



# [12] 发明专利申请公开说明书

[21] 申请号 200310111041. X

[43] 公开日 2005 年 6 月 8 日

[11] 公开号 CN 1625101A

[22] 申请日 2003. 12. 1

[21] 申请号 200310111041. X

[71] 申请人 中国电子科技集团公司第三十研究所  
地址 610041 四川省成都市高新区创业路 6 号

[72] 发明人 罗 超

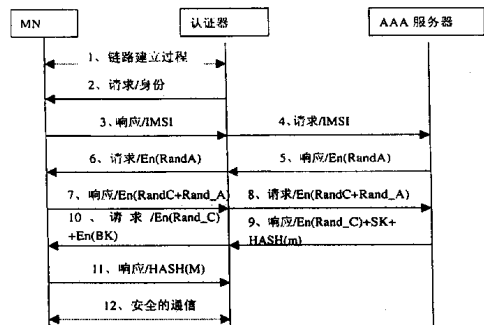
[74] 专利代理机构 成都天元专利事务所  
代理人 刘世权

权利要求书 2 页 说明书 11 页 附图 1 页

[54] 发明名称 一种基于对称密码算法的强鉴别方法

### [57] 摘要

本发明公开一种基于对称密码算法的强鉴别方法，步骤是通过无线链路建立，认证器向用户发送身份鉴别请求，并将其身份信息返回服务器，服务器从数据库中找到用户的鉴别密钥和消息完整性密钥，建立同用户会话，服务器与用户双方依次通过产生随机数并用用户的鉴别密钥加密，经认证器让对方用鉴别密钥解密，如此往复三次判断鉴别结果，服务器与用户通过生成会话密钥加、解密广播密钥，并用信息完整性密钥及相关信息计算整个鉴别交换完整性值，由认证器比较判断鉴别结果，决定用户可否入网，实现用户网上通信和基站对各用户的广播通信，优点是实现对用户、服务器双方认证，确保通信安全。



1、一种基于对称密码算法的强鉴别方法，包括有用户 MN 与 AAA 服务器共有鉴别密钥和进行消息完整性处理的消息完整性密钥，该两个密钥分配过程是一个带外过程，用户 MN 和认证器之间的通信是无线信道；认证器和 AAA 服务器之间通信协议采用 RADIUS 协议，并且采用 IPsec 或 TLS 或 CMS 来进行通信保护，其特征在于鉴别过程依次按如下步骤进行：

a、用户 MN 在某基站控制器的某扇区 SC 覆盖范围内开机，通过无线链路建立过程，获得无线传输通道资源；

b、认证器向用户 MN 发送身份请求，请求用户 MN 返回它的身份信息；

c、用户 MN 向认证器返回自己的 IMSI 身份响应信息，并且建立鉴别会话；

d、认证器根据用户 MN 的 IMSI 身份信息，向其对应的 AAA 服务器发送鉴别请求/IMSI；

e、AAA 服务器收到鉴别请求/IMSI 后，从相应的数据库中找到用户 MN 的鉴别密钥和消息完整性密钥，建立同用户 MN 的鉴别会话；AAA 服务器产生一个其长度一般同分组密码算法的分组长度一样的随机数 RandA，并用用户 MN 的鉴别密钥，采用分组密码算法的电子密码本 ECB 方式加密得到 En(RandA)，然后向认证器发送响应/En(RandA)；

f、认证器收到从 AAA 服务器发送来的响应/En(RandA)，然后向用户 MN 发送鉴别请求/En(RandA)；

g、用户 MN 收到 AAA 服务器通过认证器发送来的鉴别请求 En(RandA)，用自己的鉴别密钥解密获得 RandA，并通过 T 变换获得向 AAA 服务器发送的随机数响应 Rand\_A，同时产生一个其长度一般同分组密码算法的分组长度一样的随机数 RandC，将随机数 RandC 和随机数响应 Rand\_A 并置后用鉴别密钥加密产生 En(RandC+Rand\_A)，然后向认证器发送响应/En(RandC+Rand\_A)；

