[19] 中华人民共和国国家知识产权局

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

[12] 发明专利说明书

专利号 ZL 200610160964.8

[45] 授权公告日 2010 年 1 月 20 日

[11] 授权公告号 CN 100583745C

[22] 申请日 2006.12.6
[21] 申请号 200610160964.8
[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 万长胜
[56] 参考文献
CN1859087A 2006.11.8
CN1510879A 2004.7.7
US2006/0251022A1 2006.11.9
JP2006-246073A 2006.9.14
CN1543118A 2004.11.3
审查员 杨 颖

[74] 专利代理机构 北京三高永信知识产权代理有限责任公司
代理人 何文彬

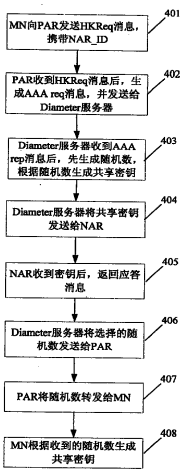
权利要求书 3 页 说明书 6 页 附图 4 页

[54] 发明名称

一种基于 Diameter 服务器的密钥生成与分发方法及系统

[57] 摘要

本发明提供了一种基于 Diameter 服务器的密钥生成与分发方法及系统，属于移动通信领域。为了解决现有技术中移动节点的密钥分发不安全及费用高的问题，本发明提供了一种基于 Diameter 服务器的密钥生成与分发方法，包括：MN 将 NAR 的标识发送给 PAR，PAR 收到后，将 NAR 的标识和 MN 的标识发送给 Diameter 服务器，Diameter 服务器收到标识后，先生成随机数，根据随机数生成共享密钥，并将共享密钥发送给 NAR，将随机数发送给 MN，MN 收到随机数后，生成共享密钥。本发明还提供了一种基于 Diameter 服务器的密钥生成与分发系统。采用本发明的技术方案避免了多米诺骨牌效应，增强了共享密钥的安全性。



1. 一种基于 Diameter 服务器的密钥生成与分发方法，其特征在于，所述方法包括以下步骤：

步骤 A：移动节点将后接入路由器的标识发送给前接入路由器；

步骤 B：所述前接入路由器收到所述后接入路由器的标识后，将所述后接入路由器的标识和所述移动节点的标识发送给 Diameter 服务器；

步骤 C：所述 Diameter 服务器收到标识后，生成一个随机数，根据所述随机数生成所述移动节点与后接入路由器间的共享密钥，将所述共享密钥发送给后接入路由器，并通过所述前接入路由器将所述随机数发送给移动节点；

步骤 D：所述移动节点收到所述随机数后，生成所述移动节点与后接入路由器间的共享密钥。

2. 如权利要求 1 所述的基于 Diameter 服务器的密钥生成与分发方法，其特征在于，所述后接入路由器的标识为后接入路由器的 IP 地址。

3. 如权利要求 1 所述的基于 Diameter 服务器的密钥生成与分发方法，其特征在于，所述移动节点的标识为移动节点接入标识符。

4. 如权利要求 1 所述的基于 Diameter 服务器的密钥生成与分发方法，其特征在于，所述 Diameter 服务器与所述后接入路由器之间有安全联盟。

5. 如权利要求 1 所述的基于 Diameter 服务器的密钥生成与分发方法，其特征在于，所述步骤 D 中的生成所述移动节点与后接入路由器间的共享密钥在移动节点移动到后接入路由器之前进行。

6. 如权利要求 1 所述的基于 Diameter 服务器的密钥生成与分发方法，其特征在于，所述步骤 C 和步骤 D 中的生成所述移动节点与后接入路由器间的共享密钥使用的函数为伪随机生成函数。

7. 如权利要求 1 所述的基于 Diameter 服务器的密钥生成与分发方法，其特征在于，所述步骤 C 和步骤 D 中的生成所述移动节点与后接入路由器间的共享密钥的公式具体为：

共享密钥 = PRF（AAA 服务器与移动节点间的共享密钥，随机数|后接入路由器标识|AAA 服务器标识|移动节点标识|密钥有效期），其中，PRF 是一个伪随机生成函数。

