(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 102714625 A
(43)申请公布日 2012.10.03

(21)申请号 201080062598.7
(22)申请日 2010.10.22
(30)优先权数据
61/299,493 2010.01.29 US
(85)PCT申请进入国家阶段日
2012.07.27
(86)PCT申请的申请数据
PCT/EP2010/066003 2010.10.22
(87)PCT申请的公布数据
WO2011/091871 EN 2011.08.04
(71)申请人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩
(72)发明人 M. 萨雷拉 M. 纳斯伦 P. 尼坎德
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杨美灵 朱海煜
(51)Int.Cl.
H04L 12/56(2006.01)
H04L 29/06(2006.01)

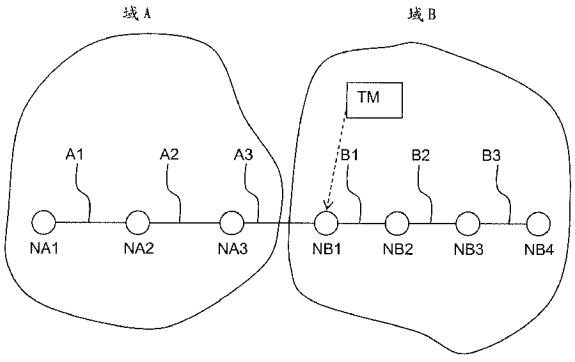
权利要求书 2 页 说明书 12 页 附图 9 页

(54)发明名称

在网络中通过修改分组中布隆过滤器的分组路由选择

(57)摘要

位于域内的网络节点(NB1)适用于从另一节点接收分组,该分组具有编码有关域内路由的信息的分组中布隆过滤器或布隆过滤器等效。节点以相对于用于添加链路到布隆过滤器或布隆过滤器等效的操作是线性的方式可反向地修改分组中布隆过滤器或布隆过滤器等效。随后,节点将其报头包含修改的布隆过滤器或布隆过滤器的分组转发到另一节点(NA1)。本发明允许在域(域B)中安全的基于布隆过滤器的路由选择,同时要求仅在域边界的路由器(NB1)是安全路由器。域中的其它路由器(NB2,NB3,NB4)可按常规操作,并且可以是安全路由器或不安全路由器。修改可以是比特置换。



CN 102714625 A

1. 一种网络节点，所述网络节点位于域内并适用于：

从另一节点接收分组，所述分组具有编码有关所述域内路由的信息的分组中布隆过滤器或布隆过滤器等效；

可反向地修改所述分组中布隆过滤器或布隆过滤器等效；以及

将其报头包含所修改的布隆过滤器或布隆过滤器的分组转发到另一节点；

其中所述节点适用于以相对于用于添加链路到所述布隆过滤器或布隆过滤器等效的操作是线性的方式可反向地修改所述分组中布隆过滤器或布隆过滤器等效。

2. 如权利要求 1 中要求保护的节点，其中将所述分组转发到另一节点包括将所述分组转发到另一域中的另一节点。

3. 如权利要求 1 中要求保护的节点，其中将所述分组转发到另一节点包括将所述分组转发到所述域中的另一节点。

4. 一种网络节点，所述网络节点与域相关联并适用于：

生成编码有关网络的域内路由的信息的布隆过滤器或布隆过滤器等效；

可反向地修改所述布隆过滤器或布隆过滤器等效；以及

将所修改的布隆过滤器或布隆过滤器转发到另一节点以便包括在要从所述另一节点发送的分组的报头中；

其中所述节点适用于以相对于用于添加链路到所述布隆过滤器或布隆过滤器等效的操作是线性的方式可反向地修改所述布隆过滤器或布隆过滤器等效。

5. 如任何前面权利要求中要求保护的节点，并且适用于修改所述布隆过滤器或布隆过滤器等效以便不大量增大所述布隆过滤器或布隆过滤器等效中“1”的数量。

6. 如任何前面权利要求中要求保护的节点，并且适用于通过应用比特置换到所述布隆过滤器或布隆过滤器等效来修改所述布隆过滤器或布隆过滤器等效。

7. 如权利要求 6 中要求保护的节点，并且适用于通过应用随机或伪随机比特置换到所述布隆过滤器或布隆过滤器等效来修改所述布隆过滤器或布隆过滤器等效。

8. 如权利要求 6 或 7 中要求保护的节点，并且适用于通过应用取决于至少密钥和会话标识符之一的比特置换来修改所述布隆过滤器或布隆过滤器等效。

9. 如权利要求 1 到 8 中任一项中要求保护的节点，并且适用于还通过加密所述布隆过滤器或布隆过滤器等效来修改所述布隆过滤器或布隆过滤器等效。

10. 如权利要求 9 中要求保护的节点，并且适用于在加密所述布隆过滤器或布隆过滤器等效前级联所述布隆过滤器或布隆过滤器和 t 个预指定的比特（其中，t 是正整数）。

11. 一种网络节点，所述网络节点位于域内并适用于：

从另一节点接收具有包含分组中布隆过滤器或布隆过滤器等效的分组报头的分组，所述分组中布隆过滤器或布隆过滤器等效包含路由选择信息，已应用修改到所述分组中布隆过滤器或布隆过滤器等效，所述修改相对于用于添加链路到所述布隆过滤器或布隆过滤器等效的操作是线性的，所述路由选择信息表示所述域内的路由；以及

从所述布隆过滤器或布隆过滤器等效恢复所述路由选择信息。

12. 如权利要求 11 中要求保护的网络节点，并且适用于根据所恢复的路由选择信息来转发所述分组。

13. 如权利要求 11 或 12 中要求保护的网络节点，其中应用到所述布隆过滤器或布隆

过滤器等效的修改包括比特置换，以及其中所述网络节点适用于通过应用反向比特置换到所述布隆过滤器或布隆过滤器等效来恢复所述路由选择信息。

14. 如权利要求 11、12 或 13 中要求保护的网络节点，其中应用到所述布隆过滤器或布隆过滤器等效的修改还包括加密，以及其中所述网络节点适用于通过解密所述布隆过滤器或布隆过滤器等效来恢复所述路由选择信息。

15. 如权利要求 14 中要求保护的网络节点，并且适用于比较所解密的布隆过滤器或布隆过滤器等效的填充系数和预设阈值，以及如果所解密的布隆过滤器或布隆过滤器等效的填充系数超过所述预设阈值，则丢弃所述分组。

16. 一种路由选择分组的方法，包括：

在域中的节点接收分组，所述分组具有编码有关所述域内路由的信息的分组中布隆过滤器或布隆过滤器等效；

可反向地修改所述分组中布隆过滤器或布隆过滤器等效；以及

将其报头包含所修改的布隆过滤器或布隆过滤器的分组转发到另一节点；

其中修改所述分组中布隆过滤器或布隆过滤器等效包括以相对于用于添加链路到所述布隆过滤器或布隆过滤器等效的操作是线性的方式，修改所述分组中布隆过滤器或布隆过滤器等效。

17. 一种提供分组路由选择信息的方法，所述方法包括：

在节点生成编码有关网络的域内路由的信息的布隆过滤器或布隆过滤器等效；

可反向地修改所述布隆过滤器或布隆过滤器等效；以及

将所修改的布隆过滤器或布隆过滤器转发到另一节点以便包括在要从所述另一节点发送的分组的报头中；

其中修改所述分组中布隆过滤器或布隆过滤器等效包括以相对于用于添加链路到所述布隆过滤器或布隆过滤器等效的操作是线性的方式，修改所述布隆过滤器或布隆过滤器等效。

18. 一种提供分组路由选择信息的方法，所述方法包括：

在网络节点接收具有包含分组中布隆过滤器或布隆过滤器等效的分组报头的分组，所述分组中布隆过滤器或布隆过滤器等效包含路由选择信息，已应用修改到所述分组中布隆过滤器或布隆过滤器等效，所述修改相对于用于添加链路到所述布隆过滤器或布隆过滤器等效的操作是线性的，所述路由选择信息表示所述域内的路由；以及

从所述布隆过滤器或布隆过滤器等效恢复所述路由选择信息。

在网络中通过修改分组中布隆过滤器的分组路由选择

技术领域

[0001] 本发明涉及网络中的分组转发。具体地说，它涉及在分组报头中包含转发信息使得网络节点可根据分组报头中的转发信息来确定应沿哪个链路(哪些链路)转发分组的方法。

背景技术

[0002] 布隆过滤器(bloom filter)是熟知的空间高效数据结构，它应答集成员查询并带有某一概率的错误肯定(false positive)。在试图解决下一代网络面临的许多实现约束(例如，Gbps 速度、日益复杂的任务、更大的系统、高速存储器可用性等)中，在 PCT/EP 2008/061167 和 PCT/EP2008/063647 中已提议在分组报头中为不同目的(路由选择、安全性、责任性等)使用小型布隆过滤器。这些文档中陈述的主要思想是一种基于分组报头中的小型布隆过滤器和链路标识符的新颖、空间和计算高效的源路由选择和分组转发机制。PCT/EP 2008/061167 和 PCT/EP2008/063647 中表述的基本思想是赋予网络中的每个链路编码为比特字符串的一个名称(或“链路标识符标志”)，并且通过在包括的所有链路上计算按比特或，命名路径。此类布置确保分组通过指定路径(或树)转发。

[0003] 在此文档中，我们将在这些类型的应用中使用的位于分组报头中的布隆过滤器称为分组中布隆过滤器 (in-packet Bloom Filter，iBF)。从某种意义上来说，与例如 Broder 和 Mitzenmacher 在因特网数学(2002)卷 1 (4)485 — 509 页的布隆过滤器的网络应用 :调查 (Network Applications of Bloom Filters: A Survey. Internet Mathematics (2002) vol. 1 (4) pp. 485-509) 中的所著文献中先前所述的传统基于 BF 的方案相比，iBF 遵照反向方案。