h、认证器收到用户 MN 发送来的鉴别响应/En(RandC+Rand\_A)，然后向 AAA 服务器发送鉴别请求/En(RandC+Rand\_A)；

i、AAA 服务器收到认证器发送来的鉴别请求/En(RandC+Rand\_A)，

首先用用户 MN 的鉴别密钥解密获得 RandC 和 Rand\_A, 比较 RandA 和 Rand\_A 是否一致, 如果不一致, 鉴别失败; 如果鉴别成功, AAA 服务器由随机数 RandC 通过 T 变换获得向 MN 发送的随机数响应 Rand\_C, 并用用户 MN 的鉴别密钥加密得到  $En(Rand\_C)$ , 然后将用户 MN 的身份信息 IMSI、随机数 RandA、RandC 通过 K 变换获得会话密钥 SK; 并且 AAA 服务器将 IMSI、RandA、RandC 和消息完整性密钥, 通过 MAC 计算得到整个鉴别交换完整性值  $HASH(m)$ ; 然后将响应/ $En(Rand\_C)+SK+HASH(m)$  发送给认证器;

j、认证器收到 AAA 服务器发送来的响应/ $En(Rand\_C)+SK+HASH(m)$ , 提取出会话密钥 SK 和  $HASH(m)$ ; 将广播密钥 BK 用会话密钥 SK 加密, 认证器然后向用户 MN 发送鉴别请求/ $En(Rand\_C)+En(BK)$ ;

k、用户 MN 收到认证器发送来的鉴别请求/ $En(Rand\_C)+En(BK)$ 后, 首先用鉴别密钥解密  $En(Rand\_C)$  获得随机数响应 Rand\_C, 比较自生随机数 RandC 和经 AAA 服务器变换产生的随机数响应 Rand\_C 是否一致, 如果一致, 则鉴别成功; 然后根据 IMSI、RandA、RandC 通过 K 变换获得会话密钥 SK, 解密  $En(BK)$  获得广播密钥 BK; 再根据用户身份信息 ISMI、随机数 RandA、随机数 RandC 和消息完整性密钥, 通过 MAC 计算得出整个鉴别交换完整性值  $HASH(M)$ ; 然后将响应  $HASH(M)$  发送给认证器。

L、认证器收到用户 MN 发来的响应  $HASH(M)$  后, 比较  $HASH(M)$  和  $HASH(m)$ , 如果一致, 则鉴别成功, 可以进行后续的处理。

## 一种基于对称密码算法的强鉴别方法

### 技术领域

本发明涉及在通信网络中，确保合法用户访问网络资源、避免其受到虚假服务器欺骗的一种验证用户与服务器双方合法身份的鉴别方法。

### 背景技术

在网络通信领域，使用最普遍的是通过 PPP 协议实现点到点链接传送数据，采用 CHAP 协议（Challenge Handshake Authentication Protocol）完成对 PPP 链接的身份鉴别，这种 CHAP 协议为质询—握手鉴别协议。链接双方通过点到点可扩展的链路控制协议，简称 PPPLCP 协议协商，对 PPP 链接进行配置和测试。在 PPP 链接建立后，先要对连接者的身份进行鉴别，然后依据鉴别结果，决定是否允许链接进入网络控制协议 NCP（Network Control Protocol）阶段的协商。CHAP 通过在 PPP 链接的双方进行一次“三次握手”，完成对对方的身份鉴别。其鉴别是在 PPPLCP 协议进入开状态（opened）后，鉴别方发起对对端的 CHAP 鉴别，其过程大致如下：

①鉴别方向被鉴别方发出 CHAP 质询，质询数据是一个随机数或伪随机数。

②被鉴别方收到 CHAP 质询后，将质询数据，共享密码等信息依据一定的计算规则，求出一个单向散列值作为对质询的应答发送给鉴别方。

③鉴别方收到应答后，在本地也依据相同的计算规则，利用共享密钥，质询数据等信息计算出一个期待的散列值，比较 CHAP 应答结果与期待的散列结果，若一致，则被鉴别方通过身份鉴别，否则为鉴别失败。

