[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/38 (2006.01)

[12] 发 明 专 利 说 明 书

专利号 ZL 200410025973.7

[45] 授权公告日 2007 年 1 月 31 日

[11] 授权公告号 CN 1298194C

[22] 申请日 2004.3.22
[21] 申请号 200410025973.7
[73] 专利权人 西安电子科技大学
地址 710071 陕西省西安市太白路 2 号
[72] 发明人 马建峰 赖晓龙 孙军帅 王卫东
史庭俊 彭志威 王 超
[56] 参考文献
WO00/79457A1 2000.12.28 G06F 17/60
WO00/11832A1 2000.3.2 H04L 9/00
CN1468024A 2004.1.14 H04Q 7/38
CN1479553A 2004.3.3 H04Q 7/38
审查员 冯美玉

[74] 专利代理机构 陕西电子工业专利中心
代理人 张问芬 王品华

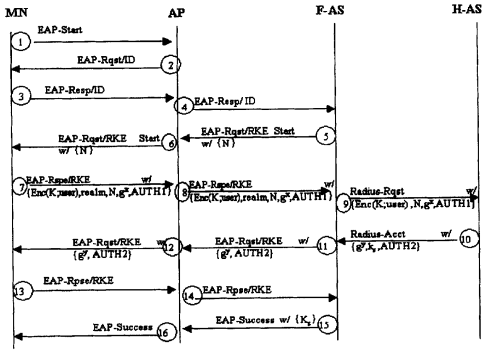
权利要求书 2 页 说明书 10 页 附图 2 页

[54] 发明名称

基于漫游密钥交换认证协议的无线局域网安全接入方法

[57] 摘要

一种基于漫游密钥交换认证协议的无线局域网安全接入方法(EAP－RKE)，用外地认证服务器 F－AS 代替家乡认证服务器 H－AS 向移动节点 MN 发出认证挑战，在移动节点 MN 与接入节点 AP 进行相互身份认证，建立共享密钥。移动节点 MN 的网络访问标识 NAI 是 user@realm，user 是用户身份，realm 是用户所属域；把 user 和 realm 分开，对 user 进行随机化加密，实现用户身份保护。本发明在保证安全性的前提下，使外地认证服务器 F－AS 和家乡认证服务器 H－AS 之间协议信息的交互轮数为 1 轮，提高了性能，同时保护了用户身份。当移动节点 MN 在家乡域和漫游在外地域时，都能够实现对移动节点 MN 的接入控制，而且可以保证移动节点安全地接入网络。



1．一种基于漫游密钥交换认证协议的无线局域网安全接入方法“EAP-RKE”，采用扩展认证协议 EAP 在移动节点 MN 与接入节点 AP 进行相互身份认证，协商建立共享密钥，其主要步骤包括开始认证、进行认证并建立共享密钥和完成认证；

所述开始认证包括：

1）移动节点 MN 把 EAP 开始消息发给接入点 AP；

2）接入点 AP 把请求移动节点身份的消息发送给移动节点 MN；

所述认证并建立共享密钥包括：

1）移动节点 MN 把响应身份请求的消息发送给接入节点 AP，但用户的身份为空；

2）接入节点 AP 把移动节点 MN 发送来的消息转发给外地认证服务器 F-AS；

3） 外地认证服务器 F-AS 向接入节点 AP 发送 EAP-RKE 开始的报文，要求开始 EAP-RKE 的认证，在消息中包含一个随机数 N，作为接入认证挑战标识；

4）接入节点 AP 把消息转发给移动节点 MN；

5）移动节点 MN 收到开始 EAP-RKE 认证的消息后，移动节点 MN 生成临时公私钥对，采用随机化加密的方法，用其临时公钥与家乡认证服务器 H-AS 的长期私钥计算身份加解密密钥，对移动节点 MN 的身份加密；所述加解密密钥为：$K=(g^x)^a$，式中，x、g^x 为 MN 的临时私钥、临时公钥；a 为 H-AS 的长期私钥；

6）移动节点 MN 将它加密后的身份、所属域 realm、外地认证服务器 F-AS 发来的认证挑战 N、移动节点 MN 的临时公钥和移动节点 MN 的签名发送给接入节点 AP；

7）接入节点 AP 将收到的消息转发给外地认证服务器 F-AS；

8）外地认证服务器 F-AS 根据消息中的所属域 realm 判断移动节点 MN 的家乡，如果移动节点是本地节点，则外地认证服务器 F-AS 就是移动节点的家乡认证服务器；如不是则将收到的消息传送给相应的移动节点的家乡认证服务器 H-AS；

