有技术中多个互联网主机共用一个 IP 地址或使用私有地址进行通信，信息溯源比较困难的情况，本发明基于 IPv6 丰富的地址资源，提供了一种互联网主机命名和通信方法及系统。本发明中，采用一部分 IPv6 地址仅用作互联网主机的身份标识，不用作路由和寻址，这样互联网主机用户的行为，特别是在网上发布垃圾信息或有害消息以及进行对其他用户主机或服务器进行入侵和攻击的行为就能够得到审计，并进行相应的处理措施。可以有效治理互联网上垃圾信息、有害信息发布，入侵和攻击其他主机或服务器的行为，有效提高了互联网的安全性。

附图说明

[0060] 图 1 是本发明互联网主机命名方法实施例的流程图；

[0061] 图 2 是本发明互联网主机命名系统的结构示意图；

[0062] 图 3 是本发明 IPv6 地址 / 密钥服务器的结构示意图；

[0063] 图 4 是本发明互联网通信系统的结构示意图；

[0064] 图 5 是本发明公 / 私密钥对生成模块的结构示意图；

[0065] 图 6 是本发明互联网主机通信方法的流程图；

[0066] 图 7 是本发明生成公 / 私密钥对的方法流程图。

具体实施方式

[0067] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0068] 本发明的核心构思之一是利用下一代网络 IPv6 丰富的地址资源，将一部分 IPv6 地址作为互联网主机的身份标识，在通信过程中，这部分 IPv6 地址只用于标识主机的身份，不用于路由和通信，实现互联网主机的实名制。

[0069] 本发明提供了一种互联网主机命名方法，采用 IPv6 地址作为互联网主机的实名地址。参照图 1，示出了本发明互联网主机命名方法实施例的流程图，该方法包括以下步骤：

[0070] 步骤 101，依据互联网主机的地址申请，生成一个标记符；

[0071] 步骤 102，分配 IPv6 地址，将分配给该主机的 IPv6 地址，连同所述标记符发送给该主机和密钥数据库；

[0072] 步骤 103，生成加密密钥，将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；

[0073] 步骤 104，将由相同标记符标记的所述 IPv6 地址和加密密钥作为一个 IPv6 地址 / 加密密钥对进行存储。

[0074] 在本发明实施例中，优先的是，所述接收地址申请步骤 101、分配 IPv6 地址步骤 102 和生成加密密钥步骤 103 分别由三个独立的服务器完成，上述三个服务器的任何一方都无法知道 IPv6 地址 / 加密密钥对，有效提高了加密密钥的安全性。

[0075] 在本发明的另一实施例中，优先的实施方式是每个所述 IPv6 地址对应一个加密

密钥。每个所述加密密钥为一个 128 位的随机数。

[0076] 对应于上述互联网主机命名方法，本发明还提供了一种互联网主机命名系统。图 2 示出了本发明一种互联网主机命名系统的结构示意图，包括：

[0077] IPv6 地址 / 密钥服务器 211，用于处理互联网主机的地址申请、发送标记符标记的地址分配命令给 IPv6 地址服务器 212 和所述标记符标记的加密密钥生成命令给加密密钥生成器 213；

[0078] IPv6 地址服务器 212，用于分配 IPv6 地址作为所述互联网主机的实名地址，发送所述标记符标记的所述 IPv6 地址给所述互联网主机和密钥数据库 214；

[0079] 加密密钥生成器 213，用于生成加密密钥，发送所述标记符标记的所述加密密钥给主机和密钥数据库 214；

[0080] 密钥数据库 214，用于存储相同标记符标记的 IPv6 地址 / 加密密钥对。在本发明一种互联网主机命名系统的实施例中，所述 IPv6 地址服务器

[0081] 212 为每一个互联网主机生成的 IPv6 地址的同时，会生成一个与所述 IPv6 地址对应的加密密钥，所述加密密钥为一个 128 位的随机数。

[0082] 图 3 示出了本发明 IPv6 地址 / 密钥服务器的结构示意图，在本发明一种互联网主机命名系统的另一实施例中，所述 IPv6 地址 / 密钥服务器 211 还可以具体包括：