CHAP 协议主要适用于网络访问服务器 NAS(Network Access Server)对来自公共交换电话网 PSTN 或综合业务数字网 ISDN 的电路交换连接，拨入连接或专有连接身份的鉴别。

由于 CHAP 协议只是一个单向鉴别协议即只对用户鉴别，而不是对用户与服务器间的双向鉴别协议，因此不能防止重放攻击。而且，CHAP 协议没有单独将身份鉴别提取出来，因而不能在漫游环境中使用。并且

CHAP 协议不支持会话密钥导出，不能用于随后的安全通信。

另一种在网络通信领域中使用最多的通信传输协议是 RADIUS 协议。

由于网络访问服务器 NAS，通过 Modem 池或其它接口与外界相连。用户通过这些接口进入网络分享信息和资源，就需要对通过这些接口进入网络的用户进行身份鉴别，完成对用户的授权访问。RADIUS (Remote Authentication Dial-up User Service) 正是为这一需要而设计的。它是一种在网络访问服务器与一个共享的鉴别服务器之间通信的规范。按照这种通信规范，网络服务器通过共享鉴别服务器对访问它的用户实现鉴别。NAS 和鉴别服务器依据规范交互它们的鉴别信息，授权信息和配置信息。RADIUS 还给出了鉴别服务器和鉴别客户端（即 NAS 或认证器）对信息的处理规范，通过这些处理规范完成对访问 NAS 的客户的鉴别，授权和配置。

概括地说，RADIUS 鉴别协议有如下主要特征：

#### 1)、客户机/服务器模型

RADIUS 将 NAS 作为客户端。客户端的主要任务是完成与访问用户的交互（目的在于收集用户鉴别信息），向服务器发送收集到的鉴别信息以及对服务器发送回的鉴别结果进行应答。鉴别服务器端称为 RADIUS 鉴别服务器，它依据客户端发送的用户鉴别请求数据，对用户身份进行鉴别，并返回鉴别结果。

#### 2)、网络安全性

RADIUS 服务器与 NAS 之间共享一对秘密密钥。它们之间的所有通信都受到这对密钥的鉴别保护，同时提供一定的完整性保护。在该服务器与 NAS 之间传递的敏感数据（如用户口令）还受到机密性保护。RADIUS 协议还提供了状态属性以及鉴别器 (Authenticator)，以防止对客户端或服务器的拒绝攻击、欺骗攻击。RFC3162 定义了 RADIUS 使用 IPSEC 即 IP 安全协议栈，但是对 IPSEC 的支持却不要求。

#### 3)、可扩展的协议设计

RADIUS 数据包通过一个相对固定的消息头和一系列属性构成。属性采用《属性类型、长度、属性值》三元组组成，用户可以自行定义其它的属性，以扩展 RADIUS 鉴别协议。

#### 4)、灵活的鉴别机制

RADIUS 协议支持不同的鉴别协议，以实现对需要进行鉴别的用户进行鉴别。鉴别的协议包括 PAP、CHAP、MS-CHAP 等，在 RFC2869 RADIUS Extensions 中也定义了支持 EAP 鉴别协议。

RADIUS 实现身份鉴别的流程：

当用户拨入 NAS，NAS 请求 RADIUS 服务器进行用户身份鉴别，在获得 RADIUS 准入回应后，用户得到希望的服务。其大致流程如下：

①拨入用户与 NAS 建立 PPP（也可能为其它协议，如 SLIP）连接，NAS 要求用户出示鉴别信息。要求出示的方式可能是一个自定义的登陆通知，以要求用户键入用户名及用户口令，或者是通过 PPP 协议的鉴别协议，如 CHAP 等链路成帧协议传送用户的名信息和口令信息。

②拨入用户向 NAS 出示鉴别信息。

③NAS 依据这些鉴别信息，构造了一个称为“Access-Request”（即访问请求）的 RADIUS 消息，发送给 RADIUS 服务器。Access-Request 消息中应包含以下内容：用户名、用户口令、NAS 名信息（用做 RADIUS 使用哪一共享密钥的依据）、用户访问的端口号等信息。其中用户口令应受到机密性保护。