9）家乡认证服务器 H-AS 收到消息后，解密得到移动节点 MN 的身份 user 并确定移动节点的长期公钥，然后利用该长期公钥验证移动节点的签名，若验证失败则终止协议；若验证通过，则家乡认证服务器 H-AS 生成自己的临时公私钥对，利用其临时私钥和移动节点 MN 的临时公钥计算出主密钥和会话密钥；

所述主密钥为：$K_{master}=(g^x)^y$

所述会话密钥为：$K_s=\mathrm{prf}(K_{master};\ 0)$

上式中，y 为 H-AS 的临时私钥；

10）家乡认证服务器 H-AS 利用认证挑战 N、移动节点 MN 的临时公钥“亦作为认证挑战”、家乡认证服务器 H-AS 的临时公钥“亦作为认证挑战” 及身份加解密密钥 K 计算出家乡认证服务器 H-AS 的身份鉴别消息 AUTH2=MAC（K；$N|g^x|g^y$），其中，g^y 为临时公钥，家乡认证服务器 H-AS 将它的身份鉴别消息 AUTH2、临时公钥 g^y 和会话密钥 K_S 发送给外地认证服务器 F-AS；

11）外地认证服务器 F-AS 把收到的消息中的会话密钥 K_S 删除，把剩余的“g^y，AUTH2”内容传送给接入节点 AP；

12）接入节点 AP 把收到的消息发给移动节点 MN；移动节点 MN 收到消息后验证家乡认证服务器的身份鉴别消息，验证失败则终止协议；验证通过后，移动节点 MN 利用自己的临时私钥和家乡认证服务器 H-AS 的临时公钥计算主密钥和会话密钥；

所述主密钥为：$K_{master}=(g^y)^x$

所述会话密钥为：K_s= prf（K_{master}； 0）；

所述完成认证包括：

1）移动节点 MN 把 EAP 响应消息发送给接入节点 AP；

2）接入节点 AP 把消息转发给外地认证服务器 F-AS；

3）外地认证服务器 F-AS 把认证成功的消息发送给接入节点 AP，消息中含有会话密钥；

4）接入节点 AP 把认证成功的消息发送给移动节点 MN。

2．根据权利要求 1 所述的基于漫游密钥交换认证协议的无线局域网安全接入方法，其特征在于移动节点在家乡域和漫游到外地域都采用相同的接入方法，即漫游对于移动节点是透明的。

3．根据权利要求 1 所述的基于漫游密钥交换认证协议的无线局域网安全接入方法，其特征在于所述移动节点 MN 将其身份与一个随机数关联，然后用家乡认证服务器 H-AS 的公钥对身份进行加密。

4．根据权利要求 1 所述的基于漫游密钥交换认证协议的无线局域网安全接入方法，其特征在于所述家乡认证服务器 H-AS 的身份鉴别消息采用如下方法产生，家乡认证服务器 H-AS 利用自己的私钥进行签名，生成家乡认证服务器 H-AS 的身份鉴别消息。

基于漫游密钥交换认证协议的无线局域网安全接入方法

技术领域

本发明属于无线通信安全技术领域，具体涉及一种基于漫游密钥交换认证协议的无线局域网安全接入方法（ EAP-RKE），为移动节点的本地接入和漫游接入提供安全保证。

术语

EAP－扩展认证协议（Extensible Authentication Protocol）

NAI－网络访问标识（Network Access Identifier）

RADIUS－远程认证拨号用户服务（Remote Authentication Dial In User Service）

AAA－认证、授权和审计（Authentication，Authorization，Accounting）

TLS－传输层安全（Transport Layer Security）

TTLS－隧道传输层安全（Tunneled TLS）

PEAP－保护可扩展身份验证协议（Protected EAP Protocol）

RKE－漫游密钥交换（Roaming Key Exchange）

MN－移动节点（Mobile Node）

AP－接入节点（Access Point）

AS－认证服务器（Authentication Server）

F-AS－外地认证服务器（Foreign Authentication Server）

H-AS－家乡认证服务器（Home Authentication Server）

KKS－已知密钥安全（Known Key Security）

PFS－完善前向保密（Perfect Forward Secrecy）

N-KCI－非密钥泄漏伪装（No Key Compromise Impersonation）

N-UKS－非未知密钥共享（No Unknown Key Share）

AVP－属性值对（Attribute Value Pairs）

MAC－消息认证码（Message Authentication Code）

WAI－无线局域网认证基础（WLAN Authentication Infrastructure）

背景技术

目前 IEEE 802.11 无线局域网是采用基于有线等价保密 WEP（Wired Equivalent Privacy）的方法进行无线终端的安全接入控制和无线链路上的数据保密。