[0083] 申请接收模块 301，用于接收互联网主机的地址申请；

[0084] 标记符生成模块 302，用于为上述地址申请生成一个标记符；

[0085] 地址分配命令发送模块 303，用于向所述 IPv6 地址服务器 212 发出一个由所述标记符标记的地址分配命令；

[0086] 加密密钥命令发送模块 304，用于向所述加密密钥生成器 213 发出一个由所述标记符标记的加密密钥生成命令。

[0087] 下面结合上述图 1、图 2 和图 3 所示的内容，详细描述所述互联网主机命名系统 21 的工作过程，具体为：互联网主机 22 向所述互联网主机命名系统 21 发送地址申请；IPv6 地址 / 密钥服务器 211 的子单元申请接收模块 301 接收到所述地址申请后，发送信号给标记符生成模块 302；所述标记符生成模块 302 接到上述信号后为该地址申请产生一个标记符；然后，地址分配命令发送模块 303 向所述 IPv6 地址服务器 212 发送由所述标记符标记的地址分配命令；同时，加密密钥命令发送模块 304 向加密密钥生成器 213 发送由所述标记符标记的加密密钥生成命令；IPv6 地址服务器 212 接收到所述地址分配命令后，分配一个 IPv6 地址，并用接收到的标记符将所述 IPv6 地址标记后发送给密钥数据库 214，也将同样的信息即所述标记符标记后的 IPv6 地址发送给互联网主机 22；加密密钥生成器 213 接收到加密密钥生成命令后，产生一个 128 位的随机数作为加密密钥，并用接收到的标记符将所述加密密钥标记后发送给密钥数据库 214，同时也将同样的信息即所述标记符标记后的加密密钥发送给互联网主机 22；密钥数据库 214 把采用相同标记符标记的 IPv6 地址和加密密钥作为一组 IPv6 地址 / 加密密钥对存储起来。这样除了密钥数据库外，所述 IPv6 地址 / 密钥服务器 211、IPv6 地址服务器 212 和加密密钥生成器 213 中的任何一方都无法得知 IPv6 地址 / 加密密钥对，增强了系统的安全性。这是因为所述加密密钥中有一个决定安全级别的安全参数，所述安全参数存在于上述 128 位加密密钥的最左边 3 位，是一个 3 位的无符号整数。所述安全参数是 000、001、010、011、111 等，安全参数 000 对应的安全级别为

0 级，安全参数 001 对应的安全级别为 1 级，以此类推，安全参数 111 对应的安全级别最高为 7 级。安全参数可以使互联网主机增加生成私钥的代价，因而可以增加对私钥的强力攻击的代价。这是因为，所述安全参数存在于加密密钥中，攻击者既无法得知也无法改变，攻击者可能采用典型的低级安全级别到高安全级别的强攻击。在本发明中，所述安全参数每增加 1，就会给攻击者破解的哈希值长度增加了 16 位，对于最高安全级别 7 级的情况，那么攻击者就需要破解 142 位的哈希值。所以采用本发明提供的互联网主机命名方法和命名系统，有效增强了互联网主机高安全级别的安全性。

[0088] 基于上述互联网主机命名系统，本发明还提供了一种基于 IPv6 时实名地址的互联网通信系统，参照图 4，示出了本发明互联网通信系统的结构示意图，包括：互联网主机命名系统 21 和互联网主机 22。其中，所述互联网主机命名系统 21 的结构和具体实施方式已经结合图 2 在上述实施例和实施方式中进行了详细描述，这里就不再重复。接下来描述互联网通信系统中的互联网主机 22，所述互联网主机 22 包括：

[0089] 公 / 私密钥对生成模块 221，利用从所述互联网主机命名系统 21 接收到的具有相同标记符标记的 IPv6 地址 / 加密密钥对，生成公 / 私密钥对；

[0090] 通信模块 222，用于与其他互联网主机或服务器通过所述生成的公 / 私密钥对进行通信。

[0091] 本发明互联网通信系统实施例的工作过程为：互联网主机向互联网命名系统 21 发送地址申请；所述互联网命名系统 21 收到命令后生成 IPv6 地址 / 加密密钥对，并将上述 IPv6 地址 / 加密密钥对发送给互联网主机 22 的公 / 私密钥对生成模块 221；公 / 私密钥对生成模块 221 生成公 / 私密钥对，并将上述公 / 私钥对发送通信模块 222；通信模块 222 与其他互联网主机或服务器进行通信的信息利用所述公 / 私密钥对加密，然后进行互联网通信。

[0092] 参照图 5，示出了本发明公 / 私密钥对生成模块的结构示意图。在本发明互联网通信系统的另外一实施例中，优选的是，公 / 私密钥对生成模块包括：

[0093] 明文生成单元 501，用于将分配 IPv6 地址 64 位的子网前缀与 64 位的全为零的场点本地地址串连，构成 128 位的明文；

[0094] 密文生成单元 502，用于利用加密算法将所述明文加密为密文；

[0095] 哈希值划分单元 503，用于对所述密文执行安全散列算法 (SHA 算法，Secure Hash Algorithm)，将所得结果划分为哈希值 1 和哈希值 2；

