(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 1799241 B
(45)授权公告日 2010.09.29

(21)申请号 200480014919.0

(22)申请日 2004.03.22

(30)优先权数据
0312681.0 2003.06.03 GB

(85)PCT申请进入国家阶段日
2005.11.29

(86)PCT申请的申请数据
PCT/EP2004/050342 2004.03.22

(87)PCT申请的公布数据
WO2004/107702 EN 2004.12.09

(73)专利权人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩

(72)发明人 P·尼坎德 J·阿科

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杨凯 刘宗杰

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 1286555 A,2001.03.07, 权利要求 29-38、说明书第5页第4段至第10页第2段、图2,5.

审查员 汤广强

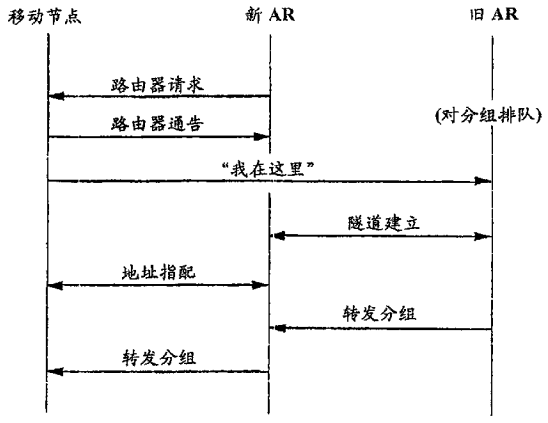
权利要求书 2 页 说明书 16 页 附图 2 页

(54)发明名称

IP移动性

(57)摘要

一种在移动节点从第一旧接入路由器切换到第二新接入路由器之后,将发往所述移动节点的旧转交地址的IP分组转发到所述移动节点的方法。该方法包括在所述切换完成之前,为所述第一路由器或另一个代理节点提供确定所述移动节点转移到所述第二接入路由器时供所述移动节点使用的新IP转交地址所需的信息。在所述第一路由器或所述代理节点上,利用所述信息为所述移动节点确定所述新转交地址,并确认所述移动节点对所述新转交地址的所有权;以及随后将所述第一接入网上接收到的、目的地为所述旧转交地址的分组转发到所述预测转交地址。



CN 1799241 B

1. 一种在移动节点从第一接入路由器切换到第二接入路由器之后，将发往所述移动节点的第一转交地址的 IP 分组转发到所述移动节点的方法，所述方法包括：

在所述切换完成之前，为所述第一接入路由器或另一个代理节点提供确定所述移动节点转移到所述第二接入路由器时供所述移动节点使用的第二转交地址所需的信息；

在所述第一接入路由器或所述代理节点上，利用所述信息为所述移动节点确定所述第二转交地址，并确认所述移动节点对所述第二转交地址的所有权；以及

随后将所述第一接入路由器上接收到的、目的地为所述第一转交地址的分组转发到所述第二转交地址。

2. 如权利要求 1 所述的方法，其特征在于：所述代理节点充当所述移动节点的因特网协议级代理，以使所述第一接入路由器相信所述移动节点尚未移动。

3. 如权利要求 1 所述的方法，其特征在于：确定所述第二转交地址的所述步骤是响应所述移动节点通知所述第一接入路由器或代理节点它已经移动或将要移动而执行的。

4. 如权利要求 3 所述的方法，其特征在于：所述移动节点从连接到所述第一接入路由器的链路将所述通知发送到所述第一接入路由器。

5. 如权利要求 3 所述的方法，其特征在于：所述移动节点从连接到所述第二接入路由器的链路将所述通知发送到所述第一接入路由器。

6. 如权利要求 3 所述的方法，其特征在于：所述第一接入路由器或代理节点在将分组转发到所述第二转交地址之前确认所述通知的及时性。

7. 如权利要求 6 所述的方法，其特征在于还包括：利用所述第一接入路由器定期发送、并在所述通知中反馈的现时来判断所述通知的及时性。

8. 如权利要求 5 所述的方法，其特征在于还包括：在所述第二接入路由器上对从所述第一接入路由器转发的 IP 分组进行排队，直到所述移动节点出现在连接到所述第二接入路由器的所述链路上，并且必需的地址解析和其它过程已完成来确保所述第二接入路由器和所述移动节点可以交换分组为止。

9. 如权利要求 8 所述的方法，其特征在于：所述第一接入路由器或代理节点在将分组转发到所述第二转交地址之前确认所述通知的及时性。

10. 如权利要求 8 所述的方法，其特征在于还包括：利用所述第一接入路由器定期发送、并在所述通知中反馈的现时来判断所述通知的及时性。

11. 如权利要求 1 至 7 中的任一权利要求所述的方法，其特征在于：确定所述第二转交地址的所述步骤是或然性的，可能失败。

12. 如权利要求 1 至 7 中的任一权利要求所述的方法，其特征在于：确定第二转交地址的步骤包括应用加密生成的地址。

13. 如权利要求 1 至 7 中的任一权利要求所述的方法，其特征在于：确定所述第二转交地址的所述步骤利用证书。

14. 如权利要求 1 至 7 中的任一权利要求所述的方法，其特征在于还包括：在所述第一接入路由器或所述代理节点确定所述第二转交地址之后，将隧道建立请求从所述第一接入路由器发送到所述第二接入路由器，随后通过所建立的隧道转发分组。

15. 如权利要求 13 所述的方法，其特征在于：所述第二接入路由器通过定期向监听移动节点发送现时来验证隧道建立请求的相关性；所述移动节点在扫描新链路时监听该现

时，并将其包含在发往所述第一接入路由器的通知中；所述第一接入路由器将所述现时包含在隧道建立消息中。

16. 一种在分组交换接入网中使用的接入路由器，包括：

用于执行如下操作的装置：确定当前或最近连接到所述接入路由器的移动节点的第二转交地址以及确认所述移动节点对所述第二转交地址的所有权；

用于执行如下操作的装置：将发往位于与所述接入路由器相关联的第一转交地址的所述移动终端的分组转发到所述第二转交地址。

17. 如权利要求 16 所述的接入路由器，其特征在于还包括用于执行如下操作的装置：在所述接入路由器以及与所述第二转交地址相关联的另一接入路由器之间建立隧道。

IP 移动性

[0001] 发明领域

[0002] 本发明涉及用于分组交换接入网中移动终端的快速切换机制。

[0003] 发明背景

[0004] 在（由 IETF 标准化的）移动 IPv6 协议中，漫游移动节点负责将它的当前转交地址 (care-of-address) 通知它的归属地代理以及对应的节点。无论何时，只要移动节点更改了它的转交地址，就会向它的归属地代理发送绑定更新消息，与对应的节点执行返回可路由性 (Return Routability) 过程，最终向对应的节点发送绑定更新。在移动节点已移动但绑定尚未更新期间，目的地为移动节点的分组继续被传递到旧的转交地址并按缺省会丢失。

[0005] 在典型的情况中，移动节点、归属地代理和 / 或对应节点（的至少其中一些）可能彼此相距很远，例如在不同的大陆上。因此，节点之间的通信时延可能非常高，通常至少 10 毫秒以及有时达到 100 毫秒级或更高。因为返回可路由性过程的原因，需要 1.5 次往返来更新对应节点上的绑定，以及需要至少 0.5 次往返来更新归属地代理上的绑定。在给定这些时延的情况下，更新绑定过程中的延迟可能高达数百毫秒或甚至更长。虽然此类延迟和分组丢失对于某些应用完全可以接受，但对诸如对话多媒体应用和其它实时应用等而言显然不可接受。