8. 一种基于 Diameter 服务器的密钥生成与分发系统，其特征在于，所述系统包括移动节点、前接入路由器、后接入路由器和 Diameter 服务器，

所述移动节点包括：

发送模块，用于将后接入路由器的标识发送给前接入路由器；

密钥生成模块，用于接收所述前接入路由器发送的随机数，并根据所述随机数生成所述移动节点与后接入路由器间的共享密钥；

所述前接入路由器包括：

接收与发送模块，用于接收所述移动节点发送的后接入路由器的标识，并将 Diameter 服务器发送的随机数发送给所述移动节点，以及将所述后接入路由器的标识和所述移动节点的标识发送给 Diameter 服务器；

所述 Diameter 服务器包括：

Diameter 密钥生成模块，用于生成一个随机数，根据所述随机数生成所述移动节点与后接入路由器间的共享密钥；

发送模块，用于将所述共享密钥发送给后接入路由器，并通过所述前接入路由器将所述随机数发送给移动节点；

所述后接入路由器包括：

接收与应答模块，用于接收所述 Diameter 服务器发送的共享密钥及向所述 Diameter 服务器发送已收到应答消息。

9. 如权利要求 8 所述的基于 Diameter 服务器的密钥生成与分发系统，其特征在于， 所述 Diameter 服务器还包括：

密钥计算单元，用于 Diameter 服务器根据公式：共享密钥 = PRF（AAA 服务器与移动节点间的共享密钥，随机数|后接入路由器标识|AAA 服务器标识|移动节点标识|密钥有效期）计算所述移动节点与后接入路由器间的共享密钥，其中，PRF 是一个伪随机生成函数；

相应地，所述移动节点还包括：密钥计算单元，用于移动节点根据公式：共享密钥 =PRF

(AAA服务器与移动节点间的共享密钥，随机数|后接入路由器标识|AAA服务器标识|移动节点标识|密钥有效期)计算所述移动节点与后接入路由器间的共享密钥。

一种基于 Diameter 服务器的密钥生成与分发方法及系统

技术领域

本发明涉及移动通信领域，特别涉及一种基于 Diameter 服务器的密钥生成与分发方法及系统。

背景技术

MIP6协议提供了一种允许移动节点在IPv6网络中漫游时仍能使用家乡IP地址通讯的方法。它要求移动节点移动到外地网络时向家乡代理注册转交地址。当移动节点从一个外地接入路由器切换到另外一个路由器时，需要重新获得COA(Care-Of Address，转交地址)，并向家乡代理注册。MIP6基本协议中的解决办法是在移动节点移动到新接入路由器后才获得新的COA。

MIP6基本协议有如下问题：

(1) 移动节点在移动到新的路由器后才获得COA，在移动节点获得新的COA之前移动节点与通讯节点的通讯会中断。从而导致很大的切换时延。

(2) 移动节点在切换到新的路由器后，向家乡代理注册新的COA之前的这段时间，发往移动节点的数据包仍然会发往移动节点的旧COA。由于旧COA不再可用，发往移动节点的数据包将被丢弃。

FMIP6协议扩展了MIP6基础协议，解决了MIP6协议的这两个问题。FMIP6协议提供了在移动节点移动到新的路由器之前，向新接入路由器获得COA的方法。减少了通讯时延。FMIP6协议还在前接入路由器和移动节点之间建立隧道。发往旧的COA的数据将通过隧道发往移动节点。

为了保证前接入路由器与移动节点间数据传输的安全，前接入路由器和移动节点之间必须建立安全联盟。建立安全联盟的关键是在前接入路由器和MN（Mobile Node，移动节点）之间分发共享密钥。

现有技术中提供了一种切换密钥的分发方法。参见图 1，该方法包括以下步骤：

步骤 101：MN 向 NAR（New access router，后接入路由器）发送 HKReq（Handover Key Request，切换密钥请求消息），请求 NAR-MN 密钥。

步骤 102：NAR 收到 HKReq 后，向 PAR（Previous access router，前接入路由器）发送 HKReq 消息，请求切换密钥的根密钥。