因为基于 WEP 的无线局域网安全技术缺陷很大，目前提出了很多改进方法。其中基于

公钥技术的协议有 EAP-TLS(EAP Transport Layer Security)、EAP-TTLS(EAP Tunneled TLS Authentication Protocol)、PEAP(Protected EAP Protocol)和 GB15629.11 中使用的 WAI（WLAN Authentication Infrastructure）等。除了 WAI 以外，其他都是封装在扩展认证协议 EAP（Extensible Authentication Protocol）中的。

1．EAP-TLS

EAP-TLS 是一种基于 TLS(Transport Layer Security)的认证方式，由 RFC2716 给出。认证服务器与客户端采用 TLS 协议协商会话密钥，协议共五轮交互。它的分析如下：

1) 由于双方使用公钥证书进行认证，而且后续的消息都是在公钥的保护下进行的，攻击者即无法得到消息的真正内容，也无法篡改消息，同时利用随机数保证新鲜性，防止重放攻击。存在攻击方式可使双方协商一个强度较低的算法组；
2) 该协议要求双方都具有公钥证书，在公钥基础设施没有广泛部署时，在实践中操作起来比较困难；
3) 该协议不对用户身份进行保护，协议交互轮数为 5 轮。

2．PEAP

PEAP 消除了对移动节点公钥证书的要求，其认证过程分为两个阶段：第一阶段建立单向服务器认证的 TLS 隧道；第二阶段在该隧道保护下，对移动节点进行认证。该协议具有较好的扩展性和适应性，对于不同的移动节点可以采用相应的认证方式。其详细描述参见文献 http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-07.txt，Oct 2003。其分析如下：

1) 该协议消除了对移动节点公钥证书的要求，具有较好的扩展性，对于不同的移动节点可以采用适合的认证方式，具有很好的适应性。由于该协议的第一部分通过 EAP-TLS 建立了安全信道，在此安全信道的保护下，完成了对移动节点的认证，移动节点的身份可以得到保密；
2) 该协议不具备前向保密性 PFS 和非密钥泄漏伪装 N-KCI 的安全性质，协议交互轮数要大于 5 轮；

3．EAP-TTLS

EAP-TTLS 也是 IETF 的一个草案，它和 PEAP 非常相似，也是第一阶段建立服务器认证的 TLS 隧道，在该隧道保护下进行第二阶段对客户端的认证。

它们的不同在于第二阶段，TTLS 使用 TLS 隧道交换"attribute-value pairs" (AVP)，AVP 的格式非常类似于 RADIUS AVP 的格式。这种一般的编码方式使 TTLS 可以进行各种方式的认证，而不仅限于 EAP 支持的认证方式，还支持其他方式（CHAP, PAP, MS-CHAP and

MS-CHAPv2)。其详细描述参见

http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-03.txt, Aug 2003。它的协议流程和PEAP是一样的。

协议分析和PEAP相同。

4. WAI

国家知识产权局在2003年公开了一项发明专利申请,(公开号:CN 14236200A) 此专利申请所涉及的专利在GB15629.11中应用,简称WAI。WAI采用公钥证书进行认证、密钥协商。当移动节点MN登录到无线接入点AP时,移动节点MN与无线接入点通过认证服务器AS进行双向认证;认证成功后,移动节点MN与无线接入点AP进行会话密钥协商,产生会话密钥。由于WAI没有采用EAP的形式,所以协议交互轮数为2轮。在移动节点漫游时,外地认证服务器和家乡认证服务器之间交互的消息为1轮。其分析如下:

1) 该协议认证部分和密钥协商部分逻辑上独立,在密钥更新时具有优势;

2) 该协议不具备身份保护的性质;

3) 移动节点MN和无线接入点AP可能生成不一致的会话密钥。

上述协议都存在明显不足。EAP-TLS虽然具有较高的安全性,却不能提供身份保护;EAP-TTLS和PEAP改变TLS的使用方式,提供了身份保护,却失去了某些安全性质,并且增加了协议交互轮数;WAI虽然协议的交互轮数少,但是WAI在接入节点AP上的公钥运算数量过多,影响了AP的性能,而且不能提供身份保护及会话密钥的一致性;在无线网环境下,用户受到的安全威胁要大于有线网,所以不能牺牲安全性来获得其他利益;但是对于无线移动用户,其身份又是需要保密的。综上所述,目前的已有技术既不能完全满足无线环境对安全性的要求,也不能满足漫游对协议的性能要求。

发明内容

本发明的目的在于克服上述已有技术的不足,提供一种基于漫游密钥交换认证协议的无线局域网安全接入方法(EAP-RKE),在保证协议安全性和计算性能的前提下,使认证协议具有身份保护的特性,并且在外地认证服务器F-AS和家乡认证服务器F-AS之间交互的消息为1轮,从而保证移动节点安全接入及满足在无线局域网的漫游要求。