④对于一个 NAS，往往配有一台主 RADIUS 服务器以及数台备用 RADIUS 服务器。如果 NAS 在发出 Access-Request 一定时间后仍不能收到回应，则 NAS 可认为该主服务器不可达。因此 NAS 可以选择与第二台备用服务器联系。选择规则没有在 RADIUS 协议中给出：协议实现可以在 NAS 重发请求一定次数失败后选择第二台服务器，也可以循环选择服务

器。比如在等待主服务器应答失败后，立即选择第二台，在等待第二台应答失败后，立即选择第三台…

⑤在 RADIUS 服务器收到 Access-Request 之后，首先依据 NAS 的名信息找到本服务器与 NAS 之间的共享密钥。如果不能找到（例如 NAS 名不合法），则访问请求应被丢弃；如果能找到，则利用共享密钥验证数据的完整性、合法性等。然后依据请求中的用户名在 RADIUS 鉴别数据库中查找相应的用户条目。该条目中给出了用户可以访问的资源，以及为访问这些资源所必须满足的条件，如必须出示的口令信息等。RADIUS 依据鉴别信息逐一地验证用户是否满足所有的鉴别条件。

⑥如果用户不能通过所有的验证，则 RADIUS 给 NAS 发送回一条“Access-Reject”（访问拒绝）消息，表示用户不能通过验证。NAS 依据此消息，拒绝为用户提供所需的服务。

⑦如果一切验证都通过，RADIUS 向 NAS 发送一条“访问接受”（Access-Accept）消息或者对用户进行新一轮的质询。如果需要新一轮的质询。则 RADIUS 服务器向 NAS 发送一条“访问质询”（Access-Challenge）消息，这个消息中给出一组数据，要求用户对数据进行相应密钥的加密。NAS 在收到此质询后，将质询信息发送给拨入用户，用户进行相应加密，并将结果发送给 NAS。NAS 依据用户的返回结果构造新的一个“访问”请求，并发送给 RADIUS 服务器。服务器对这个质询应答进行验证，若验证通过，则给 NAS 发送一条“访问接受”消息。

⑧访问接受消息中应包含可为用户提供的服务（如 PPP 或 Telnet 服务）类型，相应的配置信息（如对 PPP 的 IP 地址，子网掩码等）。NAS 接收到此消息后，对本地环境进行配置，并启动对拨入用户的相应服务。

关于 RADIUS 鉴别协议的通信规范在这里就不进行具体描述。可以参看 RFC2856、RFC2866、RFC2867、RFC2868、RFC2869、RFC2809 等标准。

RADIUS 主要用于拨号 PPP 和终端服务器访问。随着时间的推移，不断增加的互联网和引入新的访问技术，包括无线、DSL、移动 IP 和以太网，路由器和网络服务器（NAS）使复杂度和密度增加。单纯的 RADIUS 协议已经不能满足 AAA 服务器在鉴别、授权、计费方面的新要求。

RADIUS 协议存在的问题：

错误恢复问题：RADIUS 协议不支持错误恢复 failover 机制，结果是不同的实现有不同的 failover。

传输级安全问题：RADIUS 定义了响应分组中要求应用层鉴别和完整性的方案。而 RADIUS 扩展协议中定义了一个附加的鉴别和完整性机制，并且仅仅要求在扩展鉴别协议（EAP）会话中要求。虽然属性隐藏支持，RADIUS 不提供每个分组的机密性。在计费时，RADIUS 计费假设重放保护由后端的帐单服务器提供，而不是在协议自己中提供。

可靠的传输问题：RADIUS 运行在 UDP 上，并且没有定义重传的行为；其结果是，可靠性随不同的实现而变化。这在计费的时候将是问题，分组的丢失将直接导致收入丢失。

代理支持问题：RADIUS 不提供对代理的明显支持，包括代理人、重定向和中继。因为期望的行为没有定义，不同的实现是不同的。

服务器发起的消息问题：前面提到了 RADIUS 采用客户机/服务器模型，虽然在动态鉴别中定义了 RADIUS 服务器发起的消息，但是支持却是可选的。这在实现像非请求的连接断开或跨异质的网络中按需的重新鉴别/重新授权是很难实现的。