步骤 103：PAR 发送 HKResp（Handover Key Response，切换密钥应答消息），把切换的根密钥发送给 NAR。

步骤 104：NAR 根据根密钥生成 NAR-MN 密钥，发送 HKResp 给 MN。

其中 HKReq 和 HKResp 消息可以是 MIP6 的一个子选项，可以嵌在 FMIP6 消息或 MIP6 消息中发往 NAR。

上述方法中的信令可以带在FMIP6协议的信令中传输。此时，其密钥分发信令数据是FMIP6信令数据的一部分。上述方法同时提供了预切换模式和反应模式中的密钥分发信令传输模式。

参见图2，现有技术提供了一种预切换模式的密钥分发方法，该方法包括以下步骤：

步骤201：MN将发往NAR的HKReq消息附带在FBU（Fast Binding Update，快速绑定更新消息）中发给PAR。请求PAR把发往MN的数据转发给NAR。

步骤202：PAR在向NAR发送HI（Handover Initiate，切换发起）消息时，把HKReq消息带给NAR。

步骤203：NAR收到HKReq消息后，向PAR发送FBack（Fast Binding Acknowledgement，快速绑定应答消息），并把HKResp消息返回给PAR。

步骤204：PAR收到HKResp消息后，再把HKResp消息发送给MN。

参见图3，现有技术提供了一种反应模式的密钥分发方法，该方法包括以下步骤：

步骤301：MN向NAR发送的HKReq信息，并附带在FNA（Fast Neighbor Advertisement，快速邻居通告）消息中，向NAR通告自己开始使用新的转交地址。

步骤302：NAR收到HKReq消息后向PAR发送FBU消息，其中包括HKReq消息。

步骤303：PAR收到HKReq消息后，发送HKResp消息给NAR。

步骤304：NAR收到HKResp消息后，再发送HKResp消息给MN。

现有技术存在如下问题：

多米诺骨牌效应：多米诺骨牌效应是指放在一起的骨牌，一旦其中一个倒下了，将会影响其他的骨牌，从而使所有的骨牌都倒下。NAR从PAR获得切换根密钥会导致多米诺骨牌效应。一旦域内某一个AR被攻破，MN经过该AR后的切换密钥将很容易被获取；

部署代价昂贵：PAR负责认证意味着所有的AR都需要具有认证功能。部署这种网络代价非常昂贵。

发明内容

本发明实施例为了增加密钥进行切换时的安全性及缓解网络部署代价昂贵的问题，提供了一种基于 Diameter 服务器的密钥生成与分发方法及系统。所述技术方案如下：

一种基于 Diameter 服务器的密钥生成与分发方法，所述方法包括以下步骤：

步骤 A：移动节点将后接入路由器的标识发送给前接入路由器；

步骤 B：所述前接入路由器收到所述后接入路由器的标识后，将所述后接入路由器的标识和所述移动节点的标识发送给 Diameter 服务器；

步骤 C：所述 Diameter 服务器收到标识后，生成一个随机数，根据所述随机数生成所述移动节点与后接入路由器间的共享密钥，将所述共享密钥发送给后接入路由器，并通过所述前接入路由器将所述随机数发送给移动节点；

步骤 D：所述移动节点收到所述随机数后，生成所述移动节点与后接入路由器间的共享密钥。

本发明实施例还提供了一种基于 Diameter 服务器的密钥生成与分发系统，所述系统包括移动节点、前接入路由器、后接入路由器和 Diameter 服务器，

所述移动节点包括：

发送模块，用于移动节点将后接入路由器的标识发送给前接入路由器；

密钥生成模块，用于接收所述前接入路由器发送的随机数，并根据所述随机数生成所述移动节点与后接入路由器间的共享密钥；

所述前接入路由器包括：

接收与发送模块，用于接收所述移动节点发送的后接入路由器的标识，并将 Diameter 服务器发送的随机数发送给所述移动节点，以及将所述后接入路由器的标识和所述移动节点的标识发送给 Diameter 服务器；