[0004] 布隆过滤器的一个特征是它可给出“错误肯定”—即，在查询布隆过滤器以确定特殊链路是否是其名称被编码到布隆过滤器中的链路之一时，布隆过滤器查询可不正确地返回应答“是”。在基于布隆过滤器的路由选择中出现错误肯定时，结果是分组另外遍历一个或多个链路，这些链路未被编码在布隆过滤器中并且未预期沿其发送分组。一般情况下，为最小化错误肯定的概率，与链路名称中 1 的数量相比，布隆过滤器的长度需要是大的。

[0005] PCT/EP 2008/061167 和 PCT/EP2008/063647 中所述的基本方案使用静态链路标识符。PCT/EP 2009/062785 中描述了一种安全变体。这是基于“快速(on-the-fly)”计算链路标识符的思想，例如，基于分组中的信息和对每个路由器秘密的信息，例如，根据以下等式 :

$$O=F(K, I, C)$$

其中，K 是仅路由器和拓扑管理器知道的密钥，I 是从分组所取的对会话独特的信息(如发送方和目的地 IP 地址和端口号或公布标识符(publication identifier))，以及 C 是与处理有关的上下文特定信息，如用于输入和输出链路的本地标识符。根据 PCT/EP 2009/062785 的原理操作的路由器将在本文中称为“安全路由器”。

[0006] PCT/SE 2010/050001 还使得能够将 iBF 连系到每分组独特的数据。

[0007] 对于路径通过多个域的情况，尤其需要转发安全性。因此，为使 iBF 切实可在此类多域环境(例如，端对端或域间路径 / 树)中使用，转发必须是安全的。然而，基本 iBF 的安全性并不足够，并且为获得转发安全性，所有转发单元使用安全路由器会是必要的。这是因为构造 iBF 的方式—如果在路径上只有一个安全路由器，则攻击者会相对易于猜测需要如何修改 iBF，以便促使安全路由器错误地将它向路径转发。在此意义上，iBF 不在网络中的任何特殊点提供绝对安全性，并且转而采用纵深防御。每个安全跳给出一个概率安全性，并且具有多个安全跳使得发送不想要的业务变得极其困难。

[0008] 然而，提供和操作在 PCT/EP 2009/062785 中描述的类型的安全路由器比简单的“不安全”路由器更昂贵。此外，安全路由器(如果要有效)要求每会话或每分组处理。如果能够实现安全路由选择而无需每个路由器是安全路由器，则这会是优选的，因为这会降低成本，并且也会使得在现有网络中应用基于 iBF 的路由选择变得更容易。

[0009] 另外，例如出于安全性原因，一些网络使用要求滤除错误肯定。作为一个示例，如果运营商在其网络中使用基于 iBF 的路由选择，则它将不想为一个客户处理的业务在另一客户的网络中结束，因为这可能导致安全性破坏(security breach)(这已被标识为 MPLS 客户的主要安全顾虑)。然而，使用每会话或每分组 iBF 意味着每个流或每个分组具有分开的 iBF，这意味着过滤表的增长和错误肯定的风险增大(例如，参阅 Luyuan Fang 编辑的 MPLS 和 GMPLS 网络的安全性框架，因特网草案 draft-ietf-mpls-mpls-and-gmpls-security-framework-07.txt(Luyuan Fang, ed. Security Framework for MPLS and GMPLS Networks, Internet draft draft-ietf-mpls-mpls-and-gmpls-security-framework-07.txt))。

[0010] 基于 iBF 的路由选择中错误肯定造成的另外问题是“循环”和流重复的问题。在连续的路由选择节点的一系列错误肯定造成分组执行环路并返回到 iBF 指定的多播树中的边界路由器时“循环”发生。在此类情况下，分组返回到边界路由器时，其 iBF 将匹配与以前完全相同的链路—并且因此分组将不可避免地绕环路反复发送，直至它达到其跳计数限制 (TTL) 时它被丢弃。每一轮的循环造成分组的附加副本被转发到居于边界路由器的子树中的所有接收方，其可以是相当多的资源浪费。

发明内容

[0011] 本发明的第一方面提供位于域内的网络节点。节点适用于从另一节点接收分组，分组具有编码有关域内路由的信息的分组中布隆过滤器或布隆过滤器等效。节点以相对于用于添加链路到布隆过滤器或布隆过滤器等效的操作是线性的方式可反向地修改分组中布隆过滤器或布隆过滤器等效。随后，节点将其报头包含修改的布隆过滤器或布隆过滤器的分组转发到另一节点。

[0012] 节点可将分组转发到在另一域中的另一节点。这是节点是负责将分组从一个域转发到另一域的边界节点的情况(如，图 5 中的节点 NB1，其将分组从域 B 转发到域 A)。由于节点在转发分组到另一域前修改分组中布隆过滤器或布隆过滤器等效，因此，本发明使得在受信任网络核心内采用简单的不安全路由器变得可能，并且仅要求在域边界执行复杂的操作。在图 5 的示例中，例如，域 B 中的节点 NB2、NB3 和 NB4 可采用简单的非安全路由器。

[0013] 备选地，节点可将分组转发到在域中的另一节点。由于节点在转发分组前修改分组中布隆过滤器或布隆过滤器等效，因此，如果在连续转发节点的一系列误报将造成分组

执行环路，则在分组返回到该节点时，分组中包含的分组中布隆过滤器或布隆过滤器等效将与原始在该节点接收分组时分组中包含的分组中布隆过滤器或布隆过滤器等效不同。分组将因此不再绕环路转发。本发明因此在防止分组绕环路反复发送上是有效的。

[0014] 本发明的第二方面提供与域相关联并适用于生成布隆过滤器或布隆过滤器等效的网络节点，布隆过滤器或布隆过滤器等效编码有关网络的域内路由的信息。节点以相对于用于添加链路到布隆过滤器或布隆过滤器等效的操作是线性的方式可反向地修改布隆过滤器或布隆过滤器等效，并且将修改的布隆过滤器或布隆过滤器转发到另一节点以便包括在要从该另一节点发送的分组的报头中。本发明的第一方面在通过沿路由发送收集器分组而生成用于路由的分组中布隆过滤器或布隆过滤器的情况下是适当的。第二方面是对第一方面的补充，并且在由诸如拓扑管理器等至少部分知道网络路由选择信息和能力的节点生成用于路由的分组中布隆过滤器或布隆过滤器的情况下是适当的。

[0015] 第一或第二方面的节点可修改布隆过滤器或布隆过滤器等效以便不大量增大布隆过滤器或布隆过滤器等效中“1”的数量。

[0016] 第一或第二方面的节点可通过应用比特置换到布隆过滤器或布隆过滤器等效来修改布隆过滤器或布隆过滤器等效。

[0017] 第一或第二方面的节点可通过应用随机或伪随机比特置换到布隆过滤器或布隆过滤器等效来修改布隆过滤器或布隆过滤器等效。(“随机”置换意味着置换从关于 n 个比特的所有 n! 个置换的集中随机抽取置换，其中，n! 个置换的每个置换具有相同的概率。“伪随机”置换意味着以实际上与随机置换难以区分的方式抽取置换。)

第一或第二方面的节点可通过应用取决于至少时间相关密钥和会话标识符之一的比特置换来修改布隆过滤器或布隆过滤器等效。

[0018] 第一或第二方面的节点可还通过加密布隆过滤器或布隆过滤器等效来修改布隆过滤器或布隆过滤器等效。它可在加密布隆过滤器或布隆过滤器前级联布隆过滤器或布隆过滤器和 t 个预指定的比特(其中，t 是正整数)。

[0019] 本发明的第三方面提供一种网络节点，该网络节点位于域内并适用于从另一节点接收具有包含分组中布隆过滤器或布隆过滤器等效的分组报头的分组，分组中布隆过滤器或布隆过滤器等效包含表示域内的路由的路由选择信息，并且已应用相对于用于添加链路到布隆过滤器或布隆过滤器等效的操作是线性的修改。节点适用于从布隆过滤器或布隆过滤器等效恢复路由选择信息。例如，节点可应用反向修改到接收分组中包含的布隆过滤器或布隆过滤器等效，以便恢复路由选择信息。鉴于本发明的第一和第二方面涉及在发送分组前分组中布隆过滤器或布隆过滤器等效的修改，本发明的此方面涉及接收包含修改的分组中布隆过滤器或布隆过滤器等效的分组的节点。

[0020] 第三方面的节点可根据恢复的路由选择信息来转发分组。

[0021] 应用到布隆过滤器或布隆过滤器等效的修改可包括比特置换，并且网络节点可适用于通过应用反向比特置换到布隆过滤器或布隆过滤器等效来恢复路由选择信息。

[0022] 应用到布隆过滤器或布隆过滤器等效的修改可还包括加密，并且网络节点可适用于通过解密布隆过滤器或布隆过滤器等效来恢复路由选择信息。

[0023] 第三方面的节点可比较解密的布隆过滤器或布隆过滤器等效的填充系数和预设阈值，以及如果解密的布隆过滤器或布隆过滤器等效的填充系数超过预设阈值，则丢弃分

组。

[0024] 本发明的第四方面提供一种路由选择分组的方法，包括在域中的节点接收具有编码有关域内路由的信息的分组中布隆过滤器或布隆过滤器等效的分组，以及以相对于用于添加链路到布隆过滤器或布隆过滤器等效的操作是线性的方式可反向地修改分组中布隆过滤器或布隆过滤器等效。随后，该方法包括将其报头包含修改的布隆过滤器或布隆过滤器的分组转发到另一节点。

[0025] 本发明的第五方面提供一种提供分组路由选择信息的方法，该方法包括在节点生成编码有关网络的域内路由的信息的布隆过滤器或布隆过滤器等效，以及以相对于用于添加链路到布隆过滤器或布隆过滤器等效的操作是线性的方式可反向地修改布隆过滤器或布隆过滤器等效。该方法随后包括将修改的布隆过滤器或布隆过滤器转发到另一节点以便包括在要从该另一节点发送的分组的报头中。

