[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)
H04L 12/46 (2006.01)
H04L 12/56 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610103524.9

[43] 公开日 2008 年 1 月 23 日

[11] 公开号 CN 101110672A

[22] 申请日 2006.7.19
[21] 申请号 200610103524.9
[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 梁文亮 谢 勇

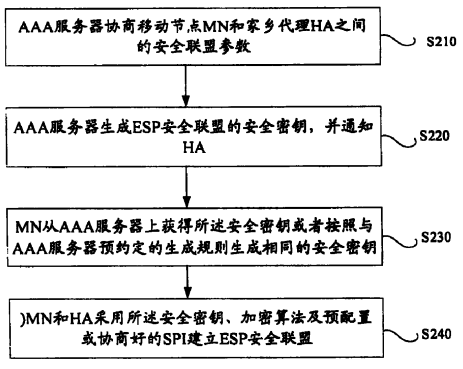
[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 胡 晶 逯长明
权利要求书 5 页 说明书 17 页 附图 4 页

[54] 发明名称

通信系统中建立 ESP 安全联盟的方法和系统

[57] 摘要

一种通信系统中建立 ESP 安全联盟的方法，第一种是通过由 AAA 服务器直接生成 ESP 安全联盟的安全密钥、移动节点 MN 从 AAA 服务器获得安全密钥或独立计算出相同安全密钥、预先设定加密算法及预先配置的 SPI；第二种是协商家乡代理 HA 和 MN 之间的 ESP 安全联盟参数、MN 从 AAA 服务器获得安全密钥或独立计算出相同安全密钥；第三种是利用将 MN 接入鉴权认证过程中产生的用于本 MN 和 HA 进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥，完成密钥交互协议过程中双方相互验证，然后由密钥交互协议协商产生 ESP 安全联盟。 通过上述三种方式建立 HA 和 MN 之间安全联盟，由此保证后续 HA 和 MN 之间业务的安全。



1、一种通信系统中建立ESP安全联盟的方法，其特征在于，包括以下步骤：

AAA服务器生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA；

移动节点MN接收从AAA服务器发送的安全密钥，或者MN按照与AAA服务器预约定的生成规则生成相同的安全密钥；

MN和HA采用所述安全密钥、预先设定或由AAA服务器指定的加密算法及预先配置的安全参数索引SPI建立ESP安全联盟。

2、如权利要求1所述的方法，其特征在于，AAA服务器生成ESP安全联盟的安全密钥具体为：

AAA服务器直接将第一密钥或第一密钥的根密钥作为所述安全密钥，或者

由第一密钥或由第一密钥的根密钥派生出所述安全密钥，其中，所述第一密钥为MN接入鉴权认证过程或HA和MN绑定更新初始过程中产生的用于该MN和HA进行绑定更新的共享密钥。

3、如权利要求2所述的方法，其特征在于， AAA服务器在下发第一密钥至HA的同时，将所述安全密钥发送至HA。

4、如权利要求1或3所述的方法，其特征在于， AAA服务器是在MN接入鉴权认证过程将安全密钥通知MN。

5、一种通信系统中建立ESP安全联盟的系统，包括MN、HA及AAA服务器，其特征在于，所述AAA服务器包括第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知HA；

所述MN还包括第二安全密钥生成单元和第一建立安全联盟单元，所述第一安全密钥生成单元：用于按照预保存的与AAA服务器约定的相同生成规则生

成安全密钥；所述第一建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数索引和生成的安全密钥建立与HA的ESP安全联盟；

所述HA包括第二建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

6、如权利要求5所述的系统，其特征在于，所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

7、一种通信系统中建立ESP安全联盟的系统，包括MN， HA及AAA服务器，其特征在于，所述AAA服务器包括第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知HA和MN;

所述MN还包括第一建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数和接收到安全密钥建立与HA的ESP安全联盟；

所述HA包括第二建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

8、如权利要求7所述的系统，其特征在于，所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

9、一种通信系统中建立ESP安全联盟的方法，其特征在于，包括:

AAA服务器协商MN和HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

AAA服务器生成ESP安全联盟的安全密钥，并通知HA;

MN从AAA服务器上获得所述安全密钥或者按照与AAA服务器预约定的生成规则生成相同的安全密钥;

MN和HA采用所述安全密钥、加密算法及预配置或协商好的SPI建立ESP安全联盟。

10、如权利要求9所述的方法，其特征在于， AAA服务器生成所述安全密钥具体为:

AAA服务器直接将第一密钥或第一密钥的根密钥作为所述安全密钥，或者

由第一密钥或由第一密钥的根密钥派生出所述安全密钥，其中，所述第一密钥为MN接入鉴权认证过程或HA和MN绑定更新初始过程中产生的用于该MN和HA进行绑定更新的共享密钥。

11、如权利要求9所述的方法，其特征在于， AAA服务器协商MN和HA之间的安全联盟参数具体为:

MN通知AAA服务器本节点所支持的所有加密算法以及分配给本MN和HA之间ESP安全联盟的SPI;

AAA服务器获得HA为本HA与MN之间ESP安全联盟分配的SPI，并从MN能够支持的加密算法之中选择HA能够支持的一种加密算法作为协商好的加密算法。

12、如权利要求11所述的方法，其特征在于，MN是在接入鉴权过程将所述加密算法和所述SPI发送至AAA服务器。

13、如权利要求11或12所述的方法，其特征在于，

AAA服务器是在MN接入鉴权认证过程或绑定更新BU过程中，询问HA所支持所有加密算法和HA为本HA与MN之间ESP安全联盟分配的SPI。

14、如权利要求12所述的方法，其特征在于，进一步包括:

预先将HA和AAA服务器配置成支持相同的加密算法或者将HA配置成支持所有的加密算法;

协商好的加密算法是AAA服务器从MN能够支持的加密算法中选择本服务器能够支持的一种加密算法。

15、一种通信系统中建立ESP安全联盟的系统，包括MN， HA及AAA服务器，其特征在于，所述AAA服务器包括协商单元和第一安全密钥生成单元，

协商单元，用于协商MN和HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知HA;

所述MN还包括第二安全密钥生成单元和第一建立安全联盟单元，所述第一安全密钥生成单元：用于按照预保存的与AAA服务器约定的相同生成规则生成安全密钥；所述第一建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数索引和生成的安全密钥建立与HA的ESP安全联盟;