所述 Diameter 服务器包括：

密钥生成模块，用于所述 Diameter 服务器收到标识后，选择一个随机数，根据所述随机数生成所述移动节点与后接入路由器间的共享密钥；

发送模块，用于将所述共享密钥发送给后接入路由器，并通过所述前接入路由器将所述随机数发送给移动节点；

所述后接入路由器包括：

接收与应答模块，用于接收所述 Diameter 服务器发送的共享密钥及向所述 Diameter 服务器发送已收到应答消息。

本发明实施例的技术方案带来的有益效果是：

避免了现有技术中的多米诺骨牌效应问题：由于 MN 和 NAR 之间的共享密钥的产生不再依赖于 PAR，一旦 PAR 被攻破，NAR 与 MN 之间的密钥分发不会受到影响；

本方案中 Diameter 服务器不直接发送密钥给 MN 而是发送随机数，由 MN 自己计算共享密钥，防止了该共享密钥被 PAR 获得。

同时，本发明实施例不需要 PAR 进行认证，因此降低了网络部署的费用。

附图说明

图 1 是现有技术中切换密钥的分发方法的信令传输示意图；

图 2 是现有技术中预切换模式的密钥分发方法流程图；

图 3 是现有技术中反应模式的密钥分发方法流程图；

图 4 是本发明实施例提供的密钥生成与分发方法流程图；

图 5 是本发明实施例提供的密钥生成与分发系统的示意图。

具体实施方式

下面结合附图和具体实施例对本发明作进一步说明，但本发明不局限于以下实施例。

本发明实施例提供了一种基于 Diameter 服务器的密钥生成与分发方法及系统，在 MN 移动到下一个路由器之前，由 Diameter 服务器向 MN 和 NAR 分发密钥，该密钥在 NAR 成为 PAR 时使用。

参见图 4，一种基于 Diameter 服务器的密钥生成与分发方法，该方法包括以下步骤：

步骤 401：MN 发送 HKReq 给 PAR，HKReq 中包含 NAR_ID 信息。NAR_ID 是后接入路由器的标识，可以是后接入路由器的 IP 地址。

步骤 402：PAR 收到 HKReq 后对 HKReq 信息进行解析，生成 AAA req 消息，并把 AAA req 消息发送给 Diameter 服务器。

其中，AAA req 消息是 PAR 发送给 Diameter 服务器的请求分配切换密钥的 Diameter 消息。它包含 NAR_ID 和 MN_ID。其中，MN_ID 是移动节点的标识，通常是移动节点接入标识符，其形式如下：mn@home.net。

步骤 403：Diameter 服务器收到 AAA req 消息后，生成一个随机数 nonce，并把 nonce，NAR_ID， AAA_ID，MN_ID，validity time，AAA-MN-Key 作为输入，利用 PRF 函数生成共享密钥 NAR-MN-Key。

其中，nonce 是一个随机数；AAA_ID 是 AAA 服务器的标识，通常是 AAA 服务器的 IP 地址；validity time 是密钥的有效期；PRF 函数是一个伪随机生成函数，根据 PRF 函数的输出很难推出 PRF 函数的输入；AAA-MN-Key 为 AAA 与 MN 间的共享密钥；NAR-MN-Key 是本发明需要生成的后接入路由器和移动节点之间的共享密钥。

共享密钥的具体计算公式为：

NAR-MN-Key = PRF (AAA-MN-Key, nonce|NAR_ID|AAA_ID|MN_ID| validity time)。

步骤 404：Diameter 服务器把 NAR-MN-Key 通过 AAA req 消息发送给 NAR。

步骤 405：NAR 收到 AAA req 消息后，向 Diameter 服务器返回应答消息。

步骤 406：Diameter 服务器收到 NAR 的应答消息后，向 PAR 返回携带 nonce 的应答消息。

步骤 407：PAR 收到 Diameter 服务器的应答消息后，把来自 AAA 服务器的 nonce 通过应答消息发送给 MN。

步骤 408：MN 根据 nonce 计算得出共享密钥 NAR-MN-Key。同上，共享密钥的具体计算公式为：

NAR-MN-Key = PRF (AAA-MN-Key, nonce|NAR_ID|AAA_ID|MN_ID| validity time)。

本发明实施例提供的密钥生成与分发方案的安全性主要体现在以下方面：

因为在步骤 402 中 PAR 不产生密钥，而是通过后面的步骤由 Diameter 服务器产生密钥，这样即使 PAR 被攻破，也不会影响 NAR 与 MN 之间的共享密钥，防止了多米诺骨牌效应的产生。