[0026] 本发明的第六方面提供一种提供分组路由选择信息的方法，该方法包括在网络节点接收具有包含分组中布隆过滤器或布隆过滤器等效的分组报头的分组，分组中布隆过滤器或布隆过滤器等效包含路由选择信息，已应用修改到分组中布隆过滤器或布隆过滤器等效，修改相对于用于添加链路到布隆过滤器或布隆过滤器等效的操作是线性的，路由选择信息表示域内的路由。该方法随后包括从布隆过滤器或布隆过滤器等效恢复路由选择信息。

[0027] 第六方面的方法可还包括根据恢复的路由选择信息来转发分组。

附图说明

[0028] 将参照附图作为示例描述本发明的优选实施例，其中：

图 1 示出基于 iBF 的路由选择方法的基本原理；

图 2 示出链路标识符的动态计算；

图 3 示出比特字符串的置换；

图 4 示出比特字符串的反向置换；

图 5 示出根据本发明的一实施例；

图 6 是根据本发明的方法的方框流程图；

图 7 是根据本发明的方法的方框流程图；

图 8 是根据本发明的方法的方框流程图；以及

图 9 是根据本发明的方法的方框流程图。

具体实施方式

[0029] 本发明要求只在网络的边缘使用安全 iBF 路由器，并且使得在网络的核心中使用简单的基本 iBF 路由器变得可能。

[0030] 编码用于路径的转发信息的 iBF 可以以任何适合的方式来形成，例如，通过沿要求 iBF 的路径发送包含收集布隆过滤器的分组，通过逐跳收集形成。在域内，如 PCT/EP 2008/061167 和 PCT/EP 2009/062785 中所述收集和形成 iBF。在将 iBF 传递到相邻域之前(优选正好在其之前)，以相对于用于生成布隆过滤器的操作是线性的方式，例如使用键控比特置换函数，可反向地变换 iBF。置换函数将以攻击者不能猜测比特的原始位置的方式把

iBF 的每个比特从其位置移到另一位置。重要的是注意可反向的变换只需要在受信任域的边界执行一次。受信任域内的其它节点无需知道使用的置换或其它修改。实际上，置换或其它修改使得路径上的每个路由器对任何外部攻击者表现得象是安全路由器。

[0031] 比特置换函数是将比特字符串的比特从比特字符串中的一个位置移到另一位置的函数(Y. Hilewitz、Z Shi 和 R. Lee 于 2004 年的有关信号、系统和计算机的第 38 年度阿西罗马会议的会刊 1856 － 1863 页中发表的“比较比特置换指令的快速实现”(Y. Hilewitz, Z Shi and R. Lee.“Comparing Fast Implementations of Bit Permutation Instructions”, in proceedings of 38th annual Asilomar Conference on Signals, Systems, and Computers, pp. 1856-1863, 2004))。作为一个示例，如果我们将原始字符串的比特命名为 B1、B2、B3 和 B4，使得索引号指示在字符串中比特的位置(即，B1B2B3B4 是原始比特字符串)，则 B4B1B3B2 是字符串的可能置换。在我们的情况中，好的伪随机置换函数是为原始比特字符串的给定比特最后处于置换的比特字符串中的任何位置提供基本相等机会的函数。

[0032] 置换可以是静态置换，即，其中始终使用相同的置换。为了附加的安全性，使用的置换(或其它修改)可例如在固定时间间隔更改，或者可被连系于给定会话标识符(如流 id 或一对 IP 地址)。

[0033] 在下述实施例中，我们假设域间 iBF 由通过逐跳方法收集 iBF 的路由器形成。也就是说，收集器分组经想要 iBF 的路径发送。沿路径的每个路由器通过逐跳对应于路径的链路的链路标识符为分组中的“收集”iBF 盖戳。随后，在收集器分组到达例如在域边界的安全路由器时，安全路由器实现本文中公开的置换函数，即，它另外置换“收集”iBF 中的比特及添加其相应的链路标识符。随后，结果 iBF 被传递到第二域，并且另外链路标识符可由在第二域中的路由器添加到 iBF(并且原则上，在第二域的边界的安全路由器可在将 iBF 转发到第三域之前应用另外置换或修改，这是因为方法在存在多个信任边界和在路径上执行的多次比特置换时有效)。然而，本发明不限于通过逐跳方法收集 iBF，并且本发明可应用到为路径形成 iBF 的任何布置，例如，在显式、离线 iBF 路径计算单元(例如，拓扑管理器)将使用的置换函数及其沿给定路径或树的相应位置考虑在内的情况下。

[0034] 本发明的一优选实施例基本上是基于使用伪随机置换。诸如比特置换等置换始终可逆(可反向)，并且置换的使用因此允许可反向地变换 iBF。也就是说，置换可逆性确保对于每个域，在 iBF 中描述用于特殊流的链路的 1 比特将在反向置换后在其原始位置中。此外，1 比特的数量在分组发送到其它域之前不增大，例如，如果转而加密 iBF 会发生的一样。这使得其它域能够添加另外链路标识符到“收集”iBF 中—如果 1 比特的数量要在分组传递到另一域前增大，则 BF 可能变得“充满”1，并且其它域中的链路的链路标识符的或操作会工作不正常。另外，增大 1 比特的数量会导致错误肯定的概率增大。另外，由于置换是伪随机的，因此，我们能够确保“错误肯定率”的现有统计分析适用。

[0035] 将描述 iBF 的形成(“Z 形成”)作为背景。在 P. Jokela、A. Zahemszky、C. Esteve Rothenberg、S. Arianfar、P. Nikander 于 ACM SIGCOMM 2009 的会刊发表的论文“LIPSIN：线路速度发布 / 预订互相连网 (LIPSIN: Line speed publish/subscribe inter-networking)”中和 PCT/EP 2008/061167 (“LIPSIN”)中，描述了一种基于链路标识符 (LID) 而不是 IP 地址(或其它类型的端对端地址)的分组转发机制。该思想是在 LIPSIN

中称为拓扑层的分开的路径计算单元上计算每个转发路径。每个计算的转发路径(或树)包含在从源到目的地的路途上必须经过的节点集。在节点集给定的条件下,需要的出局 LID 添加到布隆过滤器,构成转发树的紧凑表示。称为 iBF 的此布隆过滤器从拓扑层传递到数据源,以便在从源节点发出时被放入数据分组报头中。在使用 iBF 来对分组进行路由选择时,路径上的每个路由器检查转发标识符以查看任何其自己的出局接口 LID 是否已被包括在 iBF 中。如果情况如此,则从该接口转发分组。由于此机制,转发是非常高效的操作,其(在基本形式中)由一个按比特与操作和一个比较操作组成。

[0036] 图 1 示出根据 LIPSIN 的基于布隆过滤器的路由选择的一般原理。LIPSIN 描述基于链路标识符 (LID) 而不是 IP (或其它类型的端对端)地址的分组转发机制。该原理是在拓扑层上或在诸如拓扑管理器等分开的路径计算单元构建转发路径,转发路径包含在分组的从源到目的地的路途上分组需要经过的节点集。从此节点集中,要求的出局 LID 用于构造布隆过滤器,构成转发树的紧凑表示。在图 1 中,通过示意地标记为 4 的过程生成布隆过滤器,在示例中通过对形成路径的链路的 LID 进行“或”来示出(过程)。此布隆过滤器或“iBF”被放入要从源节点 1 发出的数据分组 2 的报头中。生成布隆过滤器的过程 4 可在源节点 1 实施,或者它可在其它地方实施,例如,在拓扑管理器(图 1 中未示出)。分组 2 示为包含标识特殊分组流的流 ID 和数据。

[0037] 路径上的每个中间节点或路由器 3 对接收分组中的 iBF 执行匹配操作(在图 1 中示意地标记为 5),以检查是否任何其自己的出局接口的 LID 已被包括在分组中携带的 iBF 中。如果情况如此,则从该接口(所述多个接口)转发分组。由于此机制,在 [LIPSIN] 中转发是非常高效的操作,其(在基本形式中)由一个按比特与操作和一个比较操作组成。

[0038] 在 Christian Esteve、Petri Jokela、Pekka Nikander、Mikko Särelä 及 Jukka Ylitalo 于 2009 年关于计算机网络防御的欧洲会议(EC2ND)的会刊(proceedings of European Conference on Computer Network Defence (EC2ND) 2009)发表的“使用分组中布隆过滤器的自路由选择抗拒绝服务能力 (Self-routing Denial-of-Service Resistant Capabilities using In-packet Bloom Filters)”和 PCT/EP 2009/62785 (“Z 形成”)中,使用了一种更成熟的方案,而不是维持包含用于每个出局接口的多个链路标识符(或链路标识符标志,参阅 [LIPSIN])的显式转发表。该方案是基于动态计算的每流或每分组链路标识符。对于每个入局分组,固定的函数 Z 用于通过使用以下所述来计算对应的标识符

- (i) 定期更改的秘密密钥 K,
- (ii) 一些分组中信息 I (流或每分组标识符),其一部分可被选定为用于 z 过滤器变化的 d 值,以及
- (iii) 入局和出局接口索引 (入 , 出)。

[0039] 函数 Z 产生动态计算的链路标识符。这在图 2 中描绘,其示出在节点接收入局分组 6 时计算的链路标识符。函数 Z 使用入局和出局索引(入端口号和出端口号)、时间相关密钥 K(t)、分组中信息(图 2 的示例中是流 ID)及 d 值作为输入来计算链路标识符。函数 Z 计算一个或多个链路标识符 LIT(d)。如在 LIPSIN 中一样,此处每个 LIT(d) = Z (I , K(t), 入 , 出) 也是大小为 m 的布隆掩码。