[0006] 为了克服分组丢失的问题，可以将发往旧转交地址的分组转发到新转交地址。此功能可以由移动节点的先前缺省路由器来执行。建立转发过程的一种可能方法由 IETF 移动 IP 工作组在如下文献中规定：[Koodli, R., " Fast Handovers for Mobile IPv6", draft-ietf-mobileip-fast-mipv6-06(work in progress), March2003]。分组转发可以在切换发生之前建立，但前提是移动节点知道新接入路由器的标识并可以将对应的标识符传递到先前的缺省路由器。否则，转发必须在切换之后建立，这可能导致一些分组丢失。

[0007] 此问题的任何解决方案必须既简单又安全。应该尽可能避免状态创建，除了其它缺点，在网络上创建状态总是一种潜在的安全风险。任何解决方案还必须是可伸缩的。应该避免显式的安全体系结构（如 AAA 或 PKI），因为它们可能造成可伸缩性瓶颈。

[0008] 发明概述

[0009] 根据本发明的第一方面，提供一种在移动节点从第一旧接入路由器切换到第二新的接入路由器之后，将发往所述移动节点的旧转交地址的 IP 分组转发到所述移动节点的方法，所述方法包括：

[0010] 在所述切换完成之前，为所述第一路由器或另一个代理节点提供确定所述移动节点转移到所述第二接入路由器时供所述移动节点使用的新 IP 转交地址所需的信息；

[0011] 在所述第一路由器或所述代理节点上，利用所述信息为所述移动节点确定所述新转交地址，并确认所述移动节点对所述新转交地址的所有权；以及

[0012] 随后将所述第一接入网上接收到的、目的地为所述旧转交地址的分组转发到所述预测转交地址。

[0013] 在涉及代理节点的情况中，代理节点可充当所述移动节点的因特网协议级代理，

以使所述第一接入路由器相信所述移动节点尚未移动。

[0014] 最好，为所述移动节点确定所述新转交地址的所述步骤包括基于一个或多个成分预测所述地址。预测所述新转交地址的所述步骤是响应所述移动节点通知所述第一路由器或代理节点它已经移动或将要移动而执行的，其中所述移动节点从与连接到所述旧接入路由器的链路将所述通知发送到所述第一接入路由器。或者，所述移动节点可以从连接到所述第二接入路由器的链路将所述通知发送到所述第一接入路由器。

[0015] 所述第一接入路由器或代理节点可以在将分组转发到所述新转交地址之前确认所述通知的及时性。这包括利用所述第一接入路由器定期发送、并在所述通知中反馈的现时 (nonce) 来判断所述通知的及时性。

[0016] 所述方法可以包括在所述第二接入路由器上对从所述第一接入路由器转发的 IP 分组进行排队，直到所述移动节点出现在所述新链路上，并且必需的地址解析和其它过程已完成来确保所述第二地址路由器和所述移动节点可以交换分组为止。

[0017] 所述方法可以包括在所述第一接入路由器上对目的地为所述移动节点的旧转交地址的分组进行排队，直到所述第一接入路由器能够确定所述移动节点的新转交地址为止。

[0018] 可以根据所述接入路由器与其它接入路由器和 / 或所述移动节点之间存在的信任关系，为所述移动节点建立队列。所述队列的最大大小取决于所述信任关系。

[0019] 预测所述新转交地址的所述步骤是或然性的，因此可能失败。

[0020] 预测所述新转交地址的所述步骤可以包括应用移动节点和接入路由器已知且理解的过程。该过程利用以加密方式生成的地址。更具体地说，该过程可以利用证书。

[0021] 确定新转交地址的所述步骤可以包括利用属于所述移动节点的公钥 - 私钥对中的公钥来生成所述新转交地址，以及确认所述移动节点对所述新转交地址的所有权的所述步骤包括利用所述私钥在所述移动节点上生成签名的消息，并将所述签名的消息发送到所述第一接入路由器。

[0022] 所述新转交地址可以是所述第一接入路由器预测的多个转交地址之一，所述第一接入路由器将分组转发到每个所述预测的转交地址。

[0023] 所述方法可以包括在所述第一路由器或所述代理节点预测所述新转交地址之后，将隧道建立请求从所述第一路由器发送到所述第二路由器，随后通过所建立的隧道转发分组。

[0024] 所述第二接入路由器可以通过定期地向监听移动节点发送现时来验证隧道建立请求的相关性，所述移动节点在扫描新链路时监听所述现时并将其包含在发往所述第一接入路由器的通知中，所述第一接入路由器将所述现时包含在所述隧道建立消息中。

[0025] 根据本发明的第二方面，提供一种在分组交换接入网中使用的接入路由器，它包括：

[0026] 执行如下操作的装置：确定当前或最近连接到所述接入路由器的移动终端的将来转交地址以及确认所述移动节点对所述新转交地址的所有权；

[0027] 执行如下操作的装置：将发往位于与所述接入路由器相关联的转交地址的所述移动终端的分组转发到所述转交地址。

[0028] 所述接入路由器可以包括用于执行如下操作的装置：在所述接入路由器与所述预

测的将来转交地址的相关的第二接入路由器之间建立隧道。

[0029] 根据本发明的第三方面，提供一种在本发明的上述第一方面中使用的移动节点，它包括用于执行如下操作的装置：通知所述第一接入路由器所述移动节点已经或将要转移到新接入路由器。

[0030] 根据本发明的第四方面，提供一种在所述移动节点从第一旧接入路由器切换到第二新的接入路由器之后，将发往所述移动节点的旧转交地址的 IP 分组转发到所述移动节点的方法，所述方法包括：

[0031] 在所述切换完成之前，为所述第一路由器或另一个代理节点提供预测所述移动节点转移到所述第二接入路由器时供所述移动节点使用的新 IP 转交地址所需的信息；

[0032] 在所述第一路由器或所述代理节点上，利用所述信息为所述移动节点预测所述新转交地址；以及

[0033] 随后将所述第一接入网上接收到的、目的地为所述旧转交地址的分组转发到所述预测转交地址。

[0034] 附图简介

[0035] 图 1 显示与本发明第一实施例相关的信令；

[0036] 图 2 显示从旧接入路由器到新接入路由器的分组转发隧道；

[0037] 图 3 显示通过图 2 的隧道转发之前和转发期间 IP 分组的结构；

[0038] 图 4 显示新 ICMP（隧道建立）消息的结构；

[0039] 图 5 显示图 4 的 ICMP 消息的内容。

[0040] 一些实施例的详细说明

[0041] 本文提出的过程提供一种为在受访网络漫游的移动节点建立从旧转交地址到新转交地址的转发的新方法。在一个示例方案中，移动节点是无线移动终端，而受访网络是蜂窝电话系统的分组交换接入网。该接入网包括移动节点可以连接到的若干接入节点。移动终端的拥有者 / 用户是某个其它“归属地”网络的订户。就安全性和消息效率而言，这里提出的切换方法优于先前提出的方法。具体而言，在移动节点与旧接入路由器之间建立转发可以利用少到一个消息来实现。利用一些网络的附加假设，有时甚至无需额外的消息即可在移动节点与接入路由器之间建立转发。

[0042] 应注意，即使本文档是针对优选的移动 IPv6 来编写的，但所提出的过程绝不限于移动 IPv6。它适用于基于移动节点通知其对等方其地址变更的机制的任何 IP 移动性技术。