在步骤 406、407、408 中，Diameter 服务器把 nonce 值通过 PAR 传给 MN，这样 PAR 只知道 nonce，无法计算出密钥 NAR-MN-Key，保证密钥 NAR-MN-Key 不被泄漏给 PAR。

由于 Diameter 服务器与 NAR 之间有安全联盟，两者之间直接分发密钥是安全的。

另外，本发明中的 AR 需要支持 Diameter client，因为 AR 通常都需要支持接入认证功能。在 MN 移动到 NAR 之前，生成切换密钥，这样可以解决 MN 快速移动的问题。

参见图 5，本发明还提供了一种基于 Diameter 服务器的密钥生成与分发系统，包括移动节点、前接入路由器、后接入路由器和 Diameter 服务器；

其中，移动节点包括：

发送模块，用于将后接入路由器的标识发送给前接入路由器；

密钥生成模块，用于接收前接入路由器发送的随机数，并根据随机数生成移动节点与后接入路由器间的共享密钥；

前接入路由器包括：

接收与发送模块，用于接收移动节点发送的后接入路由器的标识，并将 Diameter 服务器发送的随机数发送给移动节点，以及将后接入路由器的标识和移动节点的标识发送给 Diameter 服务器；

Diameter 服务器包括：

Diameter 密钥生成模块，用于生成一个随机数，根据随机数生成移动节点与后接入路由器间的共享密钥；

发送模块，用于将共享密钥发送给后接入路由器，并通过前接入路由器将随机数发送给移动节点；

后接入路由器包括：

接收与应答模块，用于接收 Diameter 服务器发送的共享密钥及向 Diameter 服务器发送已收到应答消息。

为了提高安全性，该 Diameter 服务器还包括：

密钥计算单元，用于 Diameter 服务器根据公式：共享密钥 = PRF（服务器与移动节点间的共享密钥，随机数|后接入路由器标识|AAA 服务器标识|移动节点标识|密钥有效期）计算移动节点与后接入路由器间的共享密钥；

相应地，移动节点还包括：

密钥计算单元，用于移动节点根据公式：共享密钥 = PRF（服务器与移动节点间的共享密钥，随机数|后接入路由器标识|AAA 服务器标识|移动节点标识|密钥有效期）计算移动节点与后接入路由器间的共享密钥。

以上所述的实施例，只是本发明较优选的具体实施方式的一种，本领域的技术人员在本发明技术方案范围内进行的通常变化和替换都应包含在本发明的保护范围内。

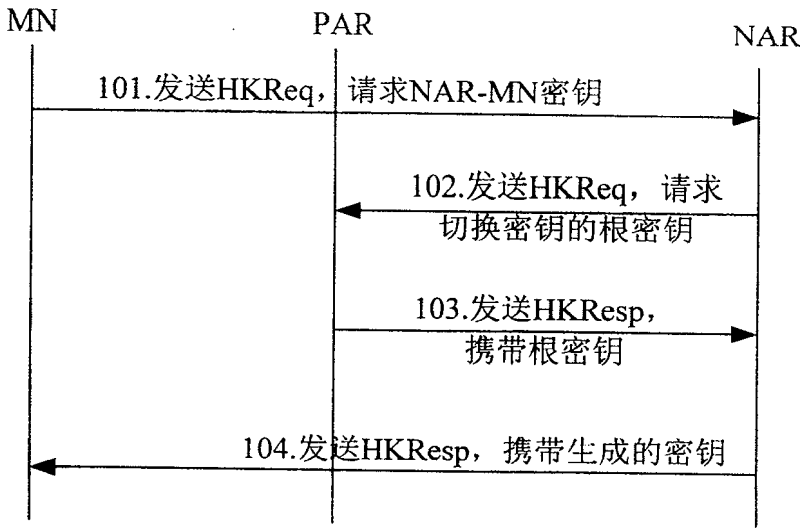

MN
PAR
NAR
101.发送HKReq，请求NAR-MN密钥
102.发送HKReq，请求切换密钥的根密钥
103.发送HKResp，携带根密钥
104.发送HKResp，携带生成的密钥