[0040] 注意，分开“d 值”和流 ID *I* 是可选的；从概念的角度而言，d 值可视为流 ID 的一部分。

[0041] 由于现在使用动态链路标识符而不是静态链路标识符来构造 iBF，因此，除如在 [LIPSIN] 中一样绑定到输出接口索引外，所得的 iBF 还绑定到流 ID、特定的时间期和输入接口索引。尤其是，具有流 ID I 作为输入参数将给定 iBF 连系于仅携带指定流 ID 的那些分组。

[0042] 虽然 [LIPSIN] 解决方案原始设计成在带有分开的会合和拓扑功能的发布 / 预订式连网（publish/subscribe style networking）中使用，但也可能在其它类型的网络中使用它。从该角度而言，在本发明中，我们优选利用逐跳 IP 转发作为拓扑功能以及每个目标端节点作为会合点。

[0043] 现在将描述在域边缘使用置换保护 iBF。对于一些使用，静态置换是足够的。这里，我们描述用于在域边缘使用键控置换保护 iBF 的方法。此部分描述在本发明中公开的最基本新功能性。

[0044] 假设收集 iBF 用于在两个域 A 与 B 之间的路径。假设路径由链路 A1-A2-A3-B1-B2-B3 组成，如图 5 中所示。我们还假设收集过程创建反向 iBF，换而言之，沿路径的目的地 NB4 最初沿链路 B3 向沿路径的 A1 发送信令分组。信令分组包含最初为空的“收集”iBF 字段，即包含所有 0 比特。

[0045] 从节点 NB4 的角度而言，域 B 是“受信任域”，因为对于域 B 中的节点知道与域 B 中的路径有关的路由选择信息，不存在阻碍。然而，域 A 从节点 NB4 的角度而言不是受信任域，使得优选的是域 A 中的节点不知道与域 B 中的路径有关的路由选择信息。

[0046] 通过对接收的“收集”iBF 和适当的链路标识符一起进行按比特或操作，路径上的每个路由器添加用于“反向”下一跳（向 B3）的链路标识符到“收集”iBF，导致要在信令分组中发送到下一节点的新的、扩大的“已收集”iBF。例如，路由器 NB3 通过对接收的“收集”iBF 和用于链路 B3 的链路标识符一起进行按比特或操作，添加用于链路 B3（其是向 NB4 的“反向”下一跳）的链路标识符到“收集”iBF，并且将新的、扩大的 iBF 发送到下一跳 (NB2)。在信令分组从域 B 传递到域 A 前，域 B 内的最后路由器（路由器 NB1）计算至此聚集的“收集”iBF 的伪随机置换。假设在路由器 NB1 接收的至此收集的 iBF 是 zFB1,B2,B3（即，B1 或 B2 或 B3），并且假设置换是 P(zFB1,B2,B3)。随后，路由器 NB1 将 iBF zFB1,B2,B3 替换为置换的 iBF P(zFB1,B2,B3)，并且将包含置换的 iBF P(zFB1,B2,B3) 的分组发送到域 A 的边界路由器（图 5 中的路由器 A3）。

[0047] 图 6 是示出在节点 NB1 实施的主要步骤的方框流程图。最初在步骤 1，节点 NB1 在此示例中从节点 NB2 接收在分组报头中包含 iBF 的分组。节点 NB1 将用于“反向”下一跳（即，用于到图 5 中的节点 NB2 的跳）的链路标识符添加到 iBF，并随后在图 6 的步骤 2，如上所述对 iBF 执行可反向的修改。随后，节点 NB1 在图 6 的步骤 3 将包含修改的 iBF 的分组转发到节点 NA3。

[0048] iBF 随后通过域 A，其中，域 A 的每个路由器添加用于“反向”下一跳的链路标识符。因此，在图 5 的示例中，最终“已收集”iBF 将是：

A1 或 A2 或 A3 或 P(B1 或 B2 或 B3)，

其中，Ax 标记如路由器 x 使用的链路标识符，并且 P 是路由器 NB1 使用的置换函数。注

意，P 函数不更改 iBF 中 1 比特的数量，而是只将它们移到伪随机位置。

[0049] 一旦已收集 iBF，发送方节点 A1 就能够使用它以沿路径发送分组。在节点 NA1、NA2、NA3、NB2 及 NB3，可如现有技术中公开的一样处理任何包含 iBF 的数据分组。然而，在接收域内的第一节点（在此情况下的节点 NB1），应用伪随机置换的逆到 iBF。

[0050] 图 8 是示出在从域 A 发送分组到域 B 时在节点 NB1 实施的主要步骤的方框流程图。最初，在步骤 1，节点 NB1 在图 5 的示例中从节点 NA3 接收分组。分组在其报头中包含 iBF。在图 5 的示例中，节点 NB1 将接收包含如 A1 发送的 iBF—即，A1 或 A2 或 A3 或 P(B1 或 B2 或 B3)—的分组。随后，在图 8 的步骤 2，节点 NB1 应用反向修改到 iBF 以恢复路由选择信息—即，在图 5 的示例中，节点 NB1 应用反向置换 P^{-1} 到接收的 iBF，其依靠 P 相对于用于添加链路到布隆过滤器的操作（在此示例中，或操作）的线性（参见下述内容），导致 P^{-1}(A1 或 A2 或 A3) 或 B1 或 B2 或 B3。通过应用反向置换获得的 iBF 又能够由节点 NB1、NB2 和 NB3 根据已知 iBF 路由选择技术来使用，使得，在图 8 的步骤 3，节点 NB1 根据恢复的路由选择信息来转发分组。

[0051] 现在将详细说明用于置换函数 P（或其它修改）的要求。

[0052] 我们要求置换函数具有以下属性：

假设算子 + 标记用于添加链路到布隆过滤器的构建操作（这是上述示例中的或操作）。假设 $P(\square)$ 是伪随机置换，并且 $P^{-1}(\square)$ 是其反向。随后，对于任何等长比特字符串 x、y 和 z，要求：

$$P^{-1}(x + P(y + z)) \equiv P^{-1}(x) + P^{-1}(P(y + z)) \equiv P^{-1}(x) + y + z$$

换而言之，P 需要相对于算子“+”是线性的。比特置换函数是满足该属性的函数的一个示例，但满足要求的任何置换函数可在本发明中使用。

[0053] 另外，为使基于布隆过滤器的转发正常工作，我们要求由于应用置换 P 而生成的任何值—诸如发送到 A 域的值，即 P(B1 或 B2 或 B3)—必须不影响在域 A 中的分组转发的其它属性。也就是说，生成的值必须与域 A 使用的无论什么 BF 路由选择方案相互操作。因此，在置换使用加密会在许多情况下不工作，这是因为它可能会对于域 A 不保持布隆过滤器属性，例如，可能会不维持错误肯定率等。

[0054] 图 3 示出比特置换函数的一个示例，并且图 4 示出对应的反向置换。将看到，应用图 3 的比特置换函数和图 4 的对应反向置换的效果是恢复原始比特字符串。

[0055] 在一优选实施例中，置换函数不是静态置换函数。在一优选实施例中，置换函数取决于时间和分组内容二者，并且这使用以下形式的键控置换函数来实现：

$$P_{K,I}(\square),$$

其中，符号 $\square$ 标记输入字符串，K 标记可基于某一定期更改的密钥材料 K_d 计算的密钥，以及 I 标记会话标识符（其能够从分组推断）。K 和 I 一起形成索引，标记用于处理输入字符串的特定置换。

[0056] 键控置换函数有几个已知示例。作为一个特定示例，能够使用伪随机比特置换（例如参阅 Y. Hilewitz、Z Shi 和 R. Lee 于 2004 年的有关信号、系统和计算机的第 38 年度阿西罗马会议的会刊 1856 － 1863 页中发表的“比较比特置换指令的快速实现”(Y. Hilewitz, Z Shi and R. Lee. “Comparing Fast Implementations of Bit Permutation

Instructions", in proceedings of 38th annual Asilomar Conference on Signals, Systems, and Computers, pp. 1856-1863, 2004))。

[0057] 会话标识符能够是例如会合标识符、MPLS 标签或来自分组的 IP 报头(并且可能是传输报头)的一些信息,如源和目的地 IP 地址(或子网前缀)、端口号和协议类型,或其任何组合。

[0058] 总之,置换函数 P (或其它修改)必须满足一个或多个并优选是所有以下要求 :

●安全性 :攻击者必须不能根据置换的比特字符串推知 1 比特的原始位置。

[0059] ●可反向性(所有置换是可反向的,并且因此满足此要求)。

[0060] ●与其它 iBF 操作的兼容性 :从应用 P 导致的 1 比特的数量必须(近似)等于在输入中的 1 比特的数量。

[0061] 另外,密钥优选是基于路由器的隐私信息和与会话有关的信息(例如,流标识符)根据需要可计算的。多种方法能够用于此,如加密散列函数(cryptographic hash function)。

[0062] 另外,置换(或其它修改)优选是非静态的—使得即使大多数或所有路由器使用 iBF 的非安全变体,表明路径中的某些链路的比特的位置也取决于流。

[0063] 从安全性的角度而言,应注意的是,猜测作为某一 iBF 的一部分 z 的有效链路 ID 的概率与猜测对应比特通过 P(z) 移到的比特位置相同。因此,这两个概率相同(取决于每个链路添加的比特数量),并且 P 函数不会使猜测域内部的链路变得更难或更容易。