所述HA包括第二建立安全联盟单元，用于通过接收到加密算法和安全密钥、预配置或接收到的安全参数建立与MN的ESP安全联盟。

16、如权利要求15所述的系统，其特征在于，所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

17、一种通信系统中建立ESP安全联盟的系统，包括MN， HA及AAA服务器，其特征在于，

所述AAA服务器包括协商单元和第一安全密钥生成单元，

协商单元，用于协商MN和HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知HA和MN;

所述MN还包括第一建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数和接收到的安全密钥建立与HA的ESP安全联盟;

所述HA包括第二建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

18、如权利要求17所述的系统，其特征在于，所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

19、一种通信系统中建立ESP安全联盟的方法，其特征在于，包括:

将MN接入鉴权认证过程中或HA和MN绑定更新初始过程中产生的用于本MN和HA进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥;

在密钥交互协议过程中，协商建立MN和HA之间的ESP安全联盟。

20、如权利要求19所述的方法，其特征在于，在密钥交互协议过程中，协商建立MN和HA之间的ESP安全联盟具体为:

MN和HA之间协商建立一安全通道;

利用所述预配置密钥进行MN和HA的互相验证，建立交互过程中的第一个Ipsec安全联盟;

将所述第一个Ipsec安全联盟作为MN和HA之间用于加密的ESP安全联盟或者，利用第一个Ipsec安全联盟重新协商用于加密的ESP安全联盟。

21、如权利要求19所述的方法，其特征在于，所述ESP安全联盟中的生成密钥的方法是在密钥交互协商过程设定的，或者

所述ESP安全联盟中的生成密钥的方法是在预先完成的MN接入鉴权认证过程中设定的。

22、一种通信系统中建立 ESP 安全联盟的系统，包括 MN 及 HA，其特征在于，所述 MN 和 HA 中均分别设有预配置密钥单元和协商单元，

所述预配置密钥：用于将 MN 接入鉴权认证过程中或 HA 和 MN 绑定更新初始过程中产生的用于本 MN 和 HA 进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥;

协商单元：用于在密钥交互协议过程中，协商建立 MN 和 HA 之间的 ESP 安全联盟。

通信系统中建立ESP安全联盟的方法和系统

技术领域

本发明涉及通信领域中通信系统中建立安全联盟的方法及系统，尤其涉及移动节点（Mobile Node,MN）和家乡代理(Home Agent,HA)之间建立ESP（Encapsulating Security Payload，安全载荷封装）安全联盟的方法和系统。

背景技术

在现有的移动IP技术中，移动IPv6是今天最有效地可移动建议之一。如图1所示，其为一个基本的移动Ipv6组成示意图。移动Ipv6包含三个实体：移动节点MN、家乡代理HA和通信节点CN。一个Ipv6移动节点是一个多主机地址节点。它同时拥有一个转交地址和一个家乡地址，其中转交地址用来路由IP包，其前缀是所访问链路网络的前缀。转交地址是临时的，必须要对它进行返回路由能力检查之后才能使用该地址参与通信；家乡地址用来识别移动节点，其前缀是家乡链路网络的前缀。移动Ipv6允许移动节点从一个链路移动到另一个链路而无需改变家乡地址。

移动节点和通信节点有两种通信模式。第一种模式是从通信节点发出的数据包会路由到家乡代理，再通过隧道发往移动节点；从移动节点发出的数据包先通过隧道发往家乡代理，再路由到通信节点。在这种模式中，家乡代理在家乡链路上使用代理邻居发现协议截取指向移动节点家乡地址的数据包。被截取的数据包通过隧道发往到移动节点当前的转交地址。这种模式双向的数据都必须经过家乡代理HA，容易引出网络阻塞，并且当家乡代理和相关链路发生故障后影响移动节点和通信节点之间的通信。

第二种模式是路由优化模式。双方通信的数据不必经由HA，而直接经过路由进行通信。这种模式由于对路由进行了优化而得到了极大的发展。在路由优化模式下，移动Ipv6引入了一个返回可路由过程（RRP），通过它保证MN与CN通信时的安全，其原理是通过对MN与CN之间交换的信令进行加密

来对它们之间的登记进行认证。通过RRP，CN知道是否能够使用MN通告的转交地址和家乡地址访问MN；如果RRP测试失败，CN将既不能直接发送分组到MN的转交地址。其测试方法是通过两个消息对（HoTI和HoT，CoTI和CoT）分别测试目的地址是家乡地址和转换地址的分组是否能够到达MN，据此接收来自MN的绑定（请参阅图2）。

在RRP过程中，HoTI用于把MN的家乡地址和Cookie通知CN，请求CN提供家乡密钥生成令牌。而CoTI主要是把MN的转交地址和Cookie通知CN，请求CN提供转交密钥生成令牌。MN通过对家乡密钥生成令牌、转交密钥生成令牌进行SHA1散列运算得到一个共享密钥Kbm。通过该共享密钥Kbm对后续MN和CN之间的BU（绑定更新）和BA（绑定响应）进行认证。

在PPR过程中，HoTI和HoT这两个消息是以明文方式进行传输，无法保证移动节点MN和家乡代理HA之间返回可路由过程的私密性，由此容易被监听。当恶意攻击者得到HoT和CoT消息中的H-Token以及C-Token后，可以计算出后续MN和CN之间BU过程的密钥信息kbm，由此不能保证后续通信如预期那样发生在移动节点MN和相关节点CN之间。最终，WiMax等无线网络将无法正常支持路由优化RO，降低了WiMax网络效率。也就是说WiMAX等无线网络如果要支持IPv6的RO，就必须考虑移动节点MN和家乡代理HA之间的ESP安全联盟，以保证路由优化RO信令的私密性。

除了上述提到的RRP过程需要预先建立MN和HA之间的ESP安全联盟，在其它一些场合，如移动前缀请求过程、MN和HA的数据传输过程都需要保证MN和HA之间业务的安全性，同样也需要建立MN和HA之间的ESP安全联盟。

发明内容

本发明的目的在于提供一种通信系统中建立ESP安全联盟的方法和系统，以增加MN和HA之间业务的安全性。

为了达到上述目的，本发明提供了公开了一种通信系统中建立ESP安全联盟的方法，包括以下步骤：

(1)AAA服务器生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA;