为解决上述技术问题,本发明提供的技术方案是采用漫游密钥交换认证协议EAP-RKE,在移动节点MN与接入节点AP进行相互身份认证,协商建立共享密钥,其主要步骤包括开始认证、认证并建立共享密钥和完成认证;

所述开始认证包括：

1） 移动节点 MN 把 EAP 开始消息发给接入节点 AP；

2） 接入节点 AP 把请求移动节点的身份的消息发送给移动节点 MN。

所述认证并建立共享密钥包括：

1） 移动节点 MN 把响应身份请求的消息发送给接入节点 AP，但用户的身份为空；

2） 接入节点 AP 把移动节点 MN 发送来的消息转发给外地认证服务器 F-AS；

3） 外地认证服务器 F-AS 向接入节点 AP 发送 EAP-RKE 开始的报文，要求开始 EAP-RKE 的认证。在消息中包含一个随机数 N，作为接入认证挑战；

4） 接入节点 AP 把消息转发给移动节点 MN；

5） 移动节点 MN 收到开始 EAP-RKE 认证的消息后，移动节点 MN 生成临时公私钥对，用其临时公钥与家乡认证服务器 H-AS 的长期私钥计算身份加解密密钥，对移动节点 MN 的身份加密；并将加密后的身份、所属域 realm、外地认证服务器 F-AS 的发来的认证挑战 N、移动节点 MN 的临时公钥及其签名发送给接入节点 AP；

6） 接入节点 AP 将收到的消息转发给外地认证服务器 F-AS；

7） 外地认证服务器 F-AS 根据消息中的所属域 realm 判断移动节点 MN 的家乡，如果移动节点是本地节点，则外地认证服务器 F-AS 就是移动节点的家乡认证服务器；如不是则将收到的消息传送给相应的移动节点的家乡认证服务器 H-AS；

8） 家乡认证服务器 H-AS 收到消息后解密得到移动节点 MN 的身份 user 并确定移动节点的长期公钥，然后利用该长期公钥验证移动节点的签名，若验证失败则终止协议；若验证通过，则家乡认证服务器 H-AS 生成自己的临时公私钥对，利用其临时私钥和移动节点的临时公钥计算出主密钥和会话密钥；然后家乡认证服务器 H-AS 利用认证挑战 N、移动节点 MN 的临时公钥（亦作为认证挑战）和家乡认证服务器 H-AS 的临时公钥（亦作为认证挑战）及身份加解密密钥计算出家乡认证服务器 H-AS 的身份鉴别消息，最后家乡认证服务器 H-AS 将它的身份鉴别消息、它的临时公钥和会话密钥发送给外地认证服务器 F-AS；

9） 外地认证服务器 F-AS 把收到的消息中的会话密钥除去，把剩余的内容传送给接入节点 AP；

10） 接入节点 AP 把收到的消息转发给移动节点 MN；移动节点 MN 收到消息后，验证家乡认证服务器的身份鉴别消息，验证失败则终止协议；验证通过后，移动节点 MN 利用自己的临时私钥和家乡认证服务器 H-AS 的临时公钥计算主密钥和会

话密钥。

所述完成认证包括：

5） 移动节点 MN 把 EAP 响应消息发送给接入节点 AP；

6） 接入节点 AP 把消息转发给外地认证服务器 F-AS；

7） 外地认证服务器F-AS把认证成功的消息发送给接入节点AP，消息中含有会话密钥；

8） 接入节点 AP 把认证成功的消息发送给移动节点 MN。

根据本发明，移动节点 MN 在家乡域和漫游到外地域都采用相同的接入方法，即漫游对于移动节点是透明的。

根据本发明，所述移动节点 MN 加密的身份是指随机化加密的身份

上述移动节点 MN 随机化加密的身份可采用如下方法，移动节点 MN 将其身份与一个随机数关联，然后用家乡认证服务器 H-AS 的公钥加密。

上述家乡认证服务器 H-AS 的身份鉴别消息可以采用如下方法产生，家乡认证服务器 H-AS 利用自己的私钥进行签名，生成家乡认证服务器 H-AS 的身份鉴别消息。

本发明实现了家乡认证服务器 H-AS 和外地认证服务器 F-AS 之间的消息交互为 1 轮；主密钥由移动节点 MN 的临时私钥和家乡认证服务器 H-AS 的临时公钥计算产生，同时也由移动节点 MN 的临时公钥和家乡认证服务器 H-AS 的临时私钥计算产生，这两个计算得到的主密钥是一致的。

本发明和上述现有技术相比，具有以下优点：

1. 把用户身份 user 和用户所属域 realm 分开进行处理，实现了用户身份保护；
2. 移动节点和局域网之间认证协议交互为 4 轮，外地认证服务器 F-AS 和家乡认证服务器 H-AS 之间消息交互的为 1 轮，提高了协议性能；
3. 协议在 Canetti 和 Krawczyk 提出的安全模型下是可证明安全的。
4. 协议在 Canetti 和 Krawczyk 提出的安全模型下是可证明安全的，则协议就具有 KKS、PFS 和 N-UKS 的安全性质。而在协议中，通信双方都必须知道自己的私钥才能生成认证载荷，故协议也具有 N-KCI 的安全性质。