[0064] 函数 P 例如可如下实现。假设在 iBF 中的比特的总数为 n。也假设我们具有随机加密置换 F,其被应用在集 {1, 2, …, n} 上。(只要 n 是偶数)此类置换能够从熟知的 Luby-Rackoff 构造(Luby, M. 和 Rackoff, C. 于施普林格弗拉格的密码学研究中的进展 "CRYPTO'85" (Advances in cryptology "CRYPTO'85", Springer Verlag)发表的"如何从伪随机函数构造伪随机置换 (How to construct pseudo-random permutations from pseudo-random functions)")来构造。现在,为置换比特字符串 x(1)、x(2)、...、x(n),我们只将它映射到 x(F(1))、x(F(2))、...、x(F(n))。

[0065] 本发明不限于上述实施例,并且存在仍能够解决本发明公开所解决的问题的变化。

[0066] 例如,如果每个域利用其自己的 iBF,则能够在域边界加密在域内使用的过滤器。在图 5 为经链路 A1-A2-A3-B1-B2-B3 从 NA1 到 NB4 的路径创建 iBF 的上述示例中,这会意味着用于路径的转发标识符会包含两个(可能更短的)布隆过滤器 zF NA1-NB1 和 zF NB1-NB4 的级联。这很适合单播情况,并且适合跨信任边界发送 iBF 但 iBF 将不由接收方更改或扩大的情况。后者的一个示例能够是从提供商边缘 (PE) 路由器发送 iBF 到客户边缘 (CE) 路由器。

[0067] 然而,如果此变体应用到指定了域间多播树(例如,增大过滤器中比特的数量)的情况,则它可能有问题。考虑以下示例 :指定了从 A 到 (B1,B2,..., B20) 的多播树。随后,根据此变体的转发标识符应包含用于 21 个不同域的分开的 iBF—并且它应具有用于每个域的足够结构以便能够指出转发标识符的哪个部分指定其本地加密 iBF。

[0068] 在图 5 的实施例的描述中,通过从节点 NB4 发送收集器分组,生成用于域 B 中路径的部分(即,从 NB4 到 NB1 的部分)的 iBF。然而,本发明不限于此,并且用于域 B 中路径的

部分的 iBF 可备选地由具有域 B 的网络拓扑知识的拓扑管理器 TM 生成。生成的 iBF 随后从拓扑管理器 TM 发送到节点 NB1。在节点 NB1 接收 iBF 时，它随后如上所述应用可反向的修改到 iBF，将修改的 iBF 放入分组的报头中，并将分组转发到域 A。

[0069] 图 7 是示出在拓扑管理器 TM 实施的主要步骤的方框流程图。最初在步骤 1，拓扑管理器 TM 生成用于域 B 中路径的部分的 iBF，并随后在图 7 的步骤 2，拓扑管理器 TM 如上所述对 iBF 执行可反向的修改。拓扑管理器 TM 随后在图 7 的步骤 3 将在其报头中包含修改的 iBF 的分组转发到节点 NB1，以便包括在要从节点 NB1 发送的分组的报头中。

[0070] 原则上，拓扑管理器 TM 能够生成用于域 B 中路径的部分的 iBF，本身应用可反向的修改到 iBF，并且将修改的 iBF 转发到节点 NB1。在节点 NB1 接收 iBF 时，它将修改的 iBF 放入分组的报头中，并且将分组转发到域 A。此实施例会要求节点 NB1 具有拓扑管理器 TM 应用到 iBF 的修改的知识，使得节点 NB1 能够应用反向修改到从域 1 接收的分组中的 iBF 以便恢复路由选择路由选择信息。(为此，拓扑管理器 TM 和节点 NB1 需要共享要使用的置换的知识。拓扑管理器 TM 或节点 NB1 可决定要使用哪个置换，并随后通知另一方所选的置换。)。

[0071] 在仍另外的变体中，原则上拓扑管理器 TM 可能生成用于域 B 中路径的部分的 iBF，并且将 iBF 转发到域 A 中的另一节点(未示出)，其应用可反向的修改到 iBF，以及将修改的 iBF 转发到节点 NB1。这会再次要求节点 NB1 具有应用到 iBF 的修改的知识。(为此，域 A 中的节点和节点 NB1 需要共享要使用的置换的知识。域 A 中的节点或节点 NB1 可决定要使用哪个置换，并随后通知另一方所选的置换。)。

[0072] 图 5 示出在域 B 内的拓扑管理器 TM，但原则上拓扑管理器 TM 能够在域 B 外。

[0073] 现在将描述为增大安全性在客户边缘加密的变体。在上述实施例中，通过应用比特置换修改 iBF。然而，本发明不限于此，并且只要潜在攻击者不能从修改的 iBF 推断(或不能容易推断)原始路由选择信息，便可以以其它方式修改 iBF。

[0074] 作为一个示例，如上简要所述，可在发送 iBF 到其始发域外之前将其加密。加密可在比特置换之外，即，可在比特置换之后应用加密。应注意的是，比特置换可视为“加密”，因为它将一个比特字符串转换成(原则上)不知道使用的加密过程的某人不能破译的另一比特字符串。然而，比特置换不是特别强的加密，并且如果希望保护 iBF 的内容，则优选会在比特置换后应用更安全的加密。虽然加密在一些情况中是不需要的，但有能够应用对 iBF 的加密的一些情况，如接受方将不修改 iBF 的情况。在那些情况下，更改最大填充系数能够用于使强力攻击变得更困难。

[0075] 如在现有技术中所公开的一样，最大布隆过滤器填充系数将在布隆过滤器中 1 比特的最大数量定义为比特的总数的百分比。作为一个示例，带有 0.4 的最大填充系数的 256 个比特长 BF 只允许具有设为 1 的 102 个比特。在基于填充系数的过滤应用到基于 iBF 的转发时，网络中的每个路由器先检查在入局分组中的 iBF 是否具有大于指定最大值的填充系数，并且如果有，则丢弃分组。

[0076] 图 9 是示出此方法的主要步骤的方框流程图。在步骤 1，接收在其报头中包含以加密的 iBF 形式的路由选择信息(优选在比特置换已应用到 iBF 后应用加密)的分组(例如，图 5 的节点 NB1 从域 A 接收分组)，并且在步骤 2，节点解密路由选择信息以获得解密的 iBF。在图 9 的步骤 3，节点比较解密的 iBF 的填充系数和阈值，例如，检查解密的 iBF 的填充系数

是否超过 0.4。在图 9 的步骤 4，如果解密的 iBF 的填充系数超过阈值，则节点丢弃分组，否则根据在解密的 iBF 中的路由选择信息来转发分组（如果在比特置换后已应用加密，则在执行反向比特置换之后）。

[0077] 现在将更详细地考虑基于填充系数的过滤器的效果。

[0078] 我们将一对加密和解密函数相对应地标记为 E(□)和 D(□)。iBF 加密系统工作，使得边界路由器发送加密的 iBF 到其邻居路由器，即，它发送 E(zf) 而不是 zf 以防止邻居修改过滤器或者从其中恢复任何路由选择信息。在使用 iBF 进行路由选择时，邻居随后将把 iBF 的加密版本放入分组中代替 iBF。边界路由器从邻居路由器接收包含加密的 iBF 的分组时，边界路由器应用适当的解密函数 D(□)到接收的 iBF，其在加密的 iBF 的情况下返回原始 iBF。

[0079] 然而，不诚实的邻居仍能够通过以下步骤来尝试强力攻击技术：构造随机密码文本，即，发送许多分组并始终修改 iBF 的加密版本，使得每个分组包含不同的路由选择信息。在受信任域中接收任何此类分组时，边界路由器使用 D(□)将 iBF 字段解密，并且随后试图将分组转发到匹配通过应用 D(□)恢复的 iBF 的那些链路。由于不诚实的邻居将不同的路由选择信息放入每个分组中，因此，解密的结果将对于每个分组是不同的，使得每个分组在受信任域内被不同地路由选择。通过将 iBF 的最大可允许填充系数设为低于 0.5，例如设为 0.4，可抵消这种攻击，这是因为在随机字符串的解密能够被假设为产生带有 0 和 1 的随机分布的字符串时，这影响创建有效 iBF 的概率。使用 256 个比特长布隆过滤器时，二项式分布确保得到带有更小填充系数的字符串的概率是大约 $5*10^{-4}$（使用带有 128 的均值和 8 的标准差的标准分布约计）。因此，邻居发送的大部分的攻击分组将在到达信任域中其 iBF 字段被解密时产生具有大于最大可允许填充系数的填充系数的 iBF，并且因此，分组将被丢弃。

[0080] 使攻击者更难以猜测有效加密的 iBF（长度为 m）的另一种方式是：

1. 将 iBF（优选在应用比特置换后）与例如全部为零的 t 个预指定的比特级联。

[0081] 2. 加密所有 m+t 个比特。

[0082] 现在，攻击者需要猜测 m+t 个比特长的比特字符串，并且其解密成以 t 个已知比特结束的比特字符串。发现此类字符串的概率低，为 2^{-t}。

[0083] 本发明具有多个优点。如上所述，本发明甚至在存在非安全路由器 / 交换器的情况下使得能够安全使用基于 iBF 的路由选择。安全性能够在域边界处理，使得只要求边界路由器是安全路由器。域中其它地方的路由器和交换器能够是安全或非安全变体。

[0084] 本发明的核心是修改 iBF 中的比特，例如，通过安全的键控置换，其中，修改在将 iBF 传递到受信任域外的路由器前应用，并且随后在从受信任域外的节点接收分组时执行反向操作。

[0085] 与 PCT/EP 2008/061167、PCT/EP 2008/063647 和 PCT/EP 2009/062785 中所述的路由选择方法相比，本发明使得即使域在其网络中使用非安全 iBF 单元，也能够确保域内 iBF 信息的安全性和隐私。仅要求在域边界的路由器是安全的 iBF 路由器。

[0086] 本发明使得域能够形成指定路径的标识符，并且让不受信任的邻居域（客户端、支持者或竞争对手）为特殊流利用该标识符。对不受信任域中的节点隐藏受信任域内网络拓扑的细节，这有助于网络运营商保持其网络安全。作为一个示例，在使用域间 MPLS 时，运营