(2)移动节点MN接收从AAA服务器发送的安全密钥，或者MN按照与AAA服务器预约定的生成规则生成相同的安全密钥;

(3)MN和HA采用所述安全密钥、预先设定或由AAA服务器指定的加密算法及预先配置的安全参数索引SPI建立ESP安全联盟。

步骤(1)具体为：AAA服务器直接将第一密钥或第一密钥的根密钥作为所述安全密钥，或者 由第一密钥或由第一密钥的根密钥派生出所述安全密钥，其中，所述第一密钥为移动节点MN接入鉴权认证过程或HA和MN绑定更新初始过程中产生的用于该MN和HA进行绑定更新的共享密钥。

优选地，步骤(1)中，AAA服务器在下发第一密钥至HA的同时，将所述安全密钥发送至HA。步骤(2)中AAA服务器是在MN接入鉴权认证过程将安全密钥通知MN。

本发明公开的第二种通信系统中建立ESP安全联盟的方法，包括:

(1)AAA服务器协商移动节点MN和家乡代理HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

(2)AAA服务器生成ESP安全联盟的安全密钥，并通知HA;

(3)MN从AAA服务器上获得所述安全密钥或者按照与AAA服务器预约定的生成规则生成相同的安全密钥;

(4)MN和HA采用所述安全密钥、加密算法及预配置或协商好的SPI建立ESP安全联盟。

优选地，步骤(2)中AAA服务器生成所述安全密钥具体为：AAA服务器直接将第一密钥或第一密钥的根密钥作为所述安全密钥，或者 由第一密钥或由第一密钥的根密钥派生出所述安全密钥，其中，所述第一密钥为移动节点

MN接入鉴权认证过程或HA和MN绑定更新初始过程中产生的用于该MN和HA进行绑定更新的共享密钥。

步骤(1)中AAA服务器协商移动节点MN和家乡代理HA之间的安全联盟参数具体为：(11)移动节点MN通知AAA服务器本节点所支持的所有加密算法以及分配给本节点MN和HA之间ESP安全联盟的SPI；(12)AAA服务器获得家乡代理HA为本HA与MN之间ESP安全联盟分配的SPI，并从MN能够支持的加密算法之中选择HA能够支持的一种加密算法作为协商好的加密算法。

MN是在接入鉴权过程将所述加密算法和所述SPI发送至AAA服务器。

步骤(12)中AAA服务器是在MN接入鉴权认证过程或绑定更新BU过程中，询问HA所支持所有加密算法和HA为本HA与MN之间ESP安全联盟分配的SPI。

步骤(12)进一步包括：预先将HA和AAA服务器配置成支持相同的加密算法或者将HA配置成支持所有的加密算法；协商好的加密算法是AAA服务器从MN能够支持的加密算法中选择本服务器能够支持的一种加密算法。

本发明公开的第三种通信系统中建立ESP安全联盟的方法，包括：(1)将移动节点MN接入鉴权认证过程中或HA和MN绑定更新BU过程中产生的用于本MN和HA进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥；(2)在密钥交互协议过程中，协商建立MN和HA之间的ESP安全联盟。步骤(2)具体为：(21) MN和HA之间协商建立一安全通道；(22)利用所述预配置密钥进行MN和HA的互相验证，建立交互过程中的第一个Ipsec安全联盟；(23)将所述第一个Ipsec安全联盟作为MN和HA之间用于加密的ESP安全联盟或者，利用第一个Ipsec安全联盟重新协商用于加密的ESP安全联盟。

所述ESP安全联盟中的生成密钥的方法是在密钥交互协商过程设定的，或者所述ESP安全联盟中的生成密钥的方法是在预先完成的MN接入鉴权认证过程中设定的。

对应地，本发明公开的第一种通信系统中建立ESP安全联盟的系统，还包括AAA服务器，所述AAA服务器包括第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA;

所述移动节点还包括第二安全密钥生成单元和第一建立安全联盟单元，所述第一安全密钥生成单元：用于按照预保存的与AAA服务器约定的相同生成规则生成安全密钥；所述第一建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数索引和生成的安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

本发明公开的第二种通信系统中建立ESP安全联盟的系统，还包括AAA服务器，所述AAA服务器包括第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA和移动节点MN;

所述移动节点还包括第一建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数和接收到安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

本发明公开的第三种通信系统中建立ESP安全联盟的系统，还包括AAA服务器，所述AAA服务器包括协商单元和第一安全密钥生成单元，

协商单元，用于协商移动节点MN和家乡代理HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA;

所述移动节点还包括第二安全密钥生成单元和第一建立安全联盟单元，所述第一安全密钥生成单元：用于按照预保存的与AAA服务器约定的相同生成规则生成安全密钥；所述第一建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数索引和生成的安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过接收到加密算法和安全密钥、预配置或接收到的安全参数建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

本发明公开的第四种通信系统中建立ESP安全联盟的系统，还包括AAA服务器，

所述AAA服务器包括协商单元和第一安全密钥生成单元，

协商单元，用于协商移动节点MN和家乡代理HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA和移动节点MN;

所述移动节点还包括第一建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数和接收到的安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

本发明公开的第五种通信系统中建立 ESP 安全联盟的系统，所述移动节点和家乡代理中都设有预配置密钥单元和协商单元，

所述预配置密钥：用于将移动节点 MN 接入鉴权认证过程中或 HA 和 MN 绑定更新初始过程中产生的用于本 MN 和 HA 进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥；　　协商单元：用于在密钥交互协议过程中，协商建立 MN 和 HA 之间的 ESP 安全联盟。

本发明可以通过三种方式建立HA与MN之间的ESP安全联盟，能够保证HA与MN之间业务的私密性。特别是，当该安全联盟用于加密RRP过程中涉及到的相关信令时，能够增加路由优化过程中的安全性。使得WiMax等网络可以正常支持路由优化RO，提高了网络的效率。