可审计性问题：RADIUS 没有定义数据对象安全机制，其结果是不可信的代理可以修改属性或分组头而不被发现。连同对能力协商的支持，这在发生争执时很难确定。虽然数据对象安全的实现在 DIAMETER 不是必须的，但是能力协商是支持。

能力协商问题：RADIUS 不支持错误处理、能力协商、或为属性的必



须的/非必须的标志。因为 RADIUS 客户和服务器不知道相互之间的能力，它们不能够成功的协商双方之间的可接受服务，或者在一些情况下，甚至不能知道哪些服务被实现。

对方发现和配置问题：RADIUS 实现典型的要求服务器或客户的名字和地址的手工配置，连同相应的共享秘密。这将导致大的管理负荷，并且创建模板来重新使用 RADIUS 共享秘密，这将导致安全脆弱。

**综上所述单纯使用 CHAP 协议进行身份认证、使用 RADIUS 协议进行信息传输、都不能解决移动通信中用户和网络之间的双向鉴别问题，不能有效防止物理层的窃听，重放攻击、字典攻击、存在用户和接入服务器 NAS 或认证器之间的通信安全隐患。**

#### 发明内容

在现代的通信网络中，用户要访问网络资源，首先要进行用户入网认证，其鉴别的过程就是验证用户身份的合法性，鉴别完成后才能对用户访问网络资源进行授权，并对用户访问网络资源进行计费管理。一般来讲，鉴别过程由三个实体来完成：移动节点 MN 或称用户、认证器（Authenticator，在接入网络访问服务器 NAS 中实现）、AAA 服务器（Authentication、Authorization 和 Accounting，鉴别、授权和计费服务器）。用户 MN 与认证器间为无线信道连接；认证器与 AAA 服务器间为有线信道连接，二者间的通信传输协议为 RADIUS 协议。

本发明的目的在于：提供既有 AAA 服务器对用户 MN 入网身份合法性进行鉴别，防止物理层窃听、重放攻击、抵御字典攻击，也有用户 MN 对 AAA 服务器进行真实性鉴别，有效进行自我保护，实现第三代移动通信中，用户和接入服务器或认证器之间安全通信的一种基于对称密码算法的强鉴别方法。

本发明的目的是通过下述鉴别过程来实现的：

一种基于对称密码算法的强鉴别方法,包括有用户 MN 与 AAA 服务器共有鉴别密钥和进行消息完整性处理的消息完整性密钥,该两个密钥分配过程是一个带外过程,用户 MN 和认证器之间的通信是无线信道;认证器和 AAA 服务器之间通信协议采用 RADIUS 协议,并且采用 IPsec 或 TLS 或 CMS 来进行通信保护,其特征就在于鉴别过程依次按如下步骤进行:

a、用户 MN 在某基站控制器的某扇区 SC 覆盖范围内开机,通过无线链路建立过程,获得无线传输通道资源;

b、认证器向用户 MN 发送身份请求,请求用户 MN 返回它的身份信息;

c、用户 MN 向认证器返回自己的 IMSI 身份响应信息,并且建立鉴别会话;

d、认证器根据用户 MN 的 IMSI 身份信息,向其对应的 AAA 服务器发送鉴别请求/IMSI;

e、AAA 服务器收到鉴别请求/IMSI 后,从相应的数据库中找到用户 MN 的鉴别密钥和消息完整性密钥,建立同用户 MN 的鉴别会话;AAA 服务器产生一个其长度一般同分组密码算法的分组长度一样的随机数 RandA,并用用户 MN 的鉴别密钥,采用分组密码算法的电子密码本 ECB 方式加密得到 En(RandA),然后向认证器发送响应/En(RandA);

f、认证器收到从 AAA 服务器发送来的响应/En(RandA),然后向用户 MN 发送鉴别请求/En(RandA);

g、用户 MN 收到 AAA 服务器通过认证器发送来的鉴别请求 En(RandA),用自己的鉴别密钥解密获得 RandA,并通过 T 变换获得向 AAA 服务器发送的随机数响应 Rand\_A,同时产生一个其长度一般同分组密码算法的分组长度一样的随机数 RandC,将随机数 RandC 和随机数响应 Rand\_A 并置后用鉴别密钥加密产生 En(RandC+Rand\_A),然后向认证器发送响应/En(RandC+Rand\_A);