商不想显露其路由器的 IP 地址，因为这会导致攻击它们的可能性。根据本发明，能够在预定义时间内只相对于特定流向给定路由器开放路径。

[0087] 另外，在图 5 的示例中，只要求节点 NB1 执行本发明。节点 NB2、NB3 和 NB4 以与以前完全相同的方式操作，并且不要求修改。本发明由“边界节点”实现，即，由在 iBF 的构造中传递信令分组到域 A 以及在后来的路由选择期间从域 A 接收分组的节点实现。

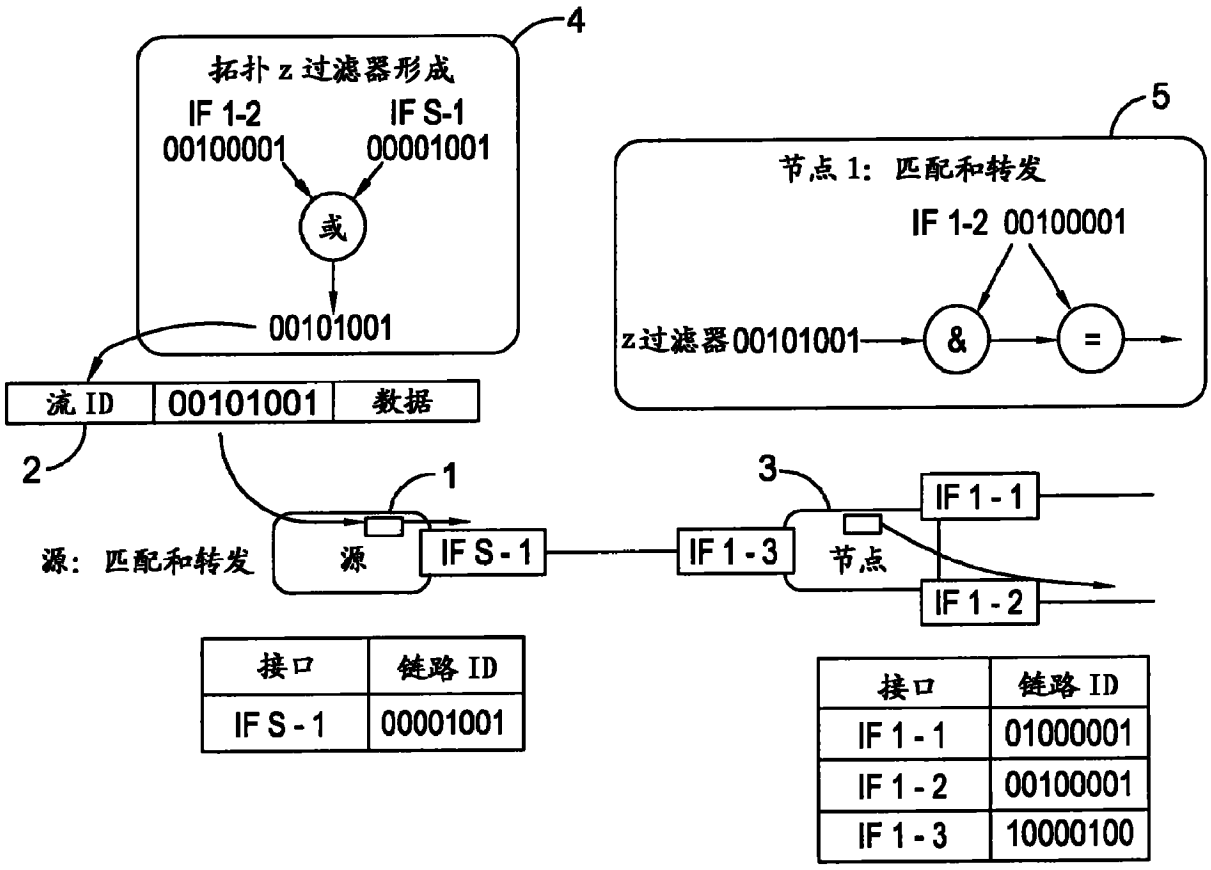
[0088] 本发明的另外优点是它也可防止环路和流重复。对于防止环路，使用的置换不必取决于分组内容，并且可使用静态置换。

[0089] 在连续系列的“错误肯定”造成分组遵照环路通过节点，使得它返回到在 iBF 指定的多播树中的边界路由器时，发生环路和流重复。在此类情况下，边界路由器将沿在分组中的 iBF 中指定的链路转发分组—但这些链路匹配与以前完全相同的链路。因此，分组将不可避免地遵照环路前进，直至它达到其跳计数限制并被丢弃。每一轮的循环造成分组的附加副本被转发到居于边界路由器的子树中的所有节点，其可以是相当多的资源浪费。

[0090] 所述发明如下解决了此问题。检验在接收分组中包含的 iBF 的每个基于 iBF 的路由器应用可反向的随机比特置换（或其它修改）到 iBF 的比特，基于置换的结果来执行转发决定，以及更新在报头中的 iBF。即使分组将遵照环路前进并返回到路由器，随机比特置换（或其它修改）的效果是在分组遵照环路前进后第二次在路由器被接收时，iBF 中的比特与它们为匹配路由器中的本地边缘对标签而需要位于的位置相比，将在随机位置中。假设比特置换是随机的，则匹配相同链路（对于“正确”路径和造成环路的路径）的概率与在任何链路上具有错误肯定的概率大约是相同的。

[0091] 本发明可与如下 PCT/SE 2010/050001 中所述的方法组合。

[0092] PCT/SE 2010/050001 提供用于每分组加密的布隆过滤器的“在线”生成的方法。实质上，沿链路序列路由选择的所有分组具有独特的“随机状”iBF，使得即使经过的 iBF 已知，攻击者也不可能预测沿相同路径的下一分组的 iBF 的值。另外，每个路由器可以以“线路速度”处理 iBF，即，无需缓冲，并且 iBF 的“解密”能够在 iBF 的每个比特到达 iBF 时递增地执行。相应地，如果图 5 的域 A 中的路由器使用 PCT/SE 2010/050001 的技术，则在域 A 的边界的节点可（在转发到域 B 之前）应用比特置换到在 A 内部产生的（已经加密的）iBF。



接口	链路 ID
IF S - 1	00001001

接口	链路 ID
IF 1 - 1	01000001
IF 1 - 2	00100001
IF 1 - 3	10000100

带有每链路单个标识符的基本 iBF 功能性

图 1

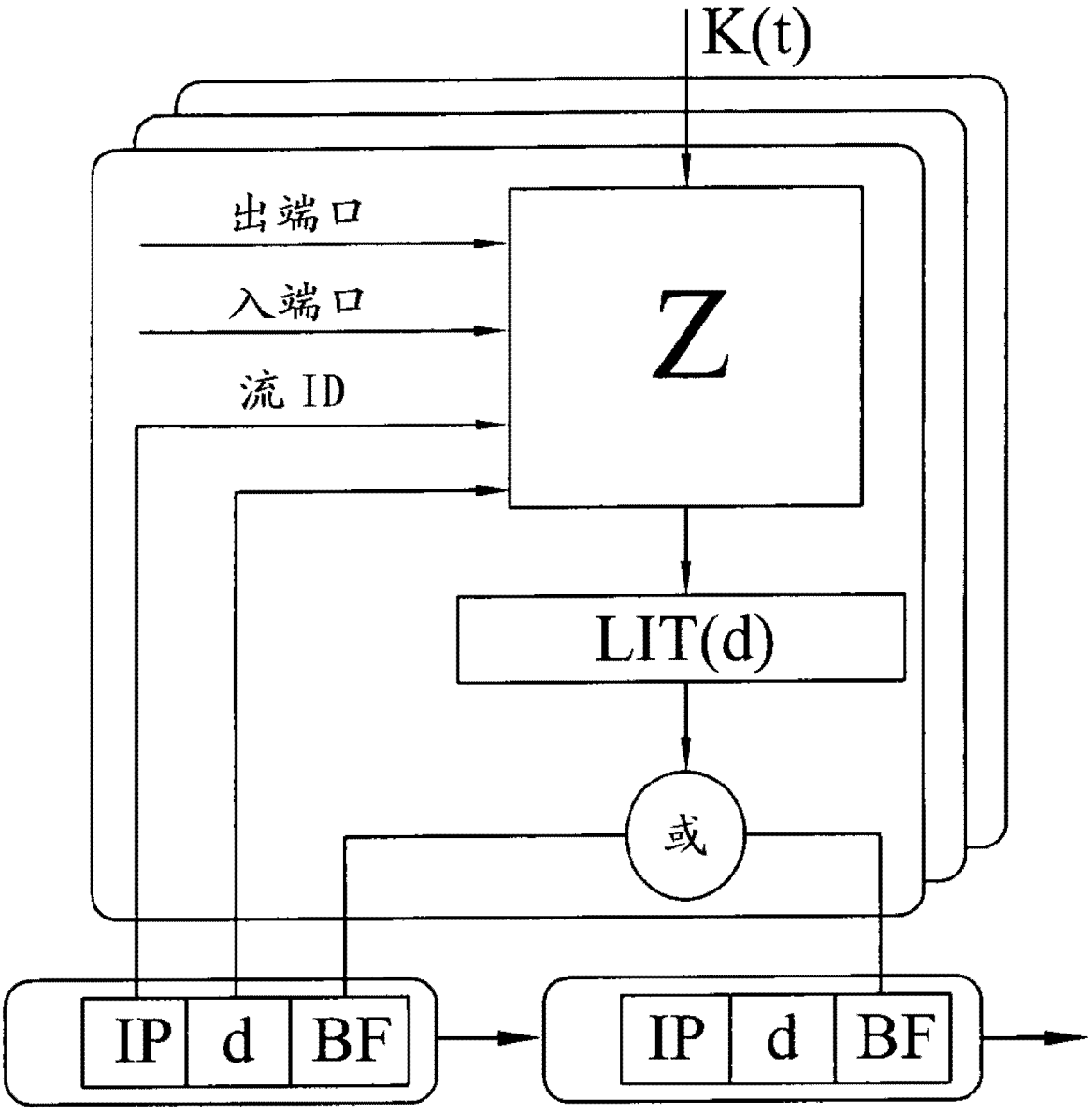
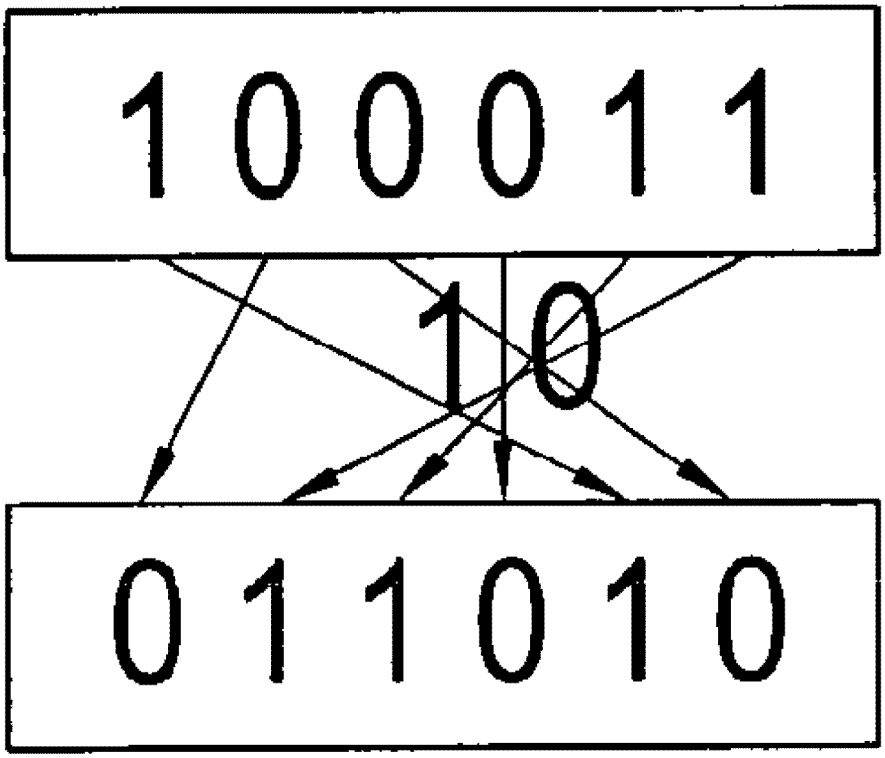