表 1 本发明与已有技术安全性比较

协议	身份保护	可证明安全性	PFS	KKS	N-KCI	N-UKS
EAP-TLS	N	*	Y#	Y	Y#	Y
PEAP	Y	*	Y#	Y	N	Y
EAP-TTLS	Y	*	Y#	Y	N	Y
WAI	N	*	N	Y	N	N
EAP-RKE	Y	Y	Y	Y	Y	Y

注：#指必须使用临时公私和签名的密钥交换算法

*表示未作

从表 1 的比较可以看出，本发明基于 EAP-RKE 的安全接入方法，其安全性能整体上大大优于现有技术。

附图说明

图 1 是本发明的 EAP-RKE 认证过程图

图 2 是本发明的安全认证系统的逻辑结构图

图 3 是本发明的移动节点在家乡 EAP-RKE 与 EAP-TLS 协议对通信的影响仿真对比图

图 4 是本发明的移动节点在外地 EAP-RKE 与 EAP-TLS 协议对通信的影响仿真对比图

图 1 中符号说明：

消息格式为：消息类型 w/{消息内容}。其中消息类型如下：

EAP-Start 开始扩展认证协议 EAP；

EAP-Rqst/RKE EAP-RKE 请求消息；

EAP-Resp/RKE EAP-RKE 响应消息；

EAP-Rqst/ID EAP 请求身份消息；

EAP-Resp/ID EAP 响应身份消息；

EAP-Rqst/RKE start 开始 EAP-RKE 协议消息；

Radius-Rqst Radius 协议请求消息；

Radius-Acct Radius 协议接受消息；

EAP-Success EAP 成功完成消息。

消息内容说明如下：

u 移动节点的私钥；

g^u 移动节点的公钥；

user	移动节点 MN 的用户身份；
realm	移动节点 MN 的所属域；
a	H-AS 的私钥；
g^a	H-AS 的公钥；
$Cert_A$	H-AS 的证书；
E（k；.）	密钥为 k 的对称加密的加密函数；
MAC（k；.）	密钥为 k 的消息认证码函数；
Sig	签名函数；
prf (k；.)	密钥为 k 的伪随机函数，用于会话密钥导出函数。

具体实施方式

下面结合附图和实施例对本发明作详细说明：

参见图 2，MN 是移动节点，AP 是接入节点，F-AS 和 H-AS 分别是外地和家乡认证服务器。

图 2 中的虚线表示逻辑上的安全连接，实线表示实际的物理连接。移动节点 MN 和它的家乡认证服务器 H-AS 共享安全联系（共享密钥或通过公钥证书）。接入节点 AP 和外地认证服务器 F-AS 存在安全信道，接入节点 AP 和外地认证服务器 F-AS 相互信任；外地认证服务器 F-AS 和家乡认证服务器 H-AS 也存在安全信道，外地认证服务器 F-AS 是被家乡认证服务器 H-AS 信任的，基于此，本发明用外地认证服务器 F-AS 代替家乡认证服务器 H-AS 向移动节点 MN 发出认证挑战，使外地认证服务器 F-AS 与家乡认证服务器 H-AS 之间的的消息交互为 1 轮得以实现。

当移动节点 MN 登录接入节点 AP，为实现 MN 的安全接入，需要移动节点 MN 和接入节点 AP 相互确认身份，并建立一个共享密钥。本发明采用 EAP-RKE 实现了身份认证和密钥协商，其身份认证和密钥建立实施方式如图 1 所示，具体包括如下步骤 ：

1．开始认证

1) 移动节点 MN 把 EAP 开始消息发给接入节点 AP；

2) 接入节点 AP 把请求移动节点 MN 的身份的消息发送给移动节点；

2．进行认证并建立共享密钥

1) 移动节点 MN 把响应身份请求的消息发送给接入节点 AP，但用户的身份为空；

2) 接入节点 AP 把移动节点 MN 发送来的消息转发给外地认证服务器 F-AS；

3) 外地认证服务器 F-AS 向接入节点 AP 发送 EAP-RKE 开始的报文，要求开始 EAP-RKE 的认证。在消息中包含一个随机数 N，作为接入认证挑战标识；