[0043] 实现快速切换的过程依赖于几个简化假设。这些假设允许以比先前方法所能实现的更少的消息和更好的安全性来建立必要的状态。这些假设在实际环境中是实际的。此外，还提出了该过程的一些变化方案，它们取消了这些假设而存在一些效率损失。

[0044] 所作的第一个假设是，移动节点可以较高概率预测切换之后可能与新接入路由器一起使用的新转交地址。在地址预测失败的不太可能的情况中，可能将少量分组发送到错误的目的地主机，但这些分组将被接收方丢弃。在本文所述的主要机制（也称为“基本”机制）中，参与切换过程的新接入路由器假定旧接入路由器不向它发送任何不必要的业务。注意，路由器已经假设因特网中的主机不向不存在的节点发送分组或不发送不必要的分组。但是，确保该假设成立的一种方法是，确保两个路由器属于同一个管理域，并且该网络执行源地址过滤，使得不可能发送含有“假冒”源地址以使它们看似来自旧接入路由器的分

组。在任何情况下，此假设失效的可能负面效应相对温和，已预计路由器能够区分资源使用的优先级，以防止资源耗尽。此外，所提出的机制的一种变型提供启发式的加密手段，用于区分伪造的业务与合法的业务。下文将对此予以详述。

[0045] 为了达到防止移动节点在接入路由器之间切换期间和之后不必要的分组丢失，需要建立一种机制，据以将目的地为旧转交地址的分组传送到新转交地址。为此，建立从旧接入路由器到新转交地址的转发隧道，由此将分组转发到移动节点的新位置。转发隧道具有有限的使用期，当然，如果需要的话，移动节点可以显式地请求延长隧道的使用期。务必要注意的是，虽然隧道端点之一位于旧接入路由器处，但另一个端点却不在新接入路由器处，而是在移动主机本身内，即在其新转交地址处。

[0046] 快速切换过程有两种主要变型。在“主动式”情况中，转发隧道在移动节点离开旧链路之前建立。在“反应式”的情况中，转发隧道在移动节点一到达新链路且可以使用它的新转交地址时建立。转发隧道本质上是一种优化，因此是“软状态”。如果需要的话，旧接入路由器可随时自由地拆除隧道，甚至在隧道使用期终止前。这可能导致分组丢失，但这在给定情况下是可以接受的。

[0047] 一旦移动节点已经移动到新链路，则可以双向使用该隧道。这允许移动节点在它用于更新绑定的时间内利用旧转交地址发送分组。新的接入路由器无需知道该转发隧道。它所看到的是，旧接入路由器将分组发送到位于新转交地址的移动节点以及移动节点从新转交地址将分组发送到旧接入路由器

[0048] • 反应式转发

[0049] 在反应式转发情况中，旧接入路由器可以对发往旧转交地址的一些分组进行排队，以希望该移动节点会复原或者会随后建立转发隧道。这种转发机制受本地策略制约，并且可以简单地通过移动节点离开旧链路而加以触发。图 1 显示了与反应式转发情况相关的信令。但应注意，消息的顺序不一定如图所示。例如，“我在这里”消息可以在地址指配消息之后发送。此外，可以不需要隧道建立消息，而是利用本文其它地方描述的邻居发现来实现隧道建立。还要注意，地址指配过程通常包括多个，且可以在整个信令方案中的不同点上执行。分组转发可以在新 AR 接收到“我在这里”消息之后即刻启动或稍后启动。转发可以通过新 AR 进行或直接寻址到移动节点。在后一种情况中，新 AR 会缓存分组，直到完成地址指配为止。

[0050] • 主动式转发

[0051] 在主动式转发的情况中，为了避免新接入路由器上丢失分组，可能需要在移动节点准备好在新转交地址接收分组之前由新接入路由器对少量分组进行排队。但此排队问题视为在结构上不同于转发问题。如上所述，新的接入路由器无需创建任何状态，即使采用转发时也是如此。另一方面，排队本身创建了状态。首先，看上去似乎旧接入路由器有必要显式地要求新接入路由器对转发的分组排队。然而，更进一步地考察可发现这种信令完全不必要。如上所述，假定新接入路由器相信旧接入路由器不会不必要地发送任何分组。基于此假设，可以在接入路由器之间创建隐含的协定。新接入路由器假设如果旧接入路由器向其发送目的地为未知节点的分组，则旧接入路由器有理由预计该节点不久会到达该新接入链路。因此，新接入路由器可以安全地使分组暂时排队（如果空间和其它资源允许的话）。这里信令并无帮助。如果新接入路由器有资源，则可以轻易对分组进行排队，即使它还没有

接收到这样做的请求。另一方面，如果新接入路由器没有足够的资源，则它无法对分组进行排队，即便旧接入路由器请求它这样做。

[0052] 如果新接入路由器不知道或不信任旧接入路由器，则情况变得稍微更复杂。如果新旧接入路由器之间完全没有任何关系，则情况变得基本上与上述的一样：新接入路由器能够对未知的分组进行排队或者它不能对其进行排队。来自未知的和不信任的旧接入路由器的信令消息并无帮助，因为它可以被伪造。更具挑战性的情形是，新接入路由器起初并没有任何理由要信任旧的接入路由器，但存在新接入路由器信任的第三方，它能够为旧接入路由器提供担保。然而，即便如此，仍无必要将各移动主机情况通知给新接入路由器。信令不会向新接入路由器增加任何资源。因此，如果首先需要信令来在路由器之间建立信任关系，则最好使信令与分组的实际排队分开。

[0053] • 信任关系

[0054] 基本协议中涉及三方：移动节点、旧接入路由器和新接入路由器。根据需要，移动节点必须信任接入路由器会提供路由选择服务。即，必须相信这些路由器在移动节点和它的对等方之间正确地传递分组。此外，最可能的是，移动节点应该或至少可以信任路由器不会故意对它发起攻击。此外，在建立转发隧道之前，移动节点必须肯定旧接入路由器会正确地执行转发。在实际情况中，移动节点可能对该接入路由器进行认证，之后才决定信任它们。但是，这种机制不属于本发明的范围。

[0055] 新接入路由器必须在某种程度上相信旧接入路由器不会不必要地发送目的地为该链路上尚不存在的节点的分组。此信任可以体现在新接入路由器准备好用于对分组进行排队的空间和资源的数量上。因为潜在的旧接入路由器可能属于可信度可变的类别，所以新接入路由器可以为每个类别预留不同的资源量。例如，它可能愿意对来自看似在与自己相同的子网内的节点的分组进行排队，而拒绝对任何其它节点发送的分组进行排队

[0056] 接入路由器不应该信任移动节点。接入路由器必须假设移动节点可能尝试对它们或其它移动节点发起各种类型的攻击。另一方面，接入路由器被视为有必要向移动节点提供服务。即，即使接入路由器不信任移动节点，它们仍必须对往来于移动节点的分组进行路由。此外，旧接入路由器应该至少在有限的时间内愿意代表最近离开链路的移动节点转发分组。

[0057] 在主动式情况中，还假设移动节点信任旧接入路由器会基于新接入路由器的标识符来正确地建立转发隧道。此外，移动节点需要能够相信旧接入路由器在移动节点实际离开该链路之前不会开始转发分组。

[0058] 在上述基本协议中，假定节点不信任网络中的任何其它方。另一方面，一些变型方案假定存在可信的第三方。

[0059] 假定移动节点在它仍然在旧链路上时从旧接入路由器获悉时间概念。这样，它可以将转发隧道建立消息与接入路由器的时间概念绑定，由此对抗重放攻击。无需假定任何方之间的时钟同步。