[0096] 判断单元 504，判断哈希值 1 的预定位数与所述安全参数乘积后得到的 (m×h) 位数值与零的比较结果，其中，m 为所述预定位数值的位数，h 为所述安全参数的安全级别；

[0097] 私钥生成单元 505，对所述哈希值 2 与整形变量 MV 串连后的数值执行所述安全散列算法，结果记为哈希值 3，将所述哈希值 3 作为私钥；

[0098] 公钥生成单元 506，依据所述私钥由预置的公钥密码算法生成对应的公钥。

[0099] 在本发明互联网通信系统实施例中，优选的是，所述哈希值划分单元对所述密文单元生成的密文执行安全散列算法如 SHA-1 后，得到一串 160 位元的数值，将最左边的 112 位记为所述哈希值 1 即 Hash1，最右边 48 位记为所述哈希值 2 即 Hash2；所述哈希值 1 的预定位数 m 为所述 Hash1 的最左边 16 位。

[0100] 相应地，本发明还提供了一种采用 IPv6 地址作为实名地址的互联网主机通信方

法。参照图 6，示出了本发明互联网主机通信方法的流程图，该方法包括：

[0101] 步骤 601，依据互联网主机的地址申请，生成一个标记符；

[0102] 步骤 602，分配 IPv6 地址，将分配给该主机的 IPv6 地址，连同所述标记符发送给该主机和密钥数据库；

[0103] 步骤 603，生成加密密钥，将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；

[0104] 步骤 604，将由相同标记符标记的所述 IPv6 地址和加密密钥作为一组 IPv6 地址 / 加密密钥对进行存储；

[0105] 步骤 605，互联网主机依据所接收的所述 IPv6 地址 / 加密密钥对，生成公 / 私密钥对；

[0106] 步骤 606，互联网主机利用所述公 / 私密钥对与其他互联网主机或服务器进行通信。

[0107] 作为本发明互联网主机通信方法的一种优选实施例，每个所述 IPv6 地址对应一个所述加密密钥，所述加密密钥为一个 128 位的随机数，所述加密密钥中包括安全参数。

[0108] 在本发明互联网主机通信方法的另一种实施例中，生成公 / 私密钥对的优选实施方式参照图 7，示出了本发明生成公 / 私密钥对的方法流程图，所述生成公 / 私密钥对的方法包括：

[0109] 步骤 701，将分配 IPv6 地址 64 位的子网前缀与 64 位的全为零的场点本地地址串连，构成 128 位的明文；

[0110] 步骤 702，将所述明文加密为密文；

[0111] 步骤 703，对所述密文执行安全散列算法，将所得结果进行划分，得到哈希值 1 和哈希值 2；

[0112] 步骤 704，判断所述哈希值 1 的预定位数据与所述安全参数乘积后得到的 (m×h) 位数值与零的比较，如果它们都为零或所述安全参数为零，则执行步骤 706；否则执行步骤 705 后返回执行步骤 703，其中，m 为所述预定位数值的位数，h 为所述安全参数的安全级别；

[0113] 步骤 705，密文加 1，整型变量 MV 加 1；

[0114] 步骤 706，对所述哈希值 2 与整形变量 MV 串连后的数值执行所述安全散列算法，结果记为哈希值 3，将所述哈希值 3 作为私钥；

[0115] 步骤 707，依据所述私钥由预置的公钥密码算法生成对应的公钥。

[0116] 在本发明互联网主机通信方法的实施例中，优选的是，在生成公 / 私密钥对的方法中，步骤 703 对密文执行安全散列算法如 SHA-1 后得到一串 160 位元的数值，将最左边的 112 位记为所述哈希值 1，最右边 48 位记为所述哈希值 2；所述哈希值 1 的预定位数据为所述哈希值 1 的最左边 16 位数据。

[0117] 作为一种本发明互联网主机通信方法和通信系统的具体实施过程，包括以下步骤：

[0118] 互联网主机从互联网命名系统接收到相同标记符标记的 IPv6 地址 / 加密密钥对；

[0119] 所述互联网主机的明文生成单元，将分配的所述 IPv6 地址的前 64 位子网前缀与

64 位全为零的场点本地地址串联，构成 128 位的明文并发送给密文生成单元；

[0120] 所述密文生成单元利用加密算法如：高级加密标准 (AVS，AdvancedEncryption Standard) 算法将所述明文加密为密文，并将所述密文发送给哈希值划分单元；