4) 接入节点 AP 把消息转发给移动节点 MN；

5) 移动节点 MN 收到开始 EAP-RKE 认证的消息后，生成临时私钥 x，临时公钥 g^x。用自己的临时公钥 g^x 与家乡认证服务器 H-AS 的长期私钥 a 计算出身份加解密密钥 K=（g^x）^{a}，对移动节点 MN 的身份加密。将它的加密身份 Enc（K；user）、所属域 realm、外地认证服务器 F-AS 发来的认证挑战 N、临时公钥 g^x 和移动节点 MN 的签名 AUTH1=Sigu（g^x|N| Enc（K；user））消息发送给接入节点 AP；

6) 接入节点 AP 把消息转发给外地认证服务器 F-AS；

7) 外地认证服务器 F-AS 根据消息中的所属域 Realm 判断移动节点 MN 的家乡，如果移动节点是本地节点，则外地认证服务器 F-AS 就是移动节点的家乡认证服务器 H-AS；如不是则把消息｛Enc（K；user），N，g^x，AUTH1｝传送给相应的移动节点的家乡认证服务器 H-AS；

8) 家乡认证服务器 H-AS 收到消息后，用自己的长期私钥 a 与移动节点 MN 的临时公钥 g^x 计算出身份加解密密钥 K=（g^x）^{a}，解密 Enc（K； user），得到移动节点 MN 的身份 user 并确定移动节点的长期公钥 g^u，然后家乡认证服务器 H-AS 利用该公钥 g^u 验证移动节点的签名认证载荷 AUTH1，若验证失败则终止协议；若验证通过，则家乡认证服务器 H-AS 产生临时私钥 y，临时公钥 g^y。家乡认证服务器 H-AS 利用自己临时私钥 y 和移动节点的临时公钥 g^x 计算出主密钥 $K_{master}=(g^x)^y$，会话密钥 K_s= prf（K_{master}；0）。然后家乡认证服务器 H-AS 利用身份加解密密钥 K 对认证挑战 N、移动节点 MN 的临时公钥 g^x （亦作为认证挑战）和家乡认证服务器 H-AS 的临时公钥 g^y（亦作为认证挑战）计算出家乡认证服务器 H-AS 的身份鉴别消息 AUTH2=MAC（K；N|g^x|g^y），然后家乡认证服务器 H-AS 将身份鉴别消息 AUTH2=MAC（K；N|g^x|g^y）、临时公钥 g^y 、会话密钥 K_s= prf（K_{master}；0）发送给外地认证服务器 F-AS。

9) 外地认证服务器 F-AS 把消息中的会话密钥 K_s 除去，把剩余的｛g^y，AUTH2｝传送给接入节点 AP；

10) 接入节点 AP 把消息转发给移动节点 MN。移动节点 MN 收到消息后，验证家乡认证服务器的身份鉴别消息 AUTH2，验证失败则终止协议；验证通过后，移动节点 MN 利用自己的临时私钥 x 和家乡认证服务器 H-AS 的临时公钥 g^y 计算主密钥 Kmaster=$(g^y)^x$，会话密钥 K_s= prf（K_{master}；0）；

3．完成相互认证和密钥协商，接入点 AP 获得与移动节点 MN 的共享密钥

1） 移动节点 MN 把 EAP 响应消息发送给接入节点 AP；

2） 接入节点 AP 把消息转发给外地认证服务器 F-AS；

3） 外地认证服务器 F-AS 把认证成功的消息发给接入节点 AP，消息中有会话密钥 K_s；

4） 接入节点 AP 把认证成功的消息发送给移动节点 MN。

至此，移动节点 MN 和接入节点 AP 完成了相互认证，并且得到了相同的会话密钥 K_s。换言之，完成了移动节点 MN 的安全接入。在上述认证、密钥协商过程中，采用外地认证服务器 F-AS 代替家乡认证服务器 H-AS 向移动节点 MN 发出挑战，实现外地认证服务器 F-AS 与家乡认证服务器 H-AS 之间信息交互为 1 轮。此外，移动节点 MN 和接入点 AP 身份认证和共享密钥的建立是同步进行的。

需要指出的是，上述基于 EAP-RKE 的接入方法既适用于移动节点 MN 在家乡域的接入，也适用于移动节点漫游到外地域的接入，即漫游对移动节点是透明的。

在图 1 所示的身份认证过程中，对移动节点 MN 身份加密的另一种实施方式是：

移动节点 MN 将其身份 user 与一个随机数 m 相关联，比如将 user 和 m 级联或者将 user 和 m 进行异或运算，然后用家乡认证服务器 H-AS 的公钥 g^a 加密。将加密后的身份和随机数 m 一并发送给家乡认证服务器 H-AS。

在图 1 所示的身份认证过程中，家乡认证服务器 H-AS 的身份鉴别的另一种实施方式是：

家乡认证服务器 H-AS 利用其私钥 a 进行签名，生成家乡认证服务器 H-AS 的身份鉴别消息。

EAP-RKE 性能比较

协议性能的一个重要方面是交互轮数。若交互轮数多，则协议完成需要的时间也多。而且随着 IEEE 802.11 无线局域网的发展，移动节点会在不同的管理域间漫游，在漫游过程中动节点可能会需要进行认证。