[0060] • 潜在的威胁

[0061] 因为上述机制在收到不信任的移动节点请求时在接入路由器上创建状态，所以该机制易受未授权的状态创建的攻击。此外，该机制可能开放新的拒绝服务可能性。在此部分中，我们简要分析已识别的威胁。

[0062] 地址窃取

[0063] 如果攻击者能够在接入路由器处创建未授权的转发隧道，则它实际可以将所有分组通过隧道传送给自己或传送到一个黑洞(blackhole)。这类似于移动IPv6的基本地址窃取攻击，而且在完整性和保密方面具有类似的后果。该攻击对任何使用易受攻击接入路由器来进行网络接入的节点产生消极影响。

[0064] 将来地址窃取

[0065] 如果攻击者能够预测到移动节点可能在链路上使用的转交地址，且如果它可以利用该特定地址来连接到该链路，则可以暂时使用该地址，离开，并请求要转发到的地址。这种请求将是得到授权的，因为攻击者在合法地使用该地址。当受害者以后来到该链路时，它将得不到任何分组，因为它的地址被转发走了(forward away)。

[0066] 未授权的转发隧道中断

[0067] 将来地址窃取的脆弱性无法通过简单地假定链路上的活动节点总是超越转发隧道而缓解。这种做法允许攻击者正好在移动节点离开之后使用移动节点的地址，从而使转发隧道中断。

[0068] 创建至伪造端的转发隧道

[0069] 攻击者可能能够创建其端点位于攻击者未打算移动到的位置上的转发隧道。如果在该位置上有一个正在进行排队的新接入路由器，则该攻击将耗用该新接入路由器上的排队资源。

[0070] 隧道建立泛洪

[0071] 如果攻击者能够同时建立大量的转发隧道，且全部指向同一个转交地址或一个网络，则攻击者能够使大量分组涌向目标。攻击者本身不需要在初始建立之后参与业务，因为分组将由攻击者在建立转发隧道之前联系的各服务器发送。这类似于移动IPv6泛洪攻击(flooding attack)。

[0072] 重放隧道建立

[0073] 如果攻击者能够记录转发建立消息，并在以后移动节点返回该链路时重放它，则攻击者能够“以黑洞方式”接收业务。其结果是拒绝服务。

[0074] 耗尽新接入路由器上的排队资源

[0075] 新接入路由器可能想要对在移动节点到达之前到达的转发分组进行排队。该路由器只有有限的资源可用于存储此类分组。如果攻击者能够使新接入路由器不必要地对分组进行排队，则可能需要非常多的资源，以致路由器无法对目的地为合法移动节点的分组进行排队。因此，希望新接入路由器可以在某种程度上区分需要排队的合法转发分组和不需要排队的随机分组。

[0076] 耗尽旧接入路由器上的排队资源

[0077] 旧接入路由器可能想要对目的地为已离开、但尚未建立至其新位置的转发信道的移动节点的分组进行排队。与新接入路由器的情况一样，只有有限的资源可用于存储此类分组。如果攻击者可以迫使该接入路由器不必要地存储从不会传递到移动节点的新位置的分组，则将束缚资源。因此，希望旧接入路由器可以在某种程度上区分可能发送到移动节点的分组与不可能发送到移动节点的分组。

[0078] • 解决方案

[0079] 基本的解决方案由两部分构成。第一部分关注的是，创建从旧接入路由器到移动节点的新位置的转发隧道。第二部分针对接入路由器上的分组排队问题。该解决方案基于一个有关转交地址的协定。即不允许移动节点随意利用它们想要使用的任何转交地址，而是移动节点和接入路由器必须就移动节点要使用或至少可能使用的转交地址达成协定。确切的协定取决于所采用的安全解决方案。基本协议采用加密生成的 IPv6 地址 [Aura, T., " Cryptographically GeneratedAddresses(CGA)" , May2003.]。

[0080] 本解决方案的特点在于仅需要最少的状态需求。在移动节点请求建立转发隧道之前，两个接入路由器都无需具有任何每个节点状态，而用于其它目的那些状态除外。自然，例如，旧接入路由器必须保存有关它正在服务的移动节点的状态信息。此状态信息通常仅在移动节点离开链路之后短暂保存，并且该状态可用于控制转发建立和分组排队。但是，这种状态并非必要，即使没有这种状态，仍可以安全地创建转发隧道。

[0081] 在移动节点实际到达链路并获得转交地址之前，新接入路由器没有且无需具有任何状态。即使此后，所需的唯一显式状态是新接入路由器必须为其它目的而保存的对应于各移动节点的自然状态。

[0082] 务必注意，状态需求对转发建立和分组排队而言稍微不同。对于转发建立，所有先验状态信息可以存储在移动节点上。而另一方面，对于分组排队，旧接入路由器可能需要保存有关它最近服务过、但已经不再服务的节点的状态信息。

[0083] 为了防止分组丢失，将发送到旧转交地址的分组转发到新转交地址。为此，建立从旧接入路由器到移动节点的新转交地址的转发隧道。所形成的隧道如图 2 所示。该隧道在旧接入路由器与位于新位置的移动节点之间创建。即，外部 IP 首部将新转交地址作为其目的地地址以及将旧接入路由器地址作为其源地址。相应地，隧道状态位于移动节点和旧接入路由器上；新接入路由器可能仍不知道隧道的存在。图 3 显示了转发（上方）之前和转发期间（下方）的 IP 分组格式。

[0084] 在“主动式”情况中，隧道逻辑上是在移动节点到达新位置之前建立的。在该情况中，（一些）分组将在新接入路由器上进行排队，直到移动节点到达新位置为止。如前所述，这不会强加要在新接入路由器上具有显式的每节点状态。

[0085] 隧道的两端点可以分开创建。旧接入路由器上的端点应移动节点的请求创建。另一个端点在移动节点一确知它的新转交地址时就创建。必须注意，在某些情况中，旧接入路由器在移动节点知道即将到来的新转交地址之前就知道该地址。如果例如转交地址是通过算法确定的，则这是可能的，如下所述。

[0086] 在基本协议中，转交地址总是 CGA 地址 [Nikander, P., " Denial-of-Service, Address Ownership, and Early Authentication in the IPv6World " , Security Protocols 9th International Workshop, Cambridge UK, April 25-272001, LNCS 2467, pages 12-26, Springer, 2002]。其基本思想是，通过对路由前缀和移动节点的公钥进行加密散列运算来创建 IPv6 的接口标识符部分。其细节在 [Aura, T., " CryptographicallyGenerated Addresses(CGA)" , May2003.] 中定义，这里不必累述。

[0087] 这种构造具有三个重要效果：

[0088] • 这些地址是随机分布的，而且如果丢失任何散列输入，则难以预测该地址会是什

么。

[0089] • 在给定路由前缀、公钥和其它参数的情况下，则任何节点都可以容易地构造最可能的地址。

[0090] • 在给定地址、公钥和其它参数的情况下，节点可以验证该公钥是否以高概率与该地址相关。换言之，在给定地址的情况下，难以构造出在同一链路条件下得到相同地址的另一个公钥。此外，在给定任何公钥的情况下，甚至更难以构造出在两个不同链路条件下得到相同地址（与给定的一样）的不同公钥。

[0091] 值得注意的是，在没有关于公钥的任何知识的情况下，地址看似几乎是随机的，不会揭示有关节点标识的任何信息。但是，如果保持相同的接口标识符较长时间，则这可能有助于确定移动节点的标识并跟踪它的移动。为对付这一潜在问题，移动节点可以定期变更它的公钥或用作接口标识符生成的输入的其它参数。