[0121] 哈希值划分单元对接收到的上述密文执行安全散列算法如 SHA-1，得到一组 160 位元的数值，将所述数值的最左边 112 位记为哈希值 1 即 Hash1，最右边 48 位记为哈希值 2 即 Hash2；

[0122] 判断单元将所述 Hash1 的最左边 16 位数据与安全参数相乘后得到的 (m×h) 位数值与零比较；

[0123] 其中，所述安全参数是一个 3 位的无符号整数，存在于所述加密密钥的最左边 3 位，决定了安全级别 h。所述安全参数对应的安全级别 h 的取值为 0-7。安全参数为 000 时，对应的安全级别 h 为 0；安全参数为 001 时，其安全级别 h 为 1；当安全参数为 111 时，安全级别 h 为最高级别 7。作为一种具体实施例，当安全级别为 1 时，所述 Hash1 的最左边 16 位数据与安全参数 001 相乘后，得到 (16×1) 位数值，然后与零比较；

[0124] 如果所述 16 位数值不全为零，则执行步骤 705，即将上述密文加 1 得到新的密文，整形变量 MV 加 1 后，返回上一步，即哈希值划分单元对所述新密文执行安全散列算法如 SHA-1，得到一个新的 160 位元的数值，将所述数值的最左边 112 位记为新的 Hash1，最右边 48 位记为新的 Hash2，然后执行判断步骤，直至判断结果为零；每返回一次，所述密文就加 1，整形变量 MV 也加 1。其中，所述整形变量 MV 实际用于记录 Hash 次数，其初始值为 0。

[0125] 如果所述 16 位数值全为零，则由私钥生成单元将所述 Hash2 与对应的整形变量 MV 串联，然后对所述串联后的数值执行所述安全散列算法如 SHA-1，将得到的结果记为 Hash3，作为私钥；

[0126] 最后公钥生成单元依据所述私钥根据预置的公钥密码算法如 RSA(Rivest Shamir Adlemen)、背包密码、McEliece 密码、Diffe Hellman、Rabin、Ong Fiat Shamir、零知识证明的算法、椭圆曲线、EIGamal 算法等生成对应的公钥。

[0127] 至此，互联网主机的公 / 私钥对生成完毕，可以用于与其他互联网主机或服务器的通信。在整个过程中，用户为了生成符合安全参数的私钥，需要维护所述整形变量 MV，其初始值为 0。

[0128] 实名地址的使用方法为：互联网主机在上网时，应该向域名服务器注册主机上网 IP 地址和 IPv6 格式实名地址的绑定关系，以及所用到的公钥，如果是网站有域名的，也应注册该域名。移动主机变更上网 IP 地址时也要更新所述新的上网 IP 地址和 IPv6 格式实名地址的绑定关系。其中，上述 IPv6 格式实名地址是由本发明互联网主机命名系统分配给主机的。每台互联网主机的 IPv6 格式实名地址是唯一确定的。通信双方在进行实名通信时，需要先根据对方的 IPv6 格式实名地址查询通信对方的 IP 地址和通信公钥，不能直接进行基于上网 IP 地址的网络通信。具体通信过程为：通信方双方的一方 (以下简称 A) 向另一方 (以下简称 B) 发送通信包；对方 B 回复信息包含回复方的问题，DH(Diffie-Hellman) 密钥交换算法的 DH 半会话密钥和签名；通信方 A 给出问题解决方案，计算得出会话密钥，创建安全关联 (SA，SecurityAssociation)，并发送 DH 算法的半会话密钥，A 的签名；通信方 B 计算得出会话密钥，创建自己的安全关联 SA，并发送签名包结束实名地址认证；通信双方在进行身份认证后，确认对方拥有公钥对应的私钥，用会话密钥进行信息交互。

[0129] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于系统实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0130] 以上对本发明所提供的一种互联网主机命名和通信方法及系统，进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