图 1

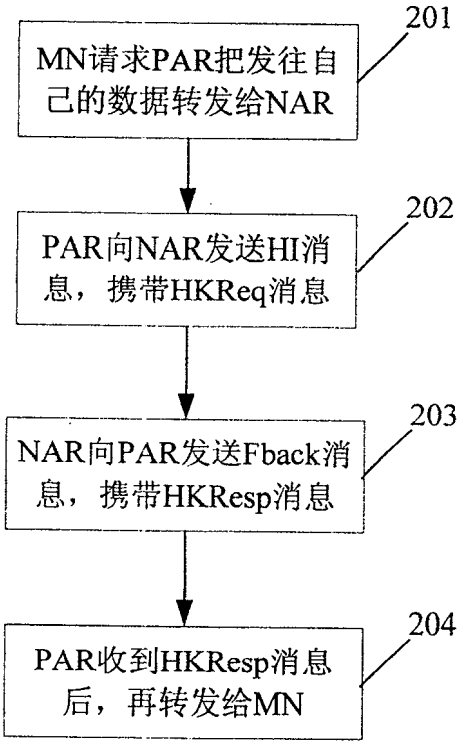

201
MN请求PAR把发往自己的数据转发给NAR
202
PAR向NAR发送HI消息，携带HKReq消息
203
NAR向PAR发送Fback消息，携带HKResp消息
204
PAR收到HKResp消息后，再转发给MN

图 2

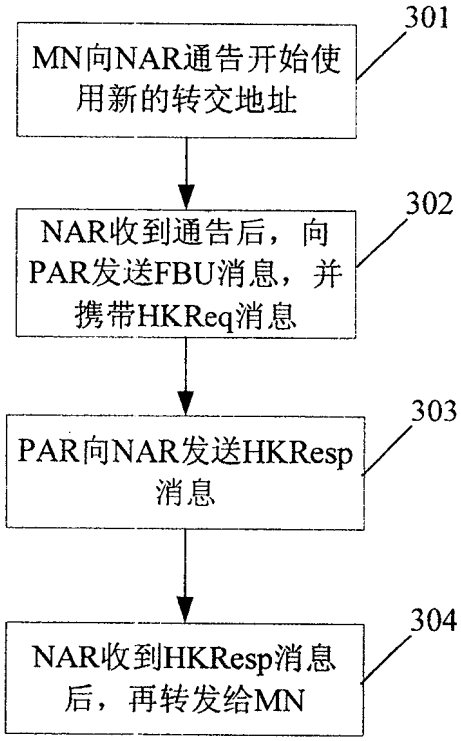

MN向NAR通告开始使用新的转交地址
301
NAR收到通告后，向PAR发送FBU消息，并携带HKReq消息
302
PAR向NAR发送HKResp消息
303
NAR收到HKResp消息后，再转发给MN
304