[0092] 移动节点可以请求旧接入路由器在它变更位置之前主动创建转发隧道或在变更位置之后反应性地创建隧道。还存在一种以下将进一步讨论的特殊情况，即旧接入路由器甚至可以自主地创建转发隧道。

[0093] 主动操作并非总是可能的。它仅仅在如下条件得到满足时可能：

[0094] 1. 移动节点可以预测到它将（可能）移动；以及

[0095] 2. 移动节点可以识别（可能的）新接入路由器。

[0096] 此外，有用的是如果旧接入路由器可以检测移动节点实际离开的时刻并且仅在那时激活所请求的隧道。

[0097] 为了能够安全地创建隧道端点，旧接入路由器必须知道如下信息：

[0098] 1. 移动节点的旧转交地址。

[0099] 2. 移动节点的（可能的）新转交地址。

[0100] 3. 没有其它节点可能存在于新转交地址上。

[0101] 4. 移动节点现在或最近出现在旧链路上，使用旧转交地址。前三个属性可以容易地利用 CGA 地址确定。但第四点需要及时性，因此需要状态、时间戳或现时。为避免时间同步化的问题，我们避免使用时间戳。基本协议采用现时，稍后定义如何利用状态来扩大现时提供的保护。

[0102] 为了减少状态需求和抵御重放攻击，接入路由器定期向本地链路广播现时。现时每隔几秒便变更一次。接入路由器必须记住当前的现时和至少一个先前的现时。用于现时生成的精确算法是接入路由器的本地事务。但是，在给定若干现时的任何历史的情况下，必须难于以密码学方法预测将来的现时。

[0103] 为了请求转发隧道，移动节点向旧接入路由器发送消息。该消息必须包含如下数据。

[0104] • 某种形式的旧接入路由器标识。

[0105] • 某种形式的新接入路由器标识。

[0106] • 旧接入路由器接收到的最近的现时。

[0107] • 用于 CGA 验证的旧转交地址。

[0108] • 公钥、CGA 参数和签名

[0109] 旧接入路由器执行如下操作：

[0110] • 检查分组是否正确地标识旧接入路由器。

[0111] • 检查现时足够新。

[0112] • 检查旧转交地址是否具有在旧接入路由器所服务的链路上使用的正确的路由前缀。

[0113] • 检查旧转交地址是否与给定的公钥和 CGA 参数对应。

[0114] • 验证签名。

[0115] 在此过程之后，旧接入路由器获知如下情况：

[0116] • 分组的发送方最近在本地链路上（或至少可以接收旧接入路由器在本地链路上广播的现时），因为该现时是新的。

[0117] • 公钥标识的分组发送方使用过给定的旧转交地址，同时它曾在本地链路上（其概率很高，假定发送方曾首先在该本地链路上）。其它方过去在使用该地址或目前在使用该地址的概率非常小。但是，如果看上去其它方正在使用该地址，则不能建立该隧道。（这是本方案的不确定特性招致的代价。但是，这种冲突的概率几乎可以忽略，而且，对攻击者而言，为所有实际目的都不可能模拟这种冲突。）

[0118] • 除了知道与给定公钥对应的私钥的节点，任何其它方都不可能发送分组，因为签名已经通过验证（而且签名涵盖了现时）。

[0119] • 分组的发送方可能（或至少宣称）现在（或不久）可以在给定的新接入路由器访问。

[0120] 在给定了分组中的信息和通过验证程序建立的确定信息的情况下，旧接入路由器现在可以开始建立转发隧道。为此，它首先必须按如下步骤导出移动节点的（可能的）新转交地址：

[0121] • 在给定消息中携带的新接入路由器标识符的情况下，旧接入路由器确定新链路中节点的路由前缀。旧接入路由器如何确定路由前缀的精确方法超出本文档的范围。

[0122] • 在给定公钥、CGA 参数和新路由选择前缀的情况下，旧接入路由器如上所述计算新的接口标识符。

[0123] • 将路由前缀与接口标识符级联而得到新的（可能的）转交地址。

[0124] • 此时，旧接入路由器知道移动节点的旧转交地址和新转交地址，由此可以建立转发隧道。在基本方案中，仅隐含地建立隧道。该隧道将在一段预设的时间之后终止。在本文档后面描述的一些变型方案中，旧接入路由器发送确认消息。

[0125] 应注意，主动式情况和反应式情况之间没有本质区别。在两种情况中，移动节点向旧接入路由器发送基本相同的信息。但是，可能存在实际的差异。

[0126] 一旦移动节点到达新链路并能够获得新转交地址，则必须准备接收转发的分组。因为它具有它自己的旧转交地址以及旧接入路由器的地址，所以它具有所需的全部信息且可以开始对通过隧道传来的分组进行解封装。如下所述，即使存在地址冲突，任何可能存在的节点会愿意对这些分组进行解封的可能性都非常小。

[0127] 因为旧接入路由器在移动节点到达新链路之前已经可以创建新的转交地址，所以有可能新转交地址不可用。即，当移动节点到达新链路时，某些其它节点已经在使用给定地址。但是，此类事件发生的可能性非常小。实际中，CGA 地址均匀且随机地分布在 2 ^ 59 个不同的值上。因此，给定其上已经有 k 个节点的链路，到达节点获得可用地址的概率为 (1-2

^ -59) ^ k，对于所有 k 个实际值，此概率稍大于 1-k*2 ^ 59。相反地，冲突的概率小于 k*2 ^ 59。例如，对于约 65000 或 2 八 16 个节点的链路，冲突的概率小于 2 ^ 16*2 ^ -59 = 2 ^ -43 = 1.137*10 ^ -13。如果新接入路由器一直在服务 2 ^ 16 个节点，且每隔 1 秒有一个新节点到达（且相应地有一个节点离开），将需要 250,000 年以上才可能有一次冲突。因此，地址冲突将是非常少见的事件。

[0128] CGA 规范定义了一种移动节点能够在已经接受缺省的选择时获取另一个转交地址的方法。但是，如果旧接入路由器已经主动地或自主地建立了转发隧道，则转发的分组被传送到错误的节点。所幸的是，该节点可能以大于 1-2 ^ 59 的概率丢弃该分组，因为接收节点的旧转交地址与到达节点的旧转交地址冲突的概率不仅要求两个节点都从相同链路到达，而且它们在旧链路上还具有相同的转交地址。因此，实际上新链路上发生地址冲突是很少发生的事件。如果这种事件发生，唯一的实际结果是将转发的分组丢弃。

[0129] 新接入路由器在移动节点到达时为它创建邻居高速缓存项。因此，在主动式或自主式转发建立情况中，如果转发的分组在移动节点到达之前到达新接入路由器，则新接入路由器仅通告它已经接收到的目的地为它不具有相应的邻居高速缓存项的地址的分组。在反应式情况中，可能在转发隧道已建立之前有分组到达旧转交地址。在这两种情况中，希望使分组排队一段有限的时间，并尽可能快地转发分组。此外，在这两种情况中，排队分组量受接入路由器上的可用资源数量严格限制。该容量可能受硬件约束，因此无法动态改变。因此，管理排队要解决的问题是确保不对分组进行不必要的排队。一旦处理了这一问题，则无需进一步区分排队的分组，除非采用了明确的 QoS 类。