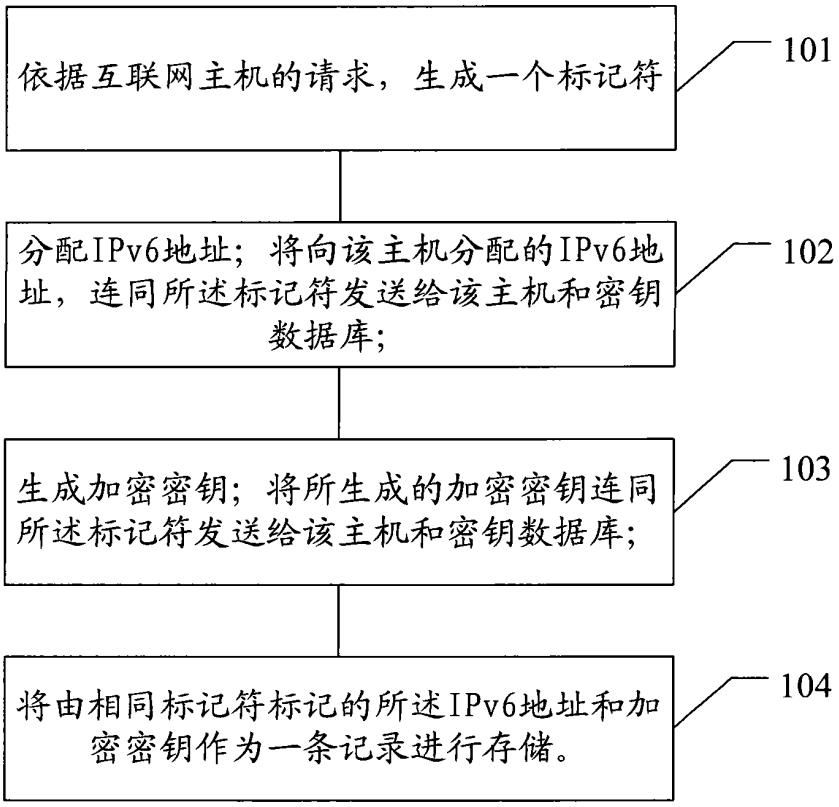

依据互联网主机的请求，生成一个标记符
101
分配IPv6地址；将向该主机分配的IPv6地址，连同所述标记符发送给该主机和密钥数据库；
102
生成加密密钥；将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；
103
将由相同标记符标记的所述IPv6地址和加密密钥作为一条记录进行存储。
104