图 2



比特字符串的置换的示例

图 3

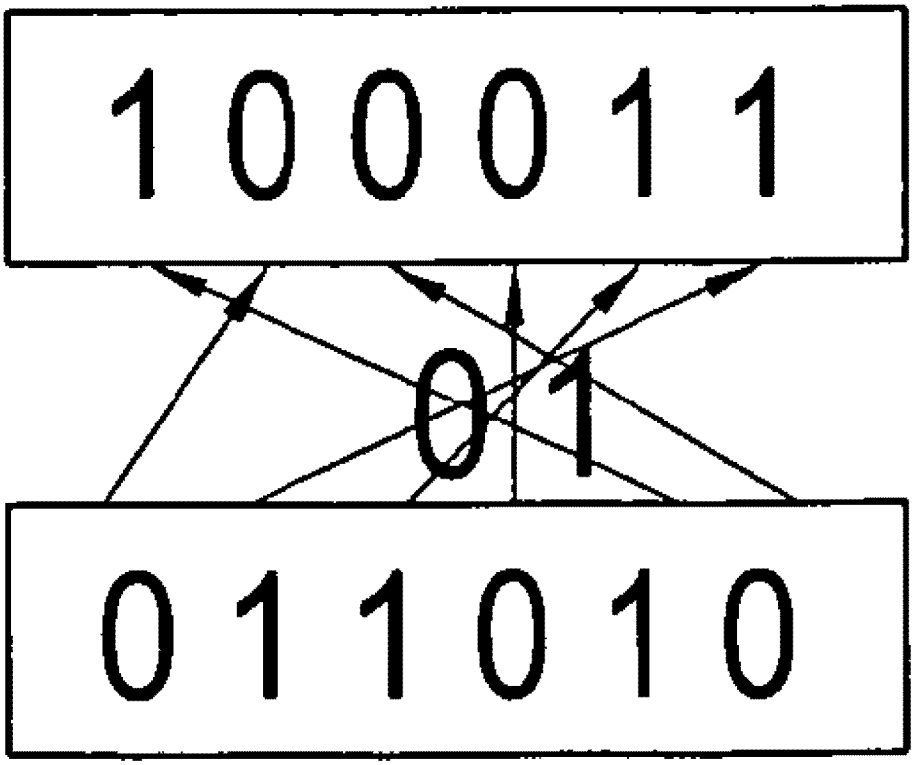


图 4

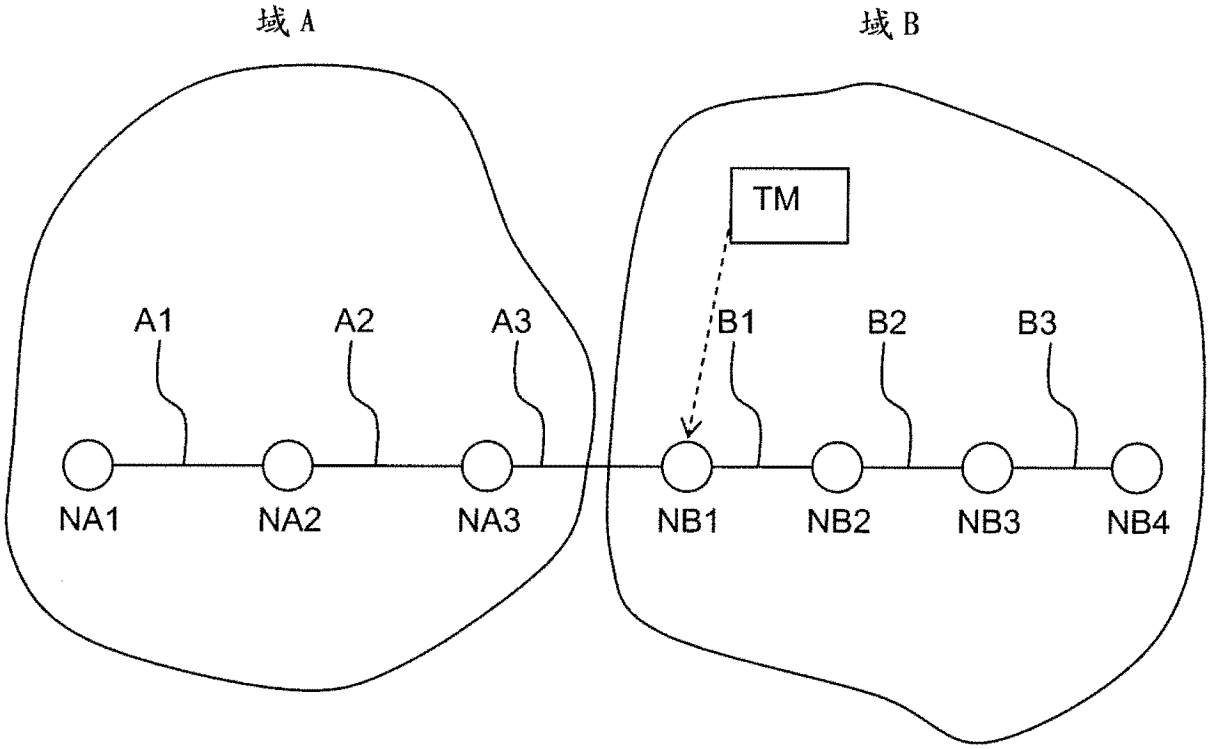


图 5

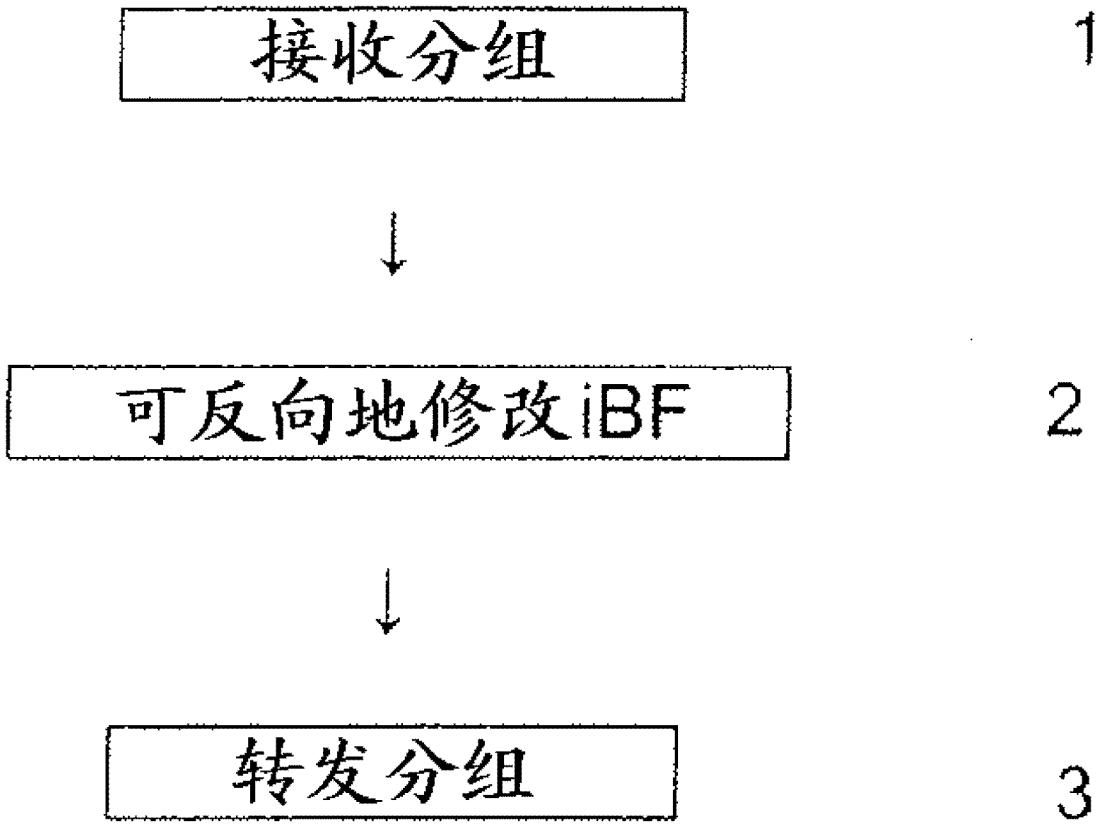