附图说明

图1为一个基本的移动Ipv6组成示意图；

图2为现有RRP过程示意图；

图3为本发明公开的第一种通信系统中建立ESP安全联盟的方法的流程图；

图4为本发明公开的第一种通信系统中建立ESP安全联盟的系统结构示意图；

图5为本发明公开的第二种通信系统中建立ESP安全联盟的系统结构示意图；

图6为本发明公开的第二种通信系统中建立ESP安全联盟的方法的流程图；

图7为本发明公开的第三种通信系统中建立ESP安全联盟的系统结构示意图；

图8为本发明公开的第四种通信系统中建立ESP安全联盟的系统的结构示意图；

图9为本发明公开的第三种通信系统中建立ESP安全联盟的方法的流程图；

图10为本发明公开的第五种通信系统中建立ESP安全联盟的系统的结构示意图。

具体实施方式

以下结合附图，具体说明本发明。

为了保证HA和MN之间业务的安全性，需要预先进行HA和MN之间建立安全联盟。本发明的核心在于：本发明提供了三种HA和MN之间建立安全联盟的方法，第一种建立方案为：通过由AAA服务器直接生成ESP安全联盟的安全密钥、移动节点MN从AAA服务器获得安全密钥或者是独立计算出相同安全密钥、预先设定加密算法及预先配置的SPI；第二种建立方案为：协商家乡代理HA和MN之间包括加密算法或包括加密算法和SPI的ESP安全联盟参数、移动节点MN从AAA服务器获得安全密钥或者是独立计算出相同安全密钥；第三种方案为：利用将移动节点MN接入鉴权认证过程中产生的用于本MN和HA进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥，完成密钥交互协议过程中双方相互证验证，然后由密钥交互协议协商产生ESP安全联盟。通过上述三种方式建立HA和MN之间安全联盟，以此保证后续HA和MN之间的业务的安全。所述HA和MN之间的

业务包括 RRP 过程、移动前缀请求过程、MN 和 HA 的数据传输过程等。后续就以 RRP 过程为例来说明本发明。

随着网络技术的迅速发展，网上数据的安全问题是最受关注的问题。现在，许多通信协议和方法中都提供了对数据的加密或验证功能，以此来保证数据的安全传输。应用较为广泛的是 IPSec（Internet Protocol Security）协议。IPSec 协议是一种协议套件，包括 AH（Authentication Header）验证头协议、ESP（Encapsulation Security Protocol）封装安全载荷协议、IKE（Internet Key Exchange）互联网密钥交换协议等。IPSec 协议支持手动配置方式或 IKE 协议自动协商方式生成安全联盟 SA（Security Association）。安全联盟是 IPSec 的基础，它决定了用于保护数据包安全的 IPSec 协议中的密钥以及密钥生成时间等，安全联盟的主要参数有 SPI、密钥、算法等。也就是说，安全联盟是对数据进行加密或验证的基本依据，也可以说每一个需要进行加密或验证处理的数据包都会配置或生成特定的安全联盟 SA。另外，本发明 HA 和 MN 之间建立的是 ESP 安全联盟。

请参阅图 3，其为本发明公开的第一种通信系统中建立 ESP 安全联盟的方法的流程图。它包括以下步骤:

S110: AAA服务器生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA;

S120: 移动节点MN接收从AAA服务器发送的安全密钥，或者MN按照与AAA服务器预约定的生成规则生成相同的安全密钥;

S130: MN和HA采用所述安全密钥、预先设定或由AAA服务器指定的加密算法及预先配置的安全参数索引SPI建立ESP安全联盟。

以下具体说明每一步骤。

一、步骤S110

MN在接入鉴权认证过程和首次家乡代理HA注册过程后，MN和HA之间有一个共享密钥信息，该共享密钥信息主要用于保护后续MN和HA之间的

BU（绑定更新）/BA（绑定响应）过程的完整性，本发明将该共享密钥称之为第一密钥。AAA服务器可以直接将该第一密钥作为ESP安全联盟的安全密钥，也可以由第一密钥派生出所述安全密钥。较佳地实施方式是通过AAA服务器由第一密钥派生出安全密钥。派生主要是指根据预先设定的一计算公式或函数，将第一密钥作为一公式或函数的已知因子得到对应的安全密钥。

除了第一密钥外，也可以由接入鉴权认证过程第一密钥的根密钥MSK或EMSK来产生安全密钥。即，直接将第一密钥的根密钥MSK或EMSK作为安全密钥，或者，由第一密钥的根密钥派生出安全密钥。当然，除了第一密钥和第一密钥的根密钥外，AAA服务器也可以利用其它MN和AAA服务器或者MN和HA之前保有的密钥信息，生成MN和HA之间的ESP安全联盟的密钥。

AAA服务器在下发第一密钥至HA的同时，可以将该安全密钥发送至HA。换句话说，AAA服务器将第一密钥和安全密钥包含在AAA到HA的交互消息Access-Accept中进行发送。另外，当ESP安全联盟的加密算法是由AAA服务器指定时，AAA服务器可以将第一密钥、安全密钥和指定的加密算法同时发送至HA。

二、步骤S120

MN可以由两种方式获得安全密钥，第一种方式是通过接收AAA服务器发送的安全密钥获得所述安全密钥，比如，AAA服务器在MN接入鉴权认证过程将安全密钥发送至MN；第二种方式是MN预先保存有用于生成安全密钥的生成规则，所述生成规则和AAA服务器上生成安全密钥的生成规则相同，这样，MN按照该规则生成的安全密钥和AAA服务器上生成的安全密钥相同。所述生成规则主要是指步骤S110中AAA服务器如何得到安全密钥的流程及对应的参数。

当加密算法是由AAA服务器指定时，AAA服务器也可以将指定后的加密算法在MN接入鉴权认证过程同安全密钥一起发送至MN。

三、步骤S130

SPI（Security Parameter Index 安全参数索引）在一个实体中是唯一的。这里实体为HA和MN，可以动态的为安全联盟分配SPI，一个简单的例子就是新增一个安全联盟就为它分配一个没有使用过的SPI。可以预先预留一个SPI，不能再分配给其他用途的安全联盟，而仅仅使用于返回可路由过程。当然如果有其他应用场景，可以另外预定义一个SPI，或者就共享使用。

MN和HA之间默认的ESP安全联盟所必须满足的其它参数：如加密算法不为空、ESP模式为隧道模式、SPI为双方都知道的数值，这些信息都预先配置。

HA和MN之间利用安全密钥、SPI和加密算法建立ESP安全联盟。

请参阅图4，其为本发明公开的第一种通信系统中建立ESP安全联盟的系统的结构原于理示意图。还包括AAA服务器，所述AAA服务器包括第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA;