图 1

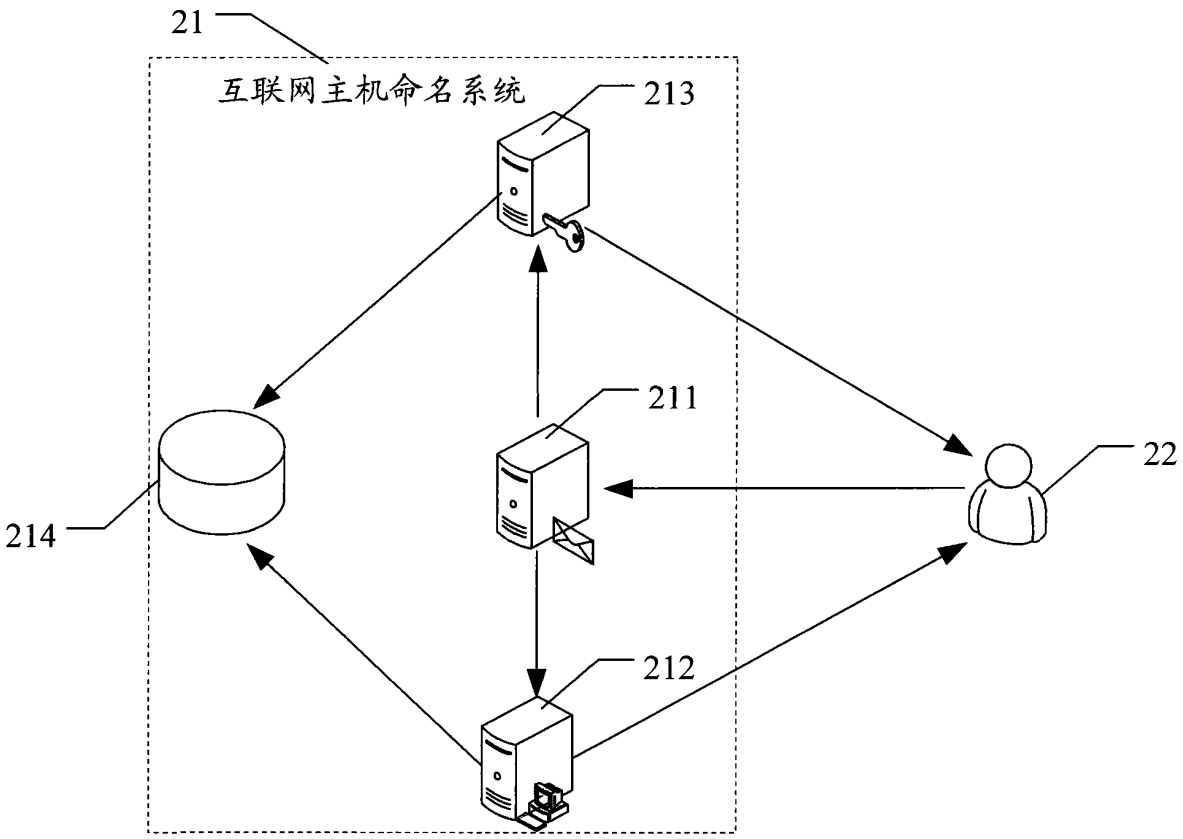

21
互联网主机命名系统
213
211
22
214
212

图 2

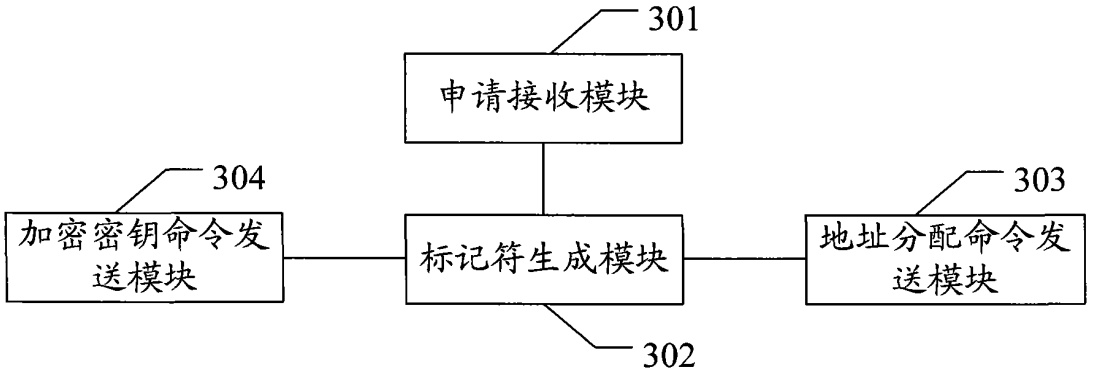

301
申请接收模块
304
303
加密密钥命令发送模块
标记符生成模块
地址分配命令发送模块
302

图 3

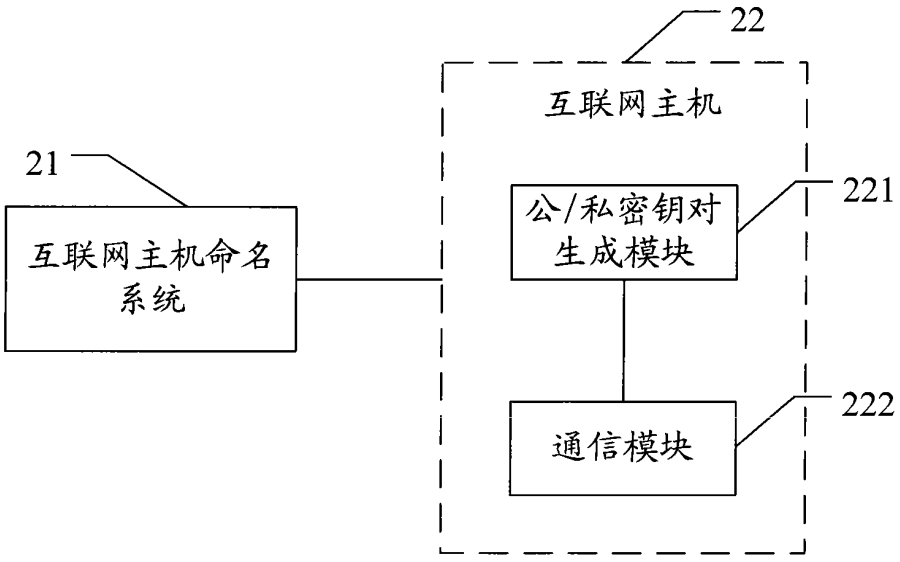

22
互联网主机
21
互联网主机命名系统
公/私密钥对生成模块
221
通信模块
222

图 4

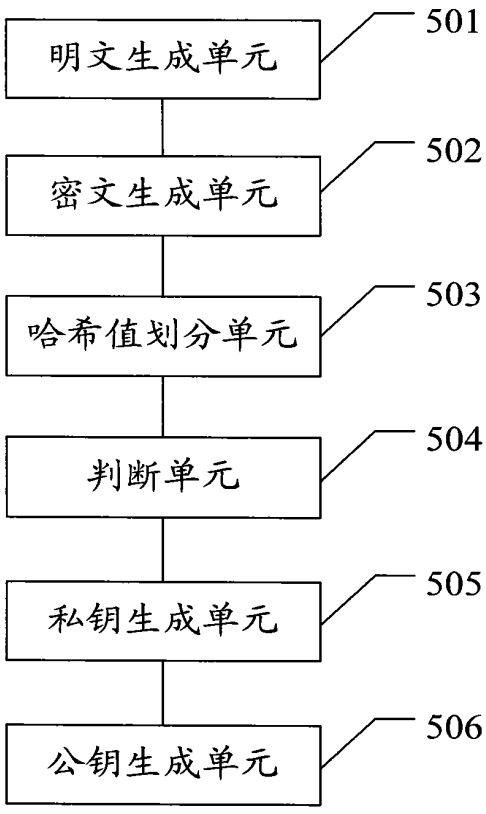

明文生成单元
501
密文生成单元