图 6

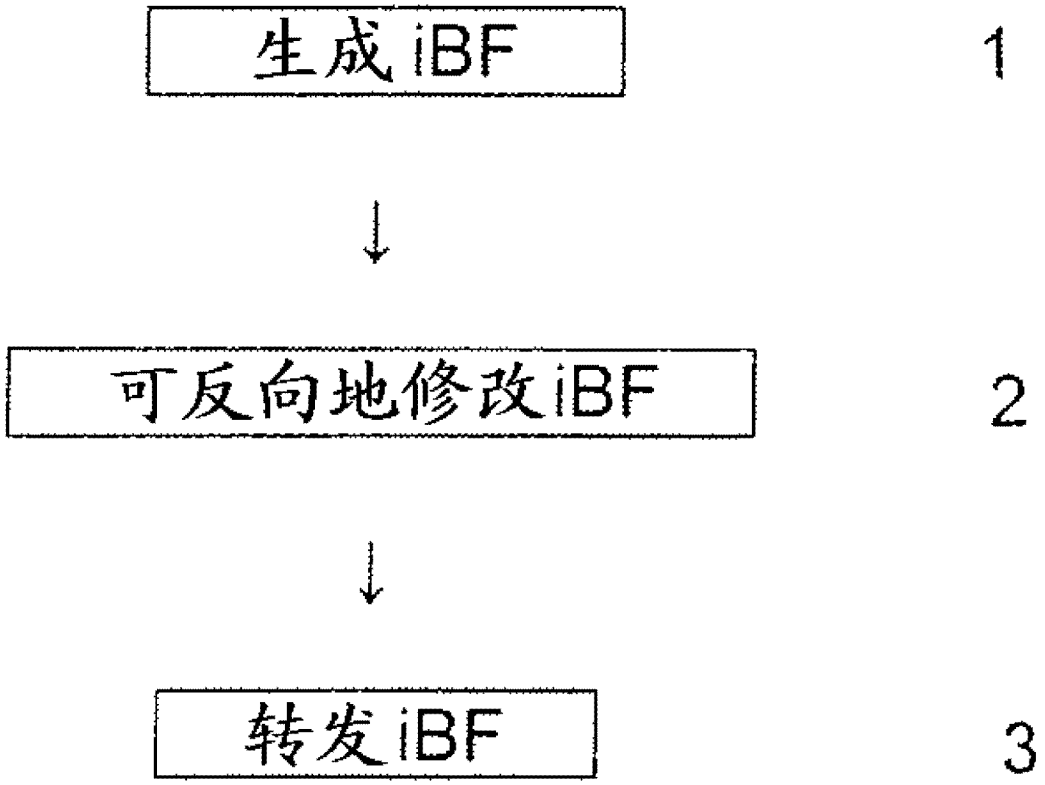


图 7

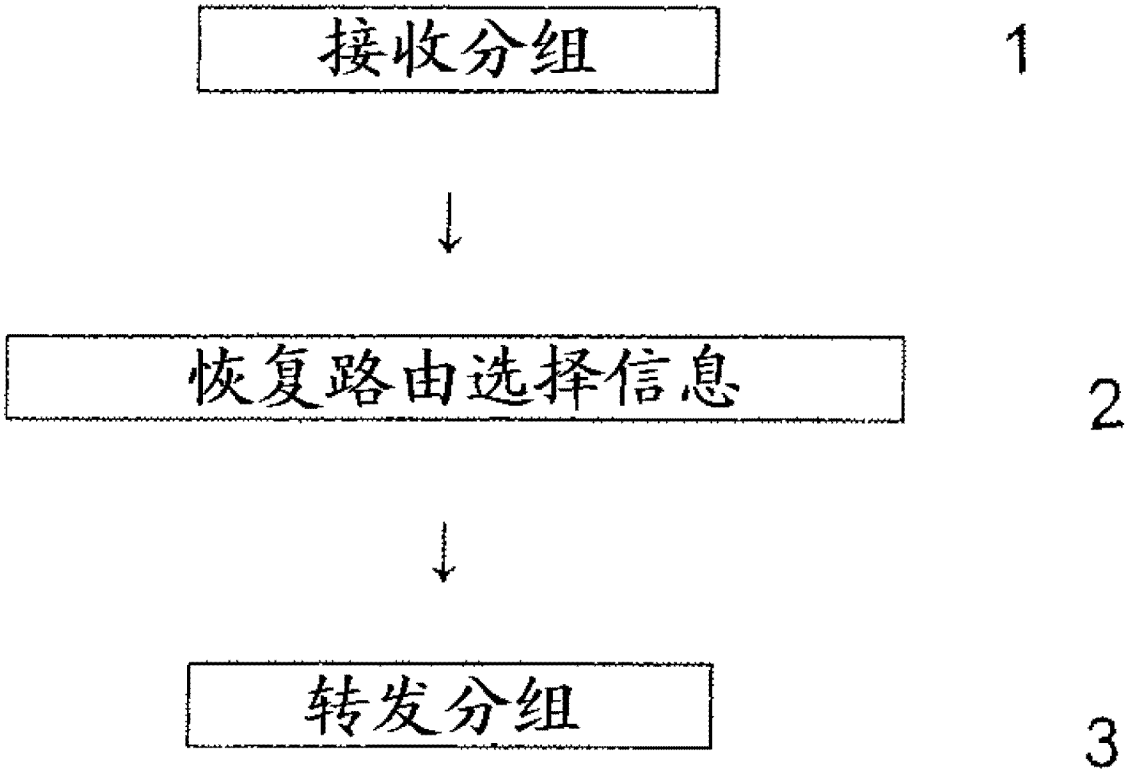


图 8

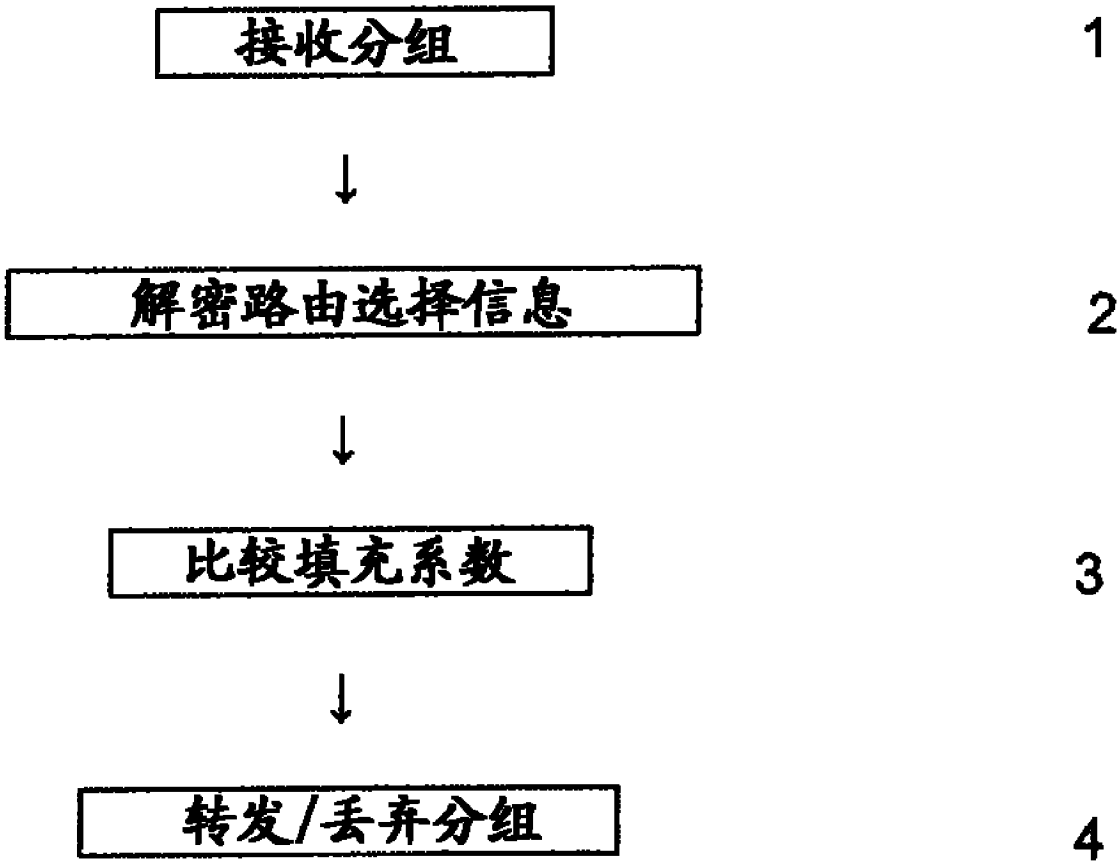


图 9