[0130] 一旦旧接入路由器意识到节点已离开链路但未建立转发隧道，则可以开始对分组进行排队。应该仅使这些分组排队一段有限的时间。排队时间应该根据可用存储空间量和要排队的分组数量改变。实际的排队管理算法属于本地事务。如果节点返回到链路或节点建立了转发隧道，则可以转发这些排队的分组。

[0131] 旧接入路由器可以通过链路层通知、通过 IPv6 邻居不可达性检测 (NLID) 失败或通过某种其它手段来注意到节点已经离开。所有这些情形的特点是：旧接入路由器具有旧转交地址的邻居高速缓存项，以及通过事件告知无法实际将分组传递到移动节点。

[0132] 如果新接入路由器开始将通过隧道传来的分组接收到当前不在其相邻高速缓存中的某个地址，则它可以开始对分组进行排队。在这种情况中，分组可能发往尚未到达链路但可能将到达且开始将该地址用作其转交地址的移动节点。如果新接入路由器具有足够的可用资源，则它可暂时使所有接收到的、但不可递交的分组排队。但是，这种惯例容易遭到拒绝服务攻击，在拒绝服务攻击中，攻击者可能利用假冒的源地址尝试以永远不会被递交的分组来填充可用存储空间。因此，新接入路由器应该基于排队的分组实际由信任的旧接入路由器发送的概率来将它们分类。

[0133] 新接入路由器可采用多种方式来将分组分类。至少有下列可能性可用：

[0134] • 新接入路由器可以决定赋予含有隧道首部的分组优先权。

[0135] • 新接入路由器可以检查隧道首部中的源地址，如果源地址属于已知的旧接入路由器，则赋予分组优先权。此方法在如下条件下可被增强：如果可能这样构造网络，使得外来者不可能发送含有假冒的属于旧接入路由器的源地址的 IP 分组。

[0136] • 如果新接入路由器和已知的旧接入路由器共享 IPSec 安全关联 (security

association)，则新接入路由器可以赋予利用这种安全关联得到保护的分组优先权。

[0137] • 在开始发送隧道传送的分组之前，旧接入路由器可以转发它接收到的转发建立消息，以及新接入路由器可以如下所述验证该消息，并创建临时“将来”的邻居高速缓存项。然后它就可以赋予具有这种临时的“将来”的邻居高速缓存项的目的地地址优先权。

[0138] 乍看似乎合乎需要的是明确知道可能在不久的将来到达链路的移动节点。现在定义一种允许新接入路由器建立这种状态的方法。

[0139] 一旦旧接入路由器完成对转发建立消息的检查，它就可以将该消息转发到新接入路由器。如果它这样做，则它应该首先转发该分组，然后才传递隧道传送的分组。当新接入路由器接收到这种传递的转发建立消息时，它应该按如下步骤验证该消息：

[0140] • 例如基于源地址 (+ 依靠如上所述的输入过滤)、基于利用 IPSec 保护的消息或通过某种其它方法来检查该消息是否是由已知旧接入路由器发送的。

[0141] •如果可能，新接入路由器应该检查该消息是否是新的（即不是重放的消息）。这是否可能主要取决于旧接入路由器中继该消息的方式。例如，如果该消息采用 IPSec 保护，则 IPSec 序号保护足以保证（除旧接入路由器可能外）无任何方已重放该消息。

[0142] •如果旧链路上使用的路由前缀是已知的（基于旧接入路由器标识），则它检查此路由前缀是否与旧转交地址中的路由前缀匹配。

[0143] • 它检查旧转交地址是否与转发的消息中的公钥和 CGA 参数对应。

[0144] • 它可选地对签名进行验证。

[0145] 应该注意，此方法需要资源，并且仅在无法完全信任旧接入路由器的情况下才会加强保护，因为不可能基于隧道源地址来实现可靠的分组分类（因为缺乏输入过滤），或者因为移动节点在某种程度上是已知的，比旧接入路由器更可信。如果仅当存在可能出现在新链路上的移动节点时才相信旧接入路由器已发送隧道传送的分组，则第一个这种隧道传送的分组隐含地包含了可能有更多这种分组到达且移动节点可能出现的指示。但是此类隧道传送的消息不包含 CGA 参数或签名。因此，此方法提供的附加保护受到限制。

[0146] 仅 CGA 不会增加多少价值，因为任何一方都可以创建新的 CGA 地址。同样地，签名仅使人相信移动节点（通过公钥识别的）（以前）曾打算从旧接入链路移动到新链路。但是，签名不增加任何价值，除非移动节点在某种程度上比旧接入路由器更可信，或者除非移动节点和旧接入路由器的联合声明被视为比仅旧接入路由器的声明更有价值。

[0147] 总之，传递转发建立消息并利用它们来控制新接入路由器上排队资源的资源分配的价值取决于确切的信任模型和基础安全性假设。

[0148] 基本协议仅使用一个消息，移动节点以主动方式或反应方式发送转发建立消息到旧接入路由器。该消息包括 IPv6 首部、公钥保护的 IPSec AH 首部和新的 ICMP 消息，如图 4 所示。AH 首部包含公钥、签名和 CGA 参数。注意，如上所述，分组的源地址可以是旧转交地址，也可以是新转交地址。在任何一种情况下，CGA 签名和参数都是有效的。

[0149] 新的 ICMP 转发隧道建立消息含有现时、新接入路由器的标识和旧转交地址。在主动式情况中，此地址必须与源地址完全相同。在反应式情况中，源地址为新转交地址。新 ICMP 消息的内容如图 5 所示。

[0150] IP 字段如下：

[0151] 源地址：移动节点的旧转交地址或新转交地址。

[0152] 属于旧接入路由器的地址。

[0153] ICMP 字段 :类型

[0154] TBD :要由 IANA 分配以用于转发建立。

[0155] 代码 :0

[0156] 校验和 :ICMP 校验和

[0157] 标识符 :16 位无符号整数,是用于帮助匹配转发建立消息和确认的标识符,如下进一步所述。

[0158] 保留 :未用。它必须被发送方初始化为零,以及必须被接收器忽略。

[0159] 强制性选项 :

[0160] 现时 :现时选项,如 [Arkko, J., " SEcure NeighborDiscovery(SEND) ", draft-ietf-send-ipsec-00(work inprogress),February2003] 中定义。

[0161] 接入路由器标识 :用于标识新接入路由器。TBD。

[0162] 其它选项 :

[0163] 转交地址 :包含移动节点的旧转交地址。TBD。

[0164] 此选项必须用于反应式情况中。

[0165] 证书 :证书选项,如 [Arkko, J., " SEcure NeighborDiscovery(SEND) ", draft-ietf-send-ipsec-00(work inprogress),February2003] 中定义。

[0166] 现在讨论主动式移动节点,这种移动节点执行如下操作 :

[0167] •监听旧接入路由器广播的现时。合乎逻辑的是将现时包含在路由器通告消息中。

[0168] •检测它 (即移动节点) 是否可能在不久的将来移动到新接入路由器,并确定该接入路由器的 (可能的) 标识。

[0169] • 创建 ICMP 转发隧道建立消息,将当前转交地址用作源地址和将旧接入路由器的 IP 地址用作目的地地址,包含新的消息标识号、最近接收到的现时和 (可能的) 新接入路由器的标识。

[0170] •将该消息封装在 AH 首部中,包含移动节点的公钥、所用的 CGA 参数以及对所有分组的签名。

[0171] • 将该消息发送到旧接入路由器。

[0172] 一旦移动节点检测到它的确已经移动,且假定新转交地址是缺省地址,则它开始接受来自旧接入路由器的转发分组。

[0173] 在反应式移动节点的情况中,该移动节点执行如下操作 :