502
哈希值划分单元
503
判断单元
504
私钥生成单元
505
公钥生成单元
506

图 5

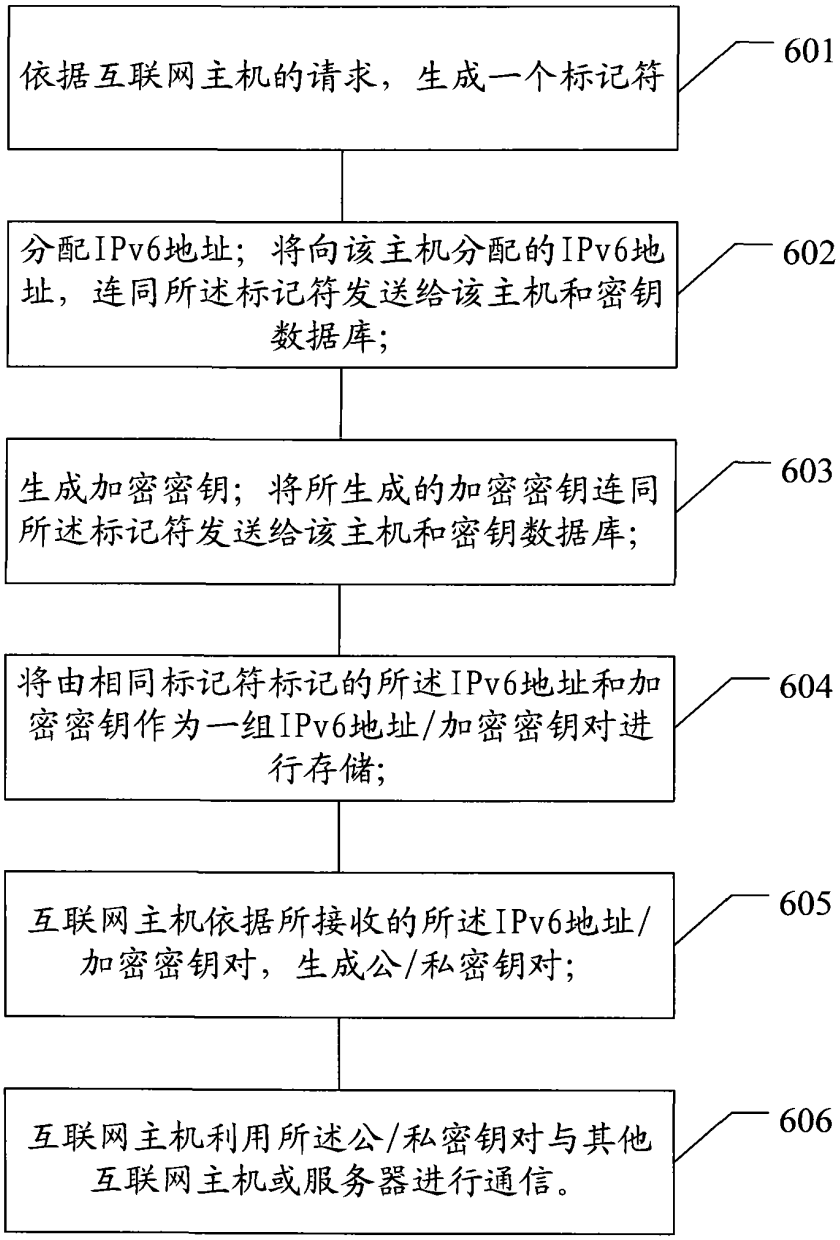

依据互联网主机的请求，生成一个标记符
601
分配IPv6地址；将向该主机分配的IPv6地址，连同所述标记符发送给该主机和密钥数据库；
602
生成加密密钥；将所生成的加密密钥连同所述标记符发送给该主机和密钥数据库；
603
将由相同标记符标记的所述IPv6地址和加密密钥作为一组IPv6地址/加密密钥对进行存储；
604
互联网主机依据所接收的所述IPv6地址/加密密钥对，生成公/私密钥对；
605
互联网主机利用所述公/私密钥对与其他互联网主机或服务器进行通信。
606