h、认证器收到用户 MN 发送来的鉴别响应/En(RandC+Rand\_A),然后向 AAA 服务器发送鉴别请求/En(RandC+Rand\_A);

i、AAA 服务器收到认证器发送来的鉴别请求/En(RandC+Rand\_A),首先用用户 MN 的鉴别密钥解密获得 RandC 和 Rand\_A,比较 RandA 和 Rand\_A 是否一致,如果不一致,鉴别失败;如果鉴别成功,AAA 服务器由随机数 RandC 通过 T 变换获得向 MN 发送的随机数响应 Rand\_C,并用用户 MN 的鉴别密钥加密得到 En(Rand\_C),然后将用户 MN 的身份信息

IMSI、随机数 RandA、RandC 通过 K 变换获得会话密钥 SK；并且 AAA 服务器将 IMSI、RandA、RandC 和消息完整性密钥，通过 MAC 计算得到整个鉴别交换完整性值 HASH (m)；然后将响应/En(Rand\_C)+SK+HASH(m) 发送给认证器；

j、认证器收到 AAA 服务器发送来的响应/En(Rand\_C)+SK+HASH(m)，提取出会话密钥 SK 和 HASH (m)；将广播密钥 BK 用会话密钥 SK 加密，认证器然后向用户 MN 发送鉴别请求/En(Rand\_C)+En(BK)；

k、用户 MN 收到认证器发送来的鉴别请求/En(Rand\_C)+En(BK)后，首先用鉴别密钥解密 En(Rand\_C) 获得随机数响应 Rand\_C，比较自生随机数 RandC 和经 AAA 服务器变换产生的随机数响应 Rand\_C 是否一致，如果一致，则鉴别成功；然后根据 IMSI、RandA、RandC 通过 K 变换获得会话密钥 SK，解密 En(BK) 获得广播密钥 BK；再根据用户身份信息 ISMI、随机数 RandA、随机数 RandC 和消息完整性密钥，通过 MAC 计算得出整个鉴别交换完整性值 HASH (M)；然后将响应 HASH (M) 发送给认证器。

L、认证器收到用户 MN 发来的响应 HASH (M) 后，比较 HASH (M) 和 HASH (m)，如果一致，则鉴别成功，可以进行后续的处理。

本发明的优点在于：实现了 AAA 认证体系的鉴别过程，可用于 MN 接入服务。采用对称分组密码算法足够的算法强度和鉴别过程实体构成的特点，以及秘密只由用户和 AAA 服务器拥有巧妙的完成了鉴别过程，并使鉴别过程足够简单，鉴别过程是一个强保密鉴别过程。在 AAA 认证体系中采用本方法，将使系统管理容易，其密钥管理复杂度为  $O(n)$ 。本发明的鉴别方法是双向的鉴别，既有用户对 AAA 服务器的鉴别，也有 AAA 服务器对用户的鉴别；能够进行自我保护，能够防止物理层的窃听，防止重放攻击，能够抵御字典攻击，能够产生会话密钥或者分配会话密钥，用于用户和接入服务器 NAS 之间的安全通信。

## 附图说明

图 1 为本发明双向身份鉴别方法过程图

图 2 为本发明通信过程流程图

图中标记**死亡**指物理连接不存在状态；标记**建立**表示链路建立状态；标记**认证**表示鉴别过程或鉴别成功或鉴别失败，标记**网络**表示可使用网络资源，标记**终止**表示通信终止状态。

## 具体实施方式

在本段中主要描述发明的鉴别方法在 PPP 协议中的具体实施应用的

例子。

为了通过点对点链路建立通信，PPP 链路的每一端，必须首先发送 LCP 分组以便来设定和测试数据链路。在链路建立好之后，对端才可以被鉴别。然后，PPP 必须发送 NCP 分组以便选择和设定一个或更多的网络层协议。一旦每个被选择的网络层协议都被设定好了，来自每个网络层协议的数据包就能在链路上发送了。链路将保持通信配置不变，直到直接的 LCP 和 NCP 分组关闭链路，或者是发生一些外部事件的时候（休止状态的定时器期满或者网络管理员干涉）。在设定、维持和终止点对点链路的过程里，PPP 链路经过几个清楚的阶段，如图 2 所示。这张图并没有给出所有的状态转换。