当移动节点漫游到外地网络之后，进行认证的最大延时是 F-AS 和 H-AS 之间的传输时延。而 EAP-TLS 的交互轮数为 5 轮，在漫游时要在 F-AS 和 H-AS 之间交互 2 轮。至于 EAP-TTLS，根据第二阶段采用的认证形式，交互轮数还要大于 EAP-TLS。因此，它们不满足要求，本发明采用 EAP-RKE 实现了的交互轮数为 4 轮，在 F-AS 和 H-AS 之间的传输消息仅为 1 轮。

为了形象的对比协议的性能，对协议的性能进行了仿真，对比协议是 EAP-TLS。采用 NS-2.26 作为仿真平台，工作在一台 PC 机上（C1.7G，256M RAM），操作系统为 Red Hat Linux 8.0。

认证对正常数据流的影响如图3、图4所示。图中横坐标为数据包的序列号，纵坐标为相邻两个数据包到达目的的时间差，单位为秒。实线表示EAP-TLS协议的情况，虚线表示

EAP-RKE协议的情况。图中的突出部分是认证协议引入的时延。

图 3 是移动节点在家乡域的情况，图 4 是移动节点在外地域的情况。

从图 3 和图 4 可以看出，协议认证时延大大优于 EAP-TLS，有力地证明本发明具有很好的性能并能大大提高 IEEE 802.11 WLAN 的漫游效率。

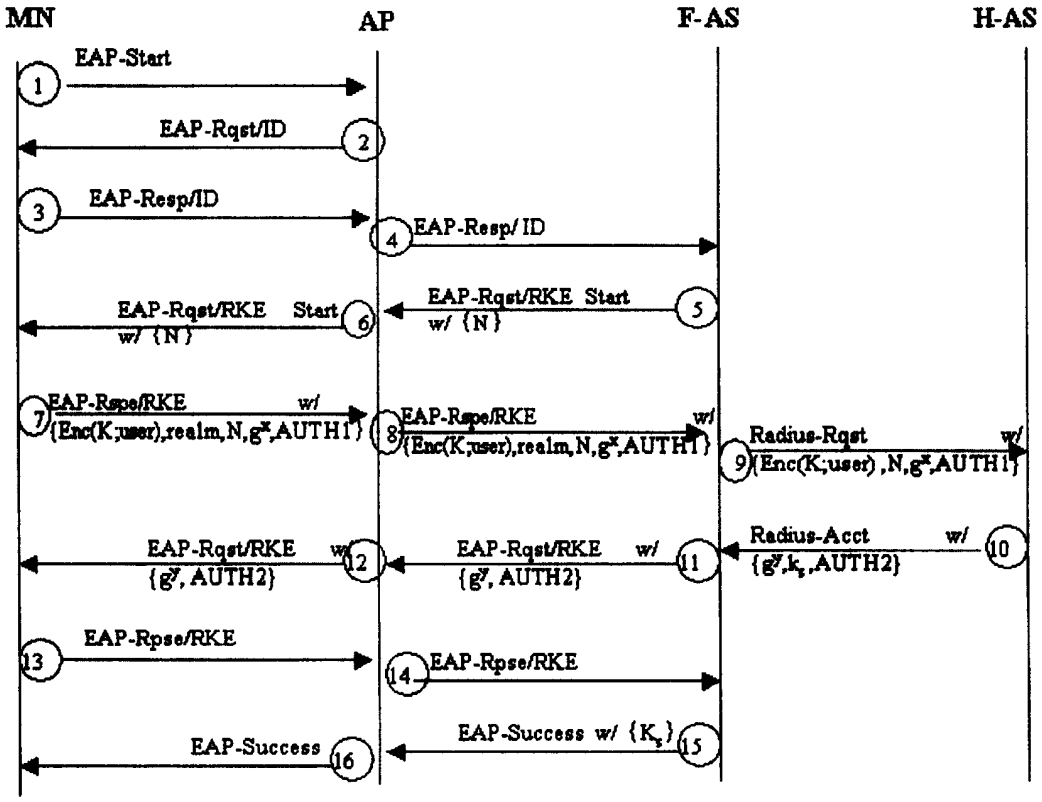

MN
AP
F-AS
H-AS
EAP-Start
EAP-Rqst/ID
EAP-Resp/ID
EAP-Resp/ ID
EAP-Rqst/RKE Start
w/ {N}
EAP-Rqst/RKE Start
w/ {N}
EAP-Rspe/RKE w/
{Enc(K;user),realm,N,g^x,AUTH1}
EAP-Rspe/RKE w/
{Enc(K;user),realm,N,g^x,AUTH1}
Radius-Rqst w/
{Enc(K;user),N,g^x,AUTH1}
EAP-Rqst/RKE w/
{g^y, AUTH2}
EAP-Rqst/RKE w/
{g^y, AUTH2}
Radius-Acct w/
{g^y,k_s,AUTH2}
EAP-Rpse/RKE
EAP-Rpse/RKE
EAP-Success w/ {K_s}
EAP-Success
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