图 6

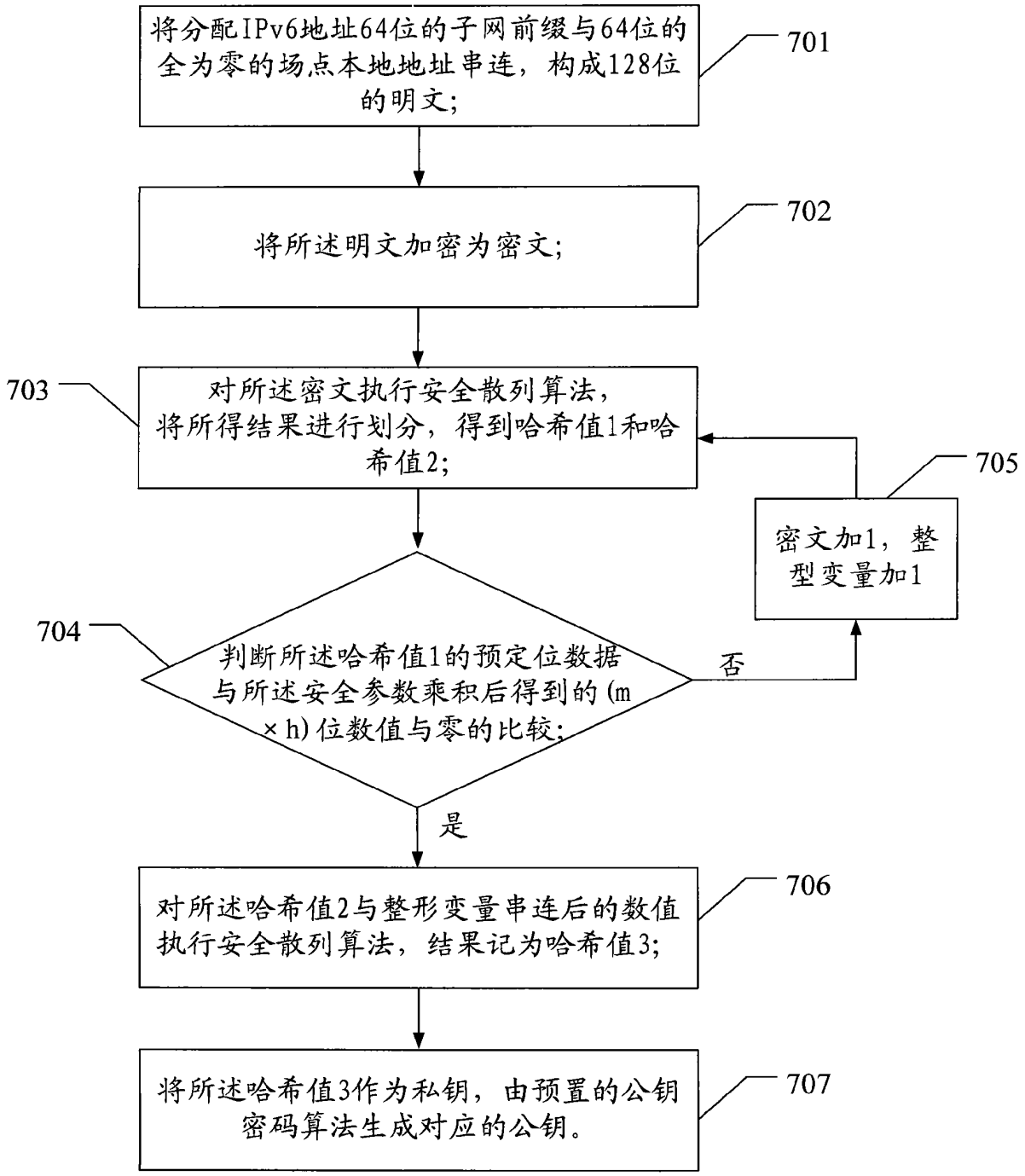

将分配IPv6地址64位的子网前缀与64位的全为零的场点本地地址串连，构成128位的明文;
701
将所述明文加密为密文;
702
对所述密文执行安全散列算法，将所得结果进行划分，得到哈希值1和哈希值2;
703
判断所述哈希值1的预定位数据与所述安全参数乘积后得到的(m×h)位数值与零的比较;
704
否
密文加1，整型变量加1
705
是
对所述哈希值2与整形变量串连后的数值执行安全散列算法，结果记为哈希值3;
706
将所述哈希值3作为私钥，由预置的公钥密码算法生成对应的公钥。
707

图 7