[0174] •监听接入路由器广播的现时。同样,合乎逻辑的是将现时包含在路由器通告消息中。

[0175] • 检测它是否已经移动到新接入路由器。

[0176] • 创建 ICMP 转发隧道建立消息,将当前转交地址用作源地址和将旧接入路由器的 IP 地址用作目的地地址,包含新的消息标识号、最近接收到的现时以及新接入路由器的标识 (路由前缀) 和旧转交地址。

[0177] •将该消息封装在 AH 首部中,包含移动节点的公钥、所用的 CGA 参数以及对所有分组的签名。

[0178] • 将该消息发送到旧接入路由器。

[0179] • 开始接受来自旧接入路由器的转发分组。

[0180] 旧接入路由器具有两个独立的功能：分组排队和转发创建。分组仅在转发隧道建立之前进行排队。

[0181] 如果旧接入路由器检测到移动节点已经变得不可达而未创建转发隧道，则它开始对发往旧转交地址的分组进行排队（如果资源允许的话）。排队的分组应该只保持有限时间。最长排队时间是一个配置选项，其值不应该超过 10 秒。如果可用资源少于使所有分组排队最长时间所需的资源，则路由器可以将排队的分组丢弃。丢弃算法是本地实现选项。

[0182] 当旧接入路由器接收到 ICMP 转发隧道建立消息时，它首先以某种实现相关的顺序执行如下操作：

[0183] • 检查消息的目的地是否为正确的节点。这通常由 IP 层自动执行。

[0184] • 检查 ICMP 选项中的现时是否是新的，即最近广播的或紧靠最近广播的之前的。否则，它默默地将该消息丢弃。

[0185] • 从 IP 首部中的源地址字段或从 ICMP 旧转交地址选项中提取旧转交地址。

[0186] •检查旧转交地址中的路由前缀是否与旧链路中所用的路由前缀匹配。否则，它默默地将该消息丢弃。

[0187] •检查是否存在该旧转交地址的邻居高速缓存项。如果没有这种邻居高速缓存项，则过程继续到下一步骤。如果存在这种缓存项且该消息是从旧转交地址接收的，则它可选地验证源 MAC 地址是否与邻居高速缓存项中的 MAC 地址匹配。如果不匹配，则它丢弃该分组。如果该消息是从某个其它 IP 地址接收到的，则它触发针对该邻居高速缓存项中所述节点的邻居不可达性检测 (NUD)。如果 NUD 显示该节点是不可达的，则过程继续；否则丢弃该消息。

[0188] •验证旧转交地址是否是由公钥和 CGA 参数正确构造的。在主动式情况中，此步骤可以作为 AH 处理的一部分来执行。如果验证失败，则默默地将该消息丢弃。

[0189] • 验证签名。在主动式情况中，此步骤通常作为 AH 处理的一部分来执行。如果验证失败，则默默地将该消息丢弃。

[0190] • 验证新接入路由器的给定标识是有效的标识。此步骤的目的是要保护无辜的网络，使其不受恶意移动节点创建其另一端点为伪造端点的转发隧道的攻击。

[0191] 注意，这些操作的执行顺序可随实现方式不同而有所不同。但是，相信以上顺序比许多其它可能的顺序更能抗拒绝服务攻击。

[0192] 验证这些消息之后，接入路由器如下启动转发：

[0193] • 利用新接入路由器的路由前缀、移动节点的公钥和 CGA 参数来计算新转交地址。

[0194] •如果未从旧转交地址接收到 ICMP 转发隧道建立消息，则检查该消息中的 IP 源地址是否与计算的新转交地址匹配。否则，将该消息丢弃，并记录警告且不创建隧道。

[0195] • 如果从旧转交地址接收到 ICMP 转发隧道建立消息，则它可选地等待移动节点变成不可达。

[0196] • 启动转发所有目的地地址为旧转交地址的分组。它将此类分组封装在隧道首部中，其源地址是旧接入路由器的 IP 地址，目的地地址是新转交地址，将这些分组传回有线网络，以便交付给新接入路由器。如果存在任何目的地为旧转交地址的排队的分组，则它首先传送这些分组。

[0197] • 同时，它开始转发外部源地址为新转交地址且目的地地址为旧接入路由器的隧道传送的分组。当将这些分组解封装时，旧接入路由器必须验证其内部源地址是否与旧转交地址匹配。这有效地创建了反向隧道，从而允许移动节点发送含有它的旧转交地址的分组。

[0198] 在主动式情况中，新接入路由器除了它的这些正常操作外，唯一需要做的是排队。除此之外，新接入路由器充当如前一样的接入路由器。但要注意，大多数接入路由器常常同时充当旧接入路由器和新接入路由器的角色。这在实现中必须加以留意。

[0199] 新接入路由器可以在接收到目的地为不具有邻居高速缓存项的某个本地地址的转发分组时启动排队。更具体地说，新接入路由器如下动作：

[0200] 当接入路由器从有线网络接收到分组时，它检查它的邻居高速缓存，如果存在对应于目的地地址的邻居高速缓存项，则它递送该分组。

[0201] 如果不存在对应的邻居高速缓存项，则接入路由器启动 RFC2461 中定义的邻居发现过程。

[0202] 如果接入路由器拥有可用于排队分组的资源，则接入路由器接着更仔细地检查该分组，并基于其首部对其进行分类。虽然确切的分类准则是实现特定的，但建议采用如下准则：

[0203] • 如果分组是转发的分组，且外部源地址属于已知的（且受信任的）接入路由器，则赋予该分组较其它情况高的排队优先权。

[0204] •如果隧道首部受到完整性保护（例如 ESP 隧道模式），则赋予该分组比隧道首部不受完整性保护的情况高的排队优先权。

[0205] •任何排队的分组不久后都应该丢弃。最长排队时间是一个配置参数，其值不应该超过 10 秒。

[0206] • 如果可用资源少于使所有接收到的分组排队上述最长时间所需的资源，则除了丢弃一些分组外别无选择。丢弃算法是一个本地实现选项。

[0207] • 如果创建了新邻居高速缓存项，则检查队列以查看是否存在目的地为该地址的任何分组。如果存在，则立即递送排队的分组。

[0208] 在此部分，我们简要地描述基本方法的一些变型。这些变型通过解释它们与基本方法的不同来描述。

[0209] • 采用证书来替代 CGA

[0210] 可能有用的是采用证书来替代CGA。在此情况中，所有参与的接入路由器必须具有签发证书的公共的可信第三方（或一组这样的可信方）。每个移动节点必须具有一个这样的证书，且证书必须包含移动节点的公钥和接口标识符。例如，网络接口卡可以包含制造商签发的对应于该卡的 MAC 地址密钥对和证书。在此方法中，并不根据 CGA 动态计算接口标识符，接口标识符是静态。通过简单地将路由前缀与证书提供的接口标识符级联，从而形成转交地址。但是，出于保密的目的，还可以将路由前缀与原始接口标识符的某种加密导出信息用作接口标识符。例如，可以对路由前缀和原始接口标识符计算散列函数，然后将来自该散列函数结果的若干比特用作实际的接口标识符。

[0211] 移动节点并不在 AH 首部中传递 CGA 参数，而是必须将证书作为 ICMP 选项来传递。而且，旧接入路由器并不验证地址是否与公钥和 CGA 参数匹配，而是验证接口标识符是否