图 3

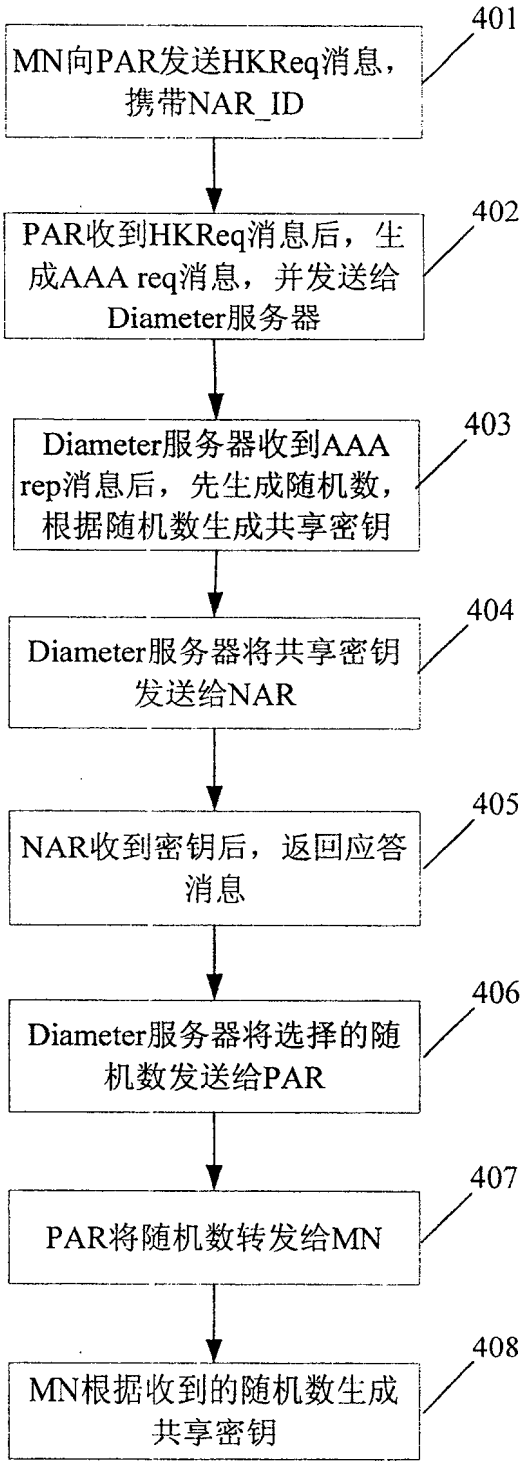

401
MN向PAR发送HKReq消息，携带NAR_ID
402
PAR收到HKReq消息后，生成AAA req消息，并发送给Diameter服务器
403
Diameter服务器收到AAA rep消息后，先生成随机数，根据随机数生成共享密钥
404
Diameter服务器将共享密钥发送给NAR
405
NAR收到密钥后，返回应答消息
406
Diameter服务器将选择的随机数发送给PAR
407
PAR将随机数转发给MN
408
MN根据收到的随机数生成共享密钥

图 4

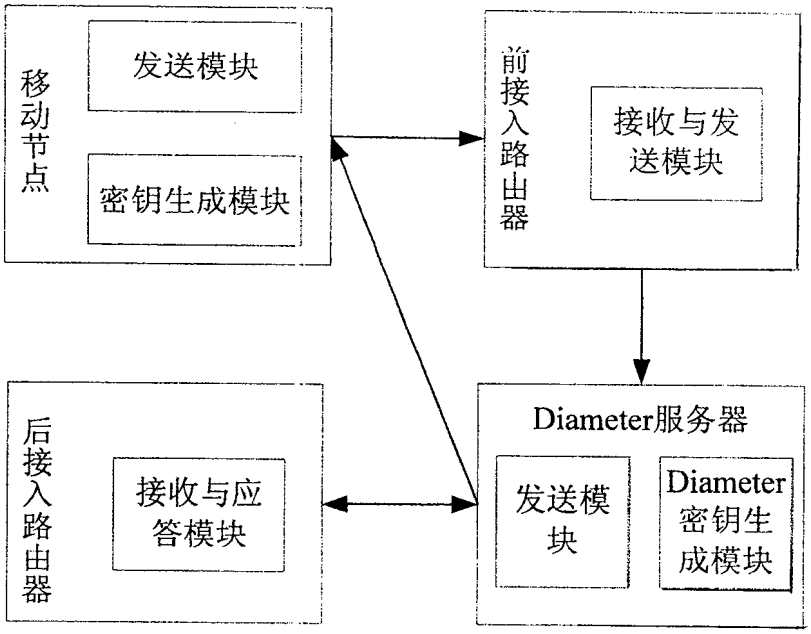

移动节点
发送模块
密钥生成模块
前接入路由器
接收与发送模块
后接入路由器
接收与应答模块
Diameter服务器
发送模块
Diameter密钥生成模块

图 5