所述移动节点还包括第二安全密钥生成单元和第一建立安全联盟单元，所述第一安全密钥生成单元：用于按照预保存的与AAA服务器约定的相同生成规则生成安全密钥；所述第一建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数索引和生成的安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。若通过加密算法指定单元指定加密算法，则HA与MN之间无需预先保存加密算法。

上述系统中移动节点是通过自身的第二安全密钥生成单元来生成安全密钥，另外，也可以直接接收从AAA服务器发送的安全密钥。即，

请参阅图5，其为本发明公开的第二种通信系统中建立ESP安全联盟的系统的结构示意图。它还包括AAA服务器，所述AAA服务器包括第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA和移动节点MN;

所述移动节点还包括第一建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数和接收到安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过预保存的加密算法、预配置的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

请参阅图6，其为本发明公开的第二种通信系统中建立ESP安全联盟的方法的流程图。它包括:

S210: AAA服务器协商移动节点MN和家乡代理HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

S220: AAA服务器生成ESP安全联盟的安全密钥，并通知HA;

S230: MN从AAA服务器上获得所述安全密钥或者按照与AAA服务器预约定的生成规则生成相同的安全密钥;

S240: MN和HA采用所述安全密钥、加密算法及预配置或协商好的SPI建立ESP安全联盟。

步骤S210 中AAA服务器协商移动节点MN和家乡代理HA之间的安全联盟参数可以通过以下步骤完成:

（1）MN通知AAA服务器本节点所支持的所有加密算法以及分配给本节点MN和HA之间ESP安全联盟的SPI。MN可以在接入鉴权过程将所述加密算法和所述SPI发送至AAA服务器。

（2）AAA服务器获得家乡代理HA为本HA与MN之间ESP安全联盟分配的SPI，并从MN能够支持的加密算法之中选择HA能够支持的一种加密算法作为协商好的加密算法。

在网络规划时，HA和AAA服务器可以预配置成支持相同的加密算法，并且预定义用于该业务的SPI。AAA 服务器接收到MN所有加密算法后，从该些加密算法中找到AAA服务器所支持的其中一种加密算法作为HA和MN之间的ESP安全联盟的加密算法。

另外，还可以在HA上预设定所有加密算法，这样，AAA 服务器接收到MN所有加密算法后，从该些加密算法中找到AAA服务器所支持的其中一种加密算法作为HA和MN之间的ESP安全联盟的加密算法。

还有，AAA服务器还可以在MN接入鉴权认证过程或绑定更新BU过程中，询问HA所支持所有加密算法和HA为本HA与MN之间ESP安全联盟分配的SPI，并且，AAA服务器从HA、MN和AAA服务器都支持的加密算法中找到其中一种算法作为HA与MN之间的ESP安全联盟的加密算法。

AAA服务器通知MN最终确定的加密算法和 HA预分配的用于该业务的ESP安全联盟的SPI。AAA服务器可以在MN接入鉴权认证过程将加密算法和SPI通知至MN。并且，AAA服务器将最终确定的加密算法和MN分配给HA与本MN之间ESP安全联盟的SPI。

步骤S220至步骤S240和上述公开的第一种HA与MN之间建立ESP安全联盟方法中的步骤S110至步骤S130类似，在此先省略。需要说明的是，安全密钥可以和加密算法、SPI一起在接入鉴权认证过程中通知至MN。

另外需要说明的一点是：HA与MN在MN接入鉴权认证过程协商完成ESP安全联盟的建立时，它和移动IP注册过程可以没有前后关系。

请参阅图7，其为本发明公开的第三种通信系统中建立ESP安全联盟的系统的结构示意图。它还包括AAA服务器，所述AAA服务器包括协商单元和第一安全密钥生成单元，

协商单元，用于协商移动节点MN和家乡代理HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA;

所述移动节点还包括第二安全密钥生成单元和第一建立安全联盟单元，所述第二安全密钥生成单元：用于按照预保存的与AAA服务器约定的相同生成规则生成安全密钥；所述第一建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数索引和生成的安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过接收到加密算法和安全密钥、预配置或接收到的安全参数建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

上述系统中移动节点是通过自身的第二安全密钥生成单元来生成安全密钥，另外，也可以直接接收从AAA服务器发送的安全密钥。即，

请参阅图8，其为本发明公开的第四种通信系统中建立ESP安全联盟的系统的结构示意图。它还包括AAA服务器，所述AAA服务器包括协商单元和第一安全密钥生成单元，

协商单元，用于协商移动节点MN和家乡代理HA之间的安全联盟参数，并将协商好的安全联盟参数分别通知MN和HA，所述安全联盟参数包括加密算法或者包括加密算法和安全参数索引SPI;

第一安全密钥生成单元，用于生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA和移动节点MN;

所述移动节点还包括第一建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数和接收到的安全密钥建立与家乡代理HA的ESP安全联盟;

所述家乡代理包括第二建立安全联盟单元，用于通过接收到的加密算法、预配置或接收到的安全参数与接收到的安全密钥建立与MN的ESP安全联盟。

所述AAA服务器还包括加密算法指定单元，用于指定HA与MN之间的ESP安全联盟的加密算法，并通知HA和MN。

请参阅图9，其为本发明公开的第三种通信系统中建立ESP安全联盟的方法的流程图。它包括:

S310: 将移动节点MN接入鉴权认证过程或中或HA和MN绑定更新初始过程中产生的用于本MN和HA进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥;

S320: 在密钥交互协议过程中，协商建立MN和HA之间的ESP安全联盟

S21: MN和HA之间协商建立一安全通道;

S22: 利用所述预配置密钥进行MN和HA的互相验证，建立交互过程中的第一个Ipsec安全联盟;

S23: 将所述第一个Ipsec安全联盟作为MN和HA之间的ESP安全联盟或者，利用第一个Ipsec安全联盟重新协商ESP安全联盟。

目前的密钥交互协议主要就是IKEv1和IKEv2。IKE过程都可以分为初始化子过程、验证子过程以及子安全联盟协商子过程。在初始化子过程中，交互双方互相发送Diffie-Hellman方法所需要的数据、协商算法以及随机数，创建一个专属于IKE协商过程的安全联盟；在初始化子过程所建立的安全联盟的私密性保护下，交互双方进行互相的验证，验证可以基于电子证书或者是预共享密钥，验证成功后第一个子安全联盟也被建立；当验证子过程成功完成以后，交互双方就可以协商创建更多的子安全联盟。