图 1

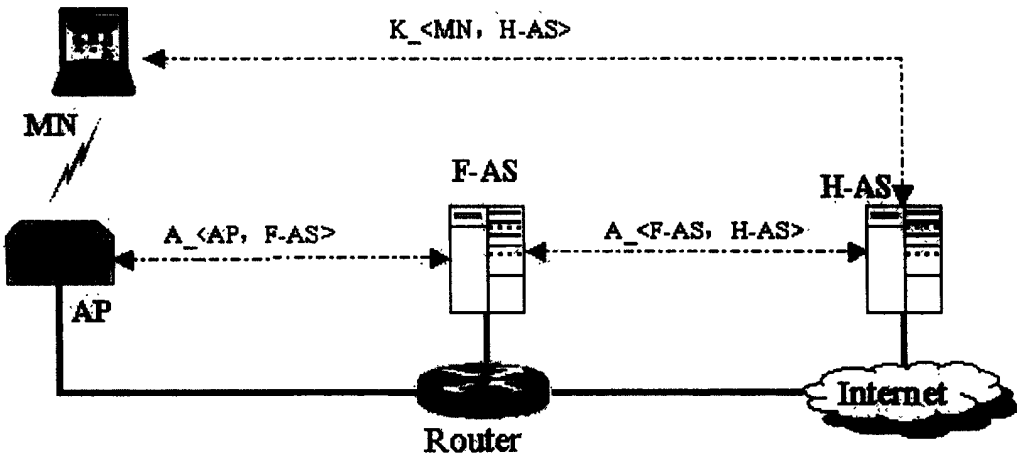

K_<MN，H-AS>
MN
F-AS
H-AS
A_<AP，F-AS>
A_<F-AS，H-AS>
AP
Internet
Router

图 2

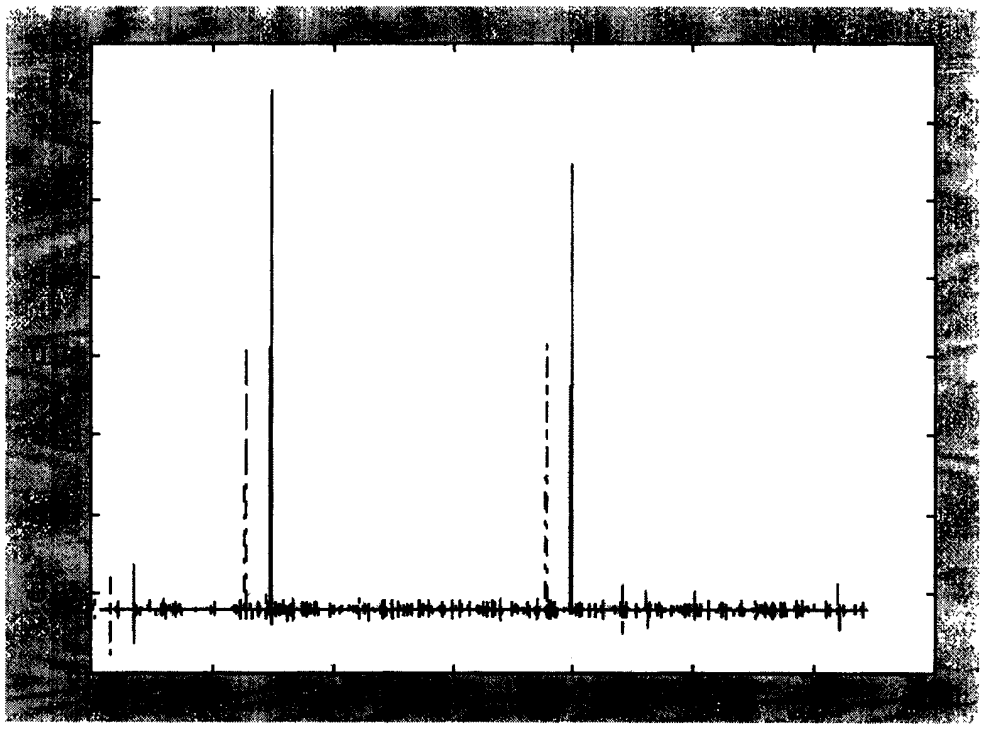


图 3