### 链路死亡（物理连接不存在）

链路一定开始并结束于这个阶段。当一个外部事件（例如载波侦听或网络管理员设定）指出物理层已经准备就绪时，PPP 将进入链路建立阶段。在这个阶段，LCP 自动机器将处于初始状态，向链路建立阶段的转换将给 LCP 自动机器一个 UP 事件信号。注意：在与调制解调器断开之后，链路将自动返回这一阶段。在用硬件实现的链路里，这一阶段相当的短——仅够侦测设备的存在。

### 链路建立阶段

LCP 用于交换配置信息分组（Configure packets），建立连接。一旦一个配置成功信息分组（Configure-Ack packet）被发送且被接收，就完成了交换，进入了 LCP 开启状态。所有的配置选项都假定使用默认值，除非被配置交换所改变。

有一点要注意：只有不依赖于特别的网络层协议的配置选项才被 LCP 配置。在网络层协议阶段，独立的网络层协议的配置由独立的网络控制协议（NCP）来处理。

在这个阶段接收的任何非 LCP 分组必须被悄悄的丢弃。收到 LCP

Configure-Request (LCP 配置要求) 能使链路从网络层协议阶段或者认证阶段返回到链路建立阶段。

## 鉴别阶段

在一些链路上, 在允许网络层协议分组交换之前, 链路的一端可能需要对端被鉴别。默认的鉴别是不需要强制执行的。如果一次执行希望对端根据某一特定的鉴别协议来鉴别, 那么它必须在链路建立阶段要求使用该鉴别协议。应该尽可能在链路建立后立即进行鉴别。而链路质量检查可以同时发生。在一次执行中, 禁止因为交换链路质量检查分组而不确定地将鉴别向后推迟这一做法。在鉴别完成之前, 禁止从鉴别阶段前进到网络层协议阶段。如果鉴别失败, 被鉴别方应该跃迁到链路终止阶段。在这一阶段里, 只有链路控制协议、鉴别协议, 和链路质量监视协议的分组是被允许的。在该阶段里接收到的其他的分组必须被悄悄的丢弃。注意: 在实现中, 仅仅是因为超时或者没有应答就造成鉴别的失败是不应该的。鉴别应该允许某种再传输, 只有在若干次的鉴别尝试失败以后, 不得已的时候, 才进入链路终止阶段。在鉴别中, 哪一方拒绝了另一方的鉴别, 哪一方就要负责开始链路终止阶段。

本发明中的鉴别方法就在本阶段使用。

## 网络层协议阶段

一旦 PPP 完成了前面的阶段, 每一个网络层协议 (例如 IP, IPX, 或 AppleTalk) 必须被适当的网络控制协议 (NCP) 分别设定。每个 NCP 可以随时被打开和关闭。注意: 因为一次实现最初可能需要大量的时间用于链路质量检测, 所以当等待 peer 设定 NCP 的时候, 执行应该避免使用固定的超时。当一个 NCP 处于 Opened 状态时, PPP 将携带相应的网络层协议分组。当相应的 NCP 不处于 Opened 状态时, 任何接收到的被支持的网络层协议分组都将被悄悄的丢弃。注意: 当 LCP 处于 Opened 状态时, 任何不被该执行所支持的协议分组必须在 Protocol-Reject 里返回。只