本方法主要是通过密钥交互协议完成移动节点MN和家乡代理HA之间的ESP安全联盟的建立，即引入密钥交互协议过程来协商建立MN和HA之间的安全联盟的建立，同时由于密钥交互协议（IKEv2为例）过程本身也需要预配置密钥在端点之间相互验证，本发明通过密钥交互协议（IKEv2为例）过程协商建立MN和HA之间的安全联盟，并且将移动节点MN和AAA服务器之间的鉴权认证过程中协商产生的密钥信息作为密钥交互协议（IKEv2为例）中的预配置密钥。

如果移动节点MN和家乡代理HA之间不存在一个ESP的安全联盟，移动节点MN和家乡代理HA之间必须发起一个密钥交互过程（这里以IKEv2为例）。

首先IKE-SA-INIT过程（初始化子过程）移动节点MN和家乡代理HA之间协商建立一个相对于其他节点安全的通路，建立安全通路是已有技术，可以参考RFC4306。大致过程是，双方交换随机数，按照DH算法，计算出仅双方知道的密钥，然后所有的后续的交互都由这个密钥加密。其他节点由于没有这个密钥信息，也就无法看到上述双方的通信内容。

然后在IKE-AUTH过程（验证子过程）中分别利用预共享密钥互相验证，并且建立IKE过程中的第一个IPsec安全联盟。双方身份验证通过后，可以在预先建立的安全通路上协商ESP安全联盟（包含相关密钥以及加密算法），或者是已经商议了第一个IPsec安全联盟作为ESP安全联盟（包含相关密钥以及加密算法），以保证有能力在移动节点MN和家乡代理HA之间提供信令或者数据的私密性。HA与MN之间建立的ESP安全联盟必须包含一个保证私密性的算法以及私密性密钥（即所述安全密钥）。

ESP安全联盟中的生成密钥的方法是在密钥交互协商过程设定的，或者所述ESP安全联盟中的生成密钥的方法是在预先完成的MN接入鉴权认证过程中设定的。

请参阅 10，其为本发明提供第五种通信系统中建立 ESP 安全联盟的系统的结构示意图。所述移动节点和家乡代理中都设有预配置密钥单元和协商单元，

所述预配置密钥：用于将移动节点MN接入鉴权认证过程中或HA和MN绑定更新初始过程中产生的用于本MN和HA进行绑定更新的共享密钥作为密钥交互协议过程的预配置密钥；

协商单元：用于在密钥交互协议过程中，协商建立MN和HA之间的ESP安全联盟。

上述三种方法的其中之一产生HA与MN之间的ESP安全联盟后，在RRP过程中可以利用建立的ESP安全联盟进行通信，由此保证了MN和HA之间返回可路由过程的私密性，进而保证了后续MN和CN之间BU过程的密钥信息kbm的安全性。最终，WiMax等无线网络可以正常支持路由优化R0，保证路由优化R0信令的私密性。