与证书中给定的地址匹配。此外，旧接入路由器必须验证证书中的签名并确保该证书签发者在此场合中是可信的。

[0212] • 向若干新链路转发分组

[0213] 旧接入路由器并不主动地将分组转发到最可能的新接入路由器，而是可以通过隧道同时将分组传送到若干可能的新接入路由器。这是可能的，条件是例如接入路由器共享拓朴和地理信息，从而允许它们“猜测”移动节点可能到达的最可能的附近的接入路由器。必须注意，此方法使用多于其它方法的资源，因为旧接入路由器将创建分组的多个副本，并且分组将在若干可能的新接入路由器上通过隧道传送。此方法可通过如下方式增强：移动节点一旦到达实际的新链路，则发送反应式转发隧道建立消息，从而允许旧接入路由器停止向除实际的新接入路由器之外的所有接入路由器转发分组。

[0214] • 自主式转发建立

[0215] 如果旧接入路由器能够检测移动节点何时离开，则由旧接入路由器建立自主式隧道是可能的，且旧接入路由器能够以较高概率猜测移动节点将要使用的（一个或多个）可能的新接入路由器。在自主式转发建立中，CGA 地址和证书通常都不需要。对接入路由器而言，共享安全关联就足够了。如资源允许的话，则旧接入路由器可以利用一组而非一个可能的新接入路由器，并开始向所有这些接入路由器转发分组。但是，这会占用多于其它方式所需的资源。

[0216] • 在排队时支持显式 QoS 类

[0217] 在基本方法中，建议同等地地使各分组排队，可能的例外是：由新接入路由器基于它们所具有的隧道首部的类型来对分组分类。但是，有可能对分组应用服务质量分类法，并适当地调整排队算法。

[0218] • 在新接入路由器上将隧道首部解封装

[0219] 有可能通过在新接入路由器上移除隧道首部而在新接入路由器上增强接入链路性能。新接入路由器会仅将分组发送到移动节点的 MAC 地址，但仍然将旧转交地址作为源地址保留。

[0220] • 各种确认消息

[0221] 在基本方法中，移动节点简单地发送 ICMP 转发隧道建立消息。没有确认消息。其原因有二。其一，它使该方法保持简单。其二，在主动式情况中，移动节点在移动之前能够接收到确认是不可能的，而在反应式情况中，开始接收转发的消息充当隐含的确认。因此，从实际的角度来看，添加确认不会为协议增加多少价值。但是，在协议中增加确认消息的确有可能。ICMP 消息中的消息标识符字段允许确认与转发隧道建立请求彼此匹配。我们看不出要显式保护确认的任何理由，因为它们仅是信息性质的，即它们不创建任何实际的状态。

[0222] • 在反应式情况中将旧转交地址用作源地址

[0223] 在基本方法中，反应式 ICMP 转发隧道建立消息将新转交地址用作 IP 首部中的源地址。但是，如果甚至在反应式情况中，网络也允许移动节点使用旧转交地址，则会简化旧接入路由器上的处理操作。从技术上说，不能使用旧转交地址是没有道理的；问题完全在于，网络中可能的源地址过滤器是否会沿路将分组从新链路传送到旧接入路由器。

[0224] • 利用主机标识协议 (HIP) 条件下的简化

[0225] 如果上述方法与主机标识协议 (HIP) 一起使用，则隧道首部可以简单的 IP 地址重

写来代替。即，将 IP 首部中的目的地字段中的旧转交地址简单地替换为新转交地址。因为 HIP 在上层校验和中采用 HIT 来替换 IP 地址，因此该替换操作不会影响上层协议。但是，新接入路由器可能需要更加注意其排队分类算法。

[0226] 存在一种本方法可能获得非最优性能的情况。如果移动节点执行主动式转发隧道创建，则在新接入路由器对隧道传送的分组排队。这基于如下假设：一旦移动节点到达新链路，这会导致更快的分组递送。但是，有可能新接入路由器的可供支配的排队资源根本没有或比旧接入路由器少。在这种特定情况下，如果在旧接入路由器上而不是在新接入路由器上对分组排队，可能会得到更好的性能。但是，将此方案包括在本方法中将是一个在少有的情况中提高性能的工程解决方案，其代价是高得多的复杂性和状态需求。

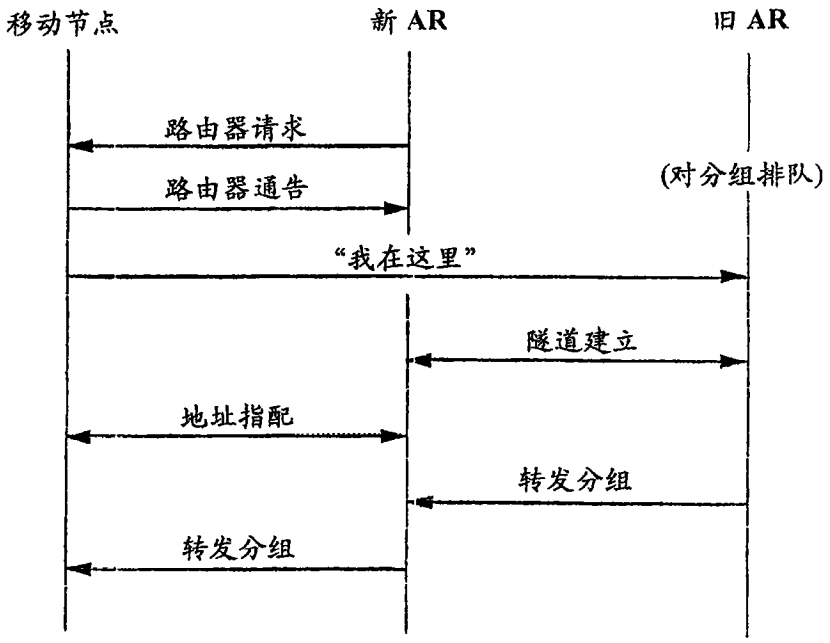

移动节点
新 AR
旧 AR
路由器请求
路由器通告
(对分组排队)
“我在这里”
隧道建立
地址指配
转发分组
转发分组

图 1

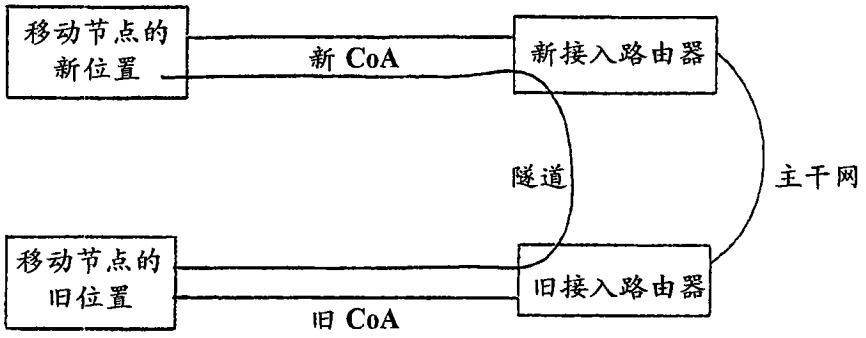

移动节点的
新位置
新 CoA
新接入路由器
隧道
主干网
移动节点的
旧位置
旧接入路由器
旧 CoA

图 2

IP 首部 src = CN dst = old-CoA	上层首部和数据

IP 首部 src = old-AR dst = new-CoA	IP 首部 src = CN dst = old-CoA	上层首部和数据

图 3

IPv6 首部	AH 首部	ICMPv6 首部	新消息特定数据	ICPM 消息选项

图 4

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

类型	代码	校验和
标识符		保留
选项.....		

图 5