有支持的协议才被悄悄的丢弃。

在这个阶段，链路通信量由 LCP，NCP，和网络层协议分组的任意可能的联合组成。

## 链路终止阶段

PPP 可以在任意时间终止链路。引起链路终止的原因很多：载波丢失、鉴别失败、链路质量失败、空闲周期定时器期满、或者管理员关闭链路。LCP 用交换 Terminate（终止）分组的方法终止链路。当链路正被关闭时，PPP 通知网络层协议，以便他们可以采取正确的行动。交换 Terminate（终止）分组之后，执行应该通知物理层断开，以便强制链路终止，尤其当鉴别失败时。Terminate-Request（终止-要求）的发送者，在收到 Terminate-Ack（终止-允许）后，或者在重启计数器期满后，应该断开连接。收到 Terminate-Request 的一方，应该等待对端去切断，在发出 Terminate-Request 后，至少也要经过一个 Restart time（重启时间），才允许断开。PPP 应该前进到链路死亡阶段。

在本阶段收到的任何非 LCP 分组，必须被悄悄的丢弃。注意：LCP 关闭链路就足够了，不需要每一个 NCP 发送一个终止分组。相反，一个 NCP 关闭却不足以引起 PPP 链路的终止，即使那个 NCP 是当前唯一一个处于 Opened 状态的 NCP。

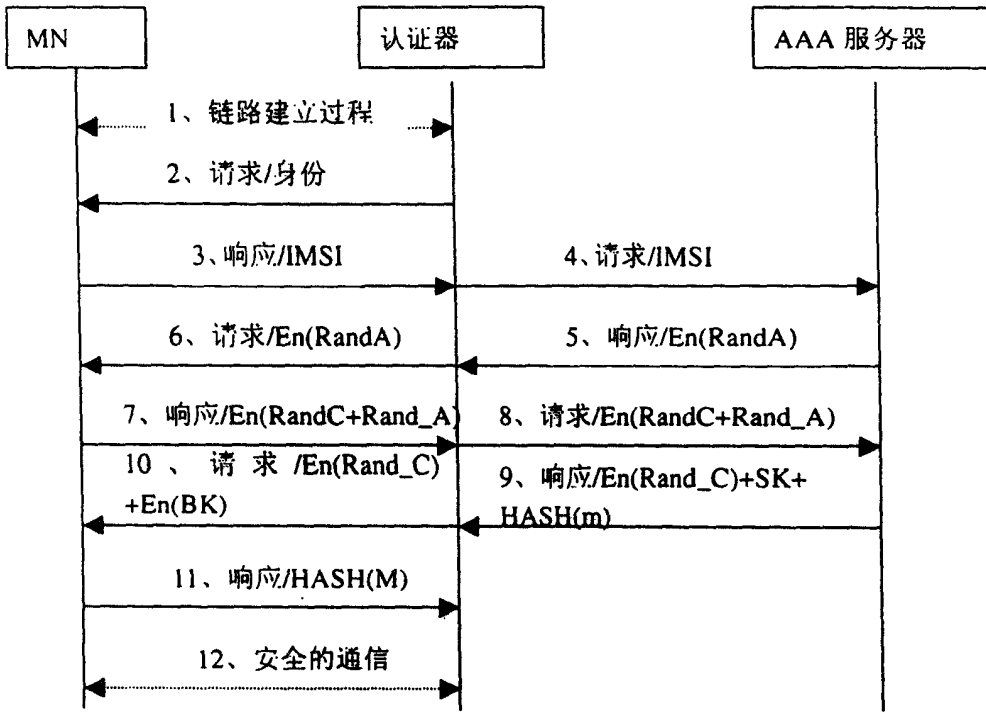


图 1

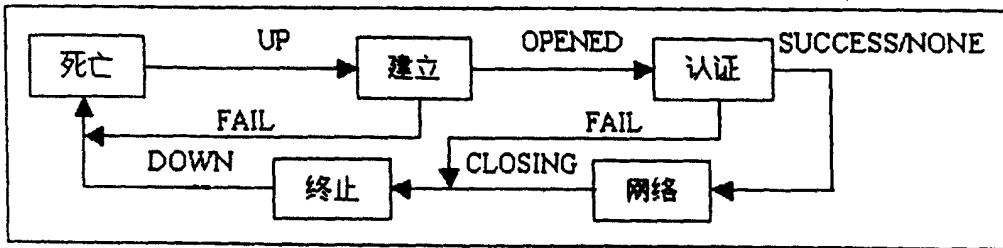


图 2