以上公开的仅为本发明的几个具体实施例，但本发明并非局限于此，任何本领域的技术人员能思之的变化，都应落在本发明的保护范围内。

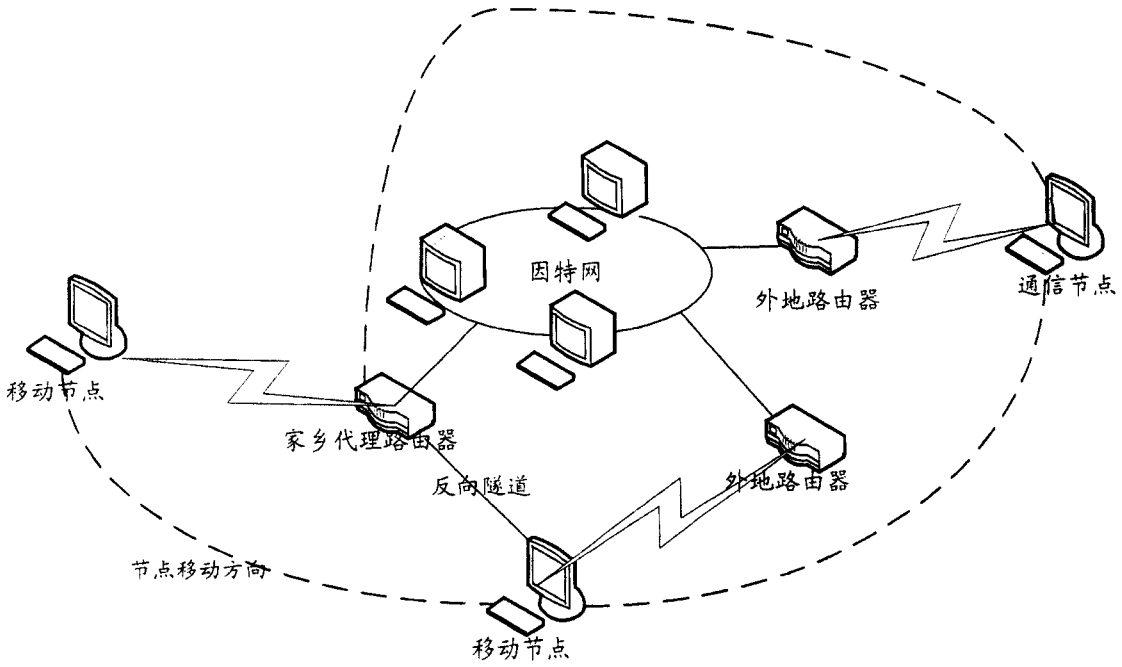

因特网
外地路由器
通信节点
移动节点
家乡代理路由器
反向隧道
外地路由器
节点移动方向
移动节点

图 1

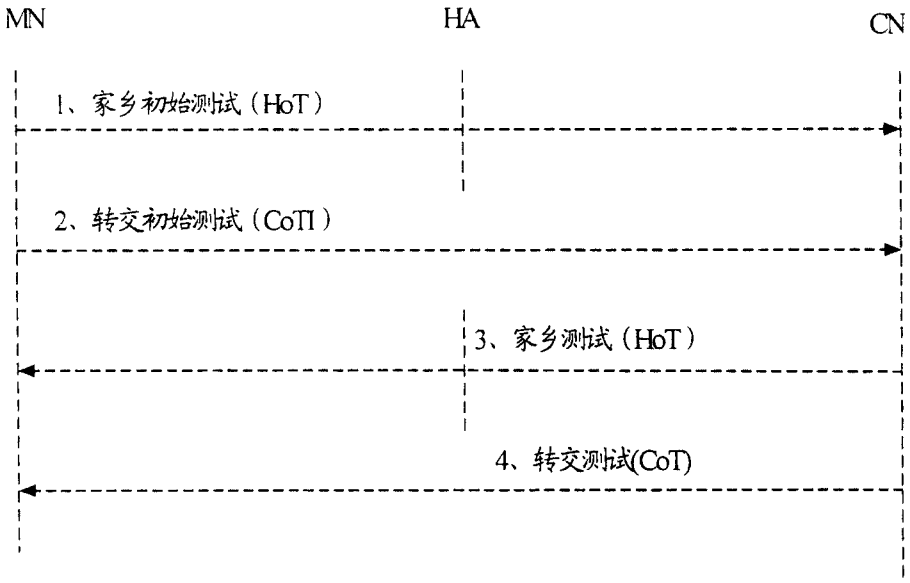

MN
HA
CN
1、家乡初始测试（HoT）
2、转交初始测试（CoTI）
3、家乡测试（HoT）
4、转交测试(CoT)

图 2

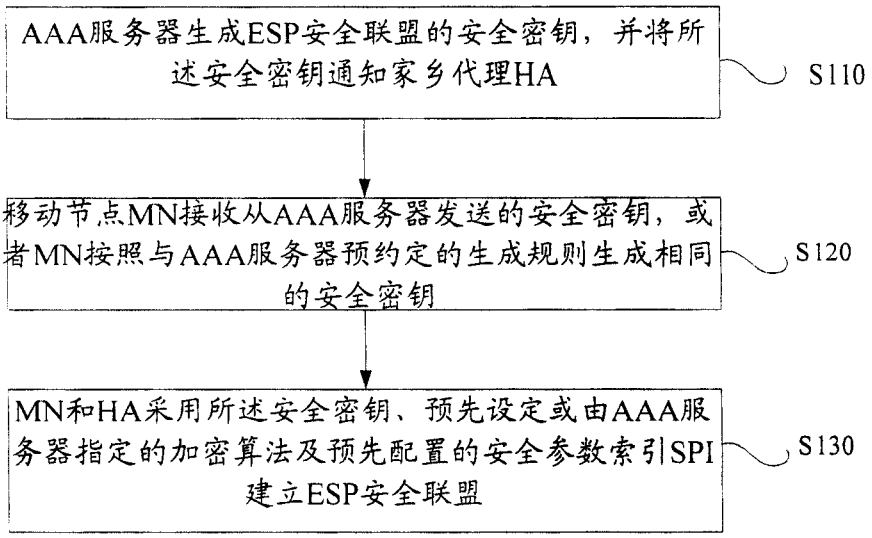

AAA服务器生成ESP安全联盟的安全密钥，并将所述安全密钥通知家乡代理HA
S110
移动节点MN接收从AAA服务器发送的安全密钥，或者MN按照与AAA服务器预约定的生成规则生成相同的安全密钥
S120
MN和HA采用所述安全密钥、预先设定或由AAA服务器指定的加密算法及预先配置的安全参数索引SPI建立ESP安全联盟
S130

图 3

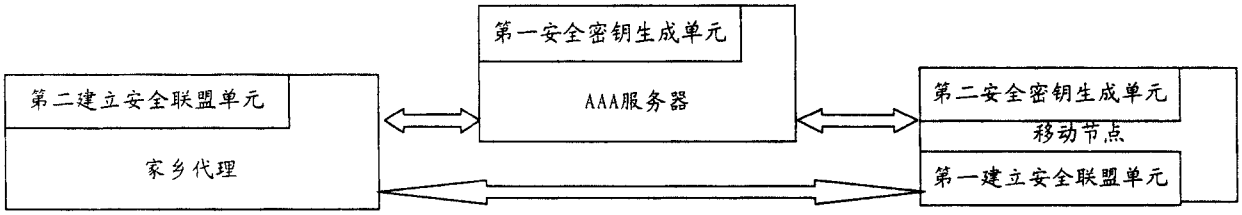

第一安全密钥生成单元
AAA服务器
第二建立安全联盟单元
家乡代理
第二安全密钥生成单元
移动节点
第一建立安全联盟单元

图 4

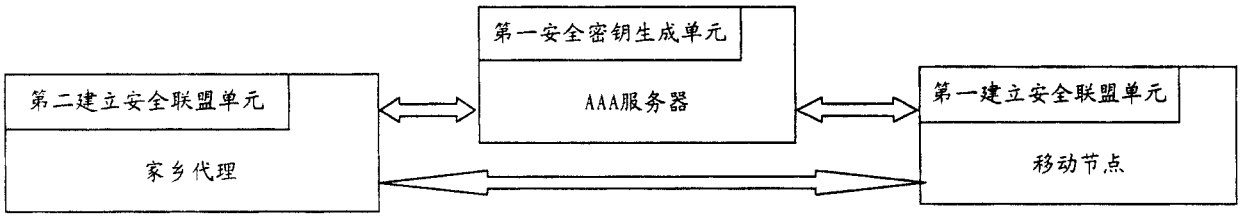

第一安全密钥生成单元
AAA服务器
第二建立安全联盟单元
家乡代理
第一建立安全联盟单元
移动节点

图 5

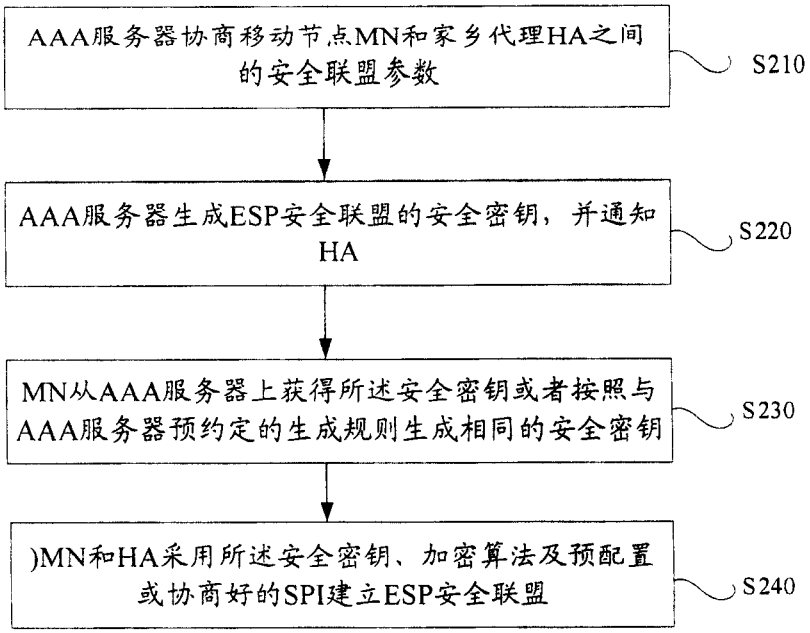

AAA服务器协商移动节点MN和家乡代理HA之间的安全联盟参数
S210
AAA服务器生成ESP安全联盟的安全密钥，并通知HA
S220
MN从AAA服务器上获得所述安全密钥或者按照与AAA服务器预约定的生成规则生成相同的安全密钥
S230
)MN和HA采用所述安全密钥、加密算法及预配置或协商好的SPI建立ESP安全联盟
S240

图 6

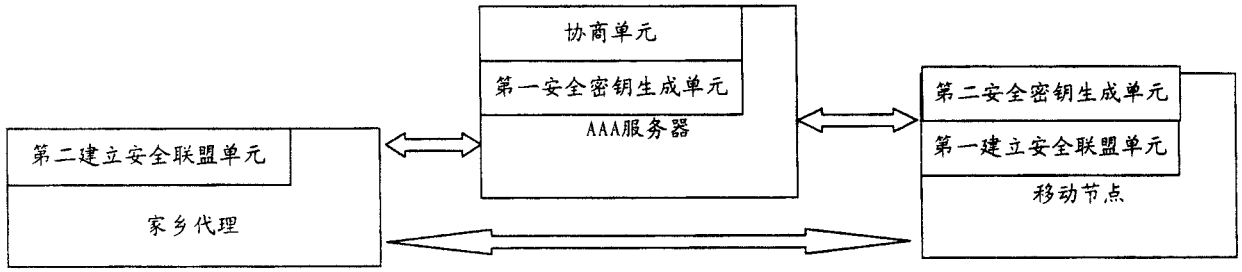

协商单元
第一安全密钥生成单元
AAA服务器
第二建立安全联盟单元
家乡代理
第二安全密钥生成单元
第一建立安全联盟单元
移动节点

图 7

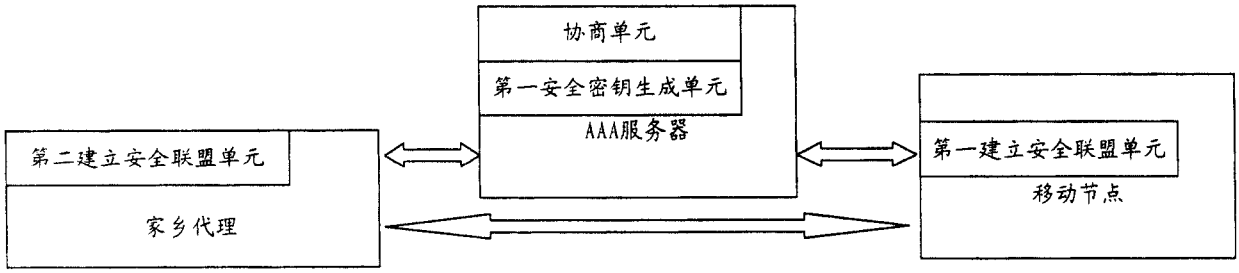

协商单元
第一安全密钥生成单元
AAA服务器
第二建立安全联盟单元
家乡代理
第一建立安全联盟单元
移动节点

图 8

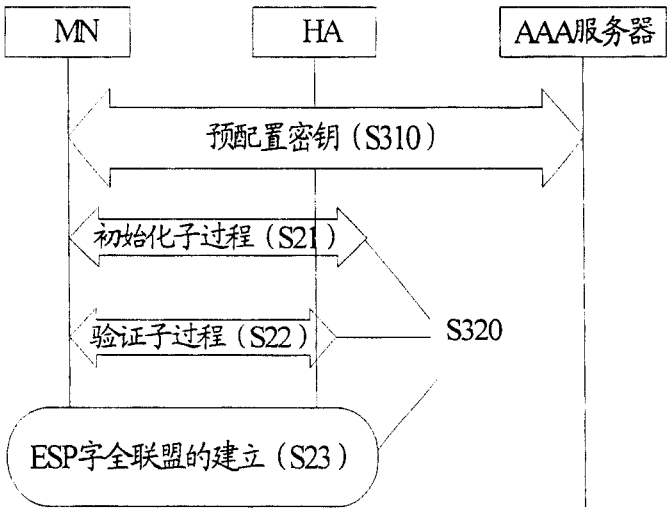

MN
HA
AAA服务器
预配置密钥（S310）
初始化子过程（S21）
验证子过程（S22）
S320
ESP字全联盟的建立（S23）

图 9

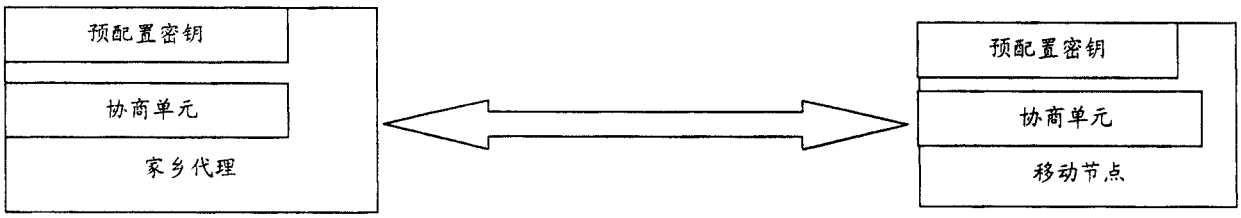

预配置密钥
协商单元
家乡代理
预配置密钥
协商单元
移动节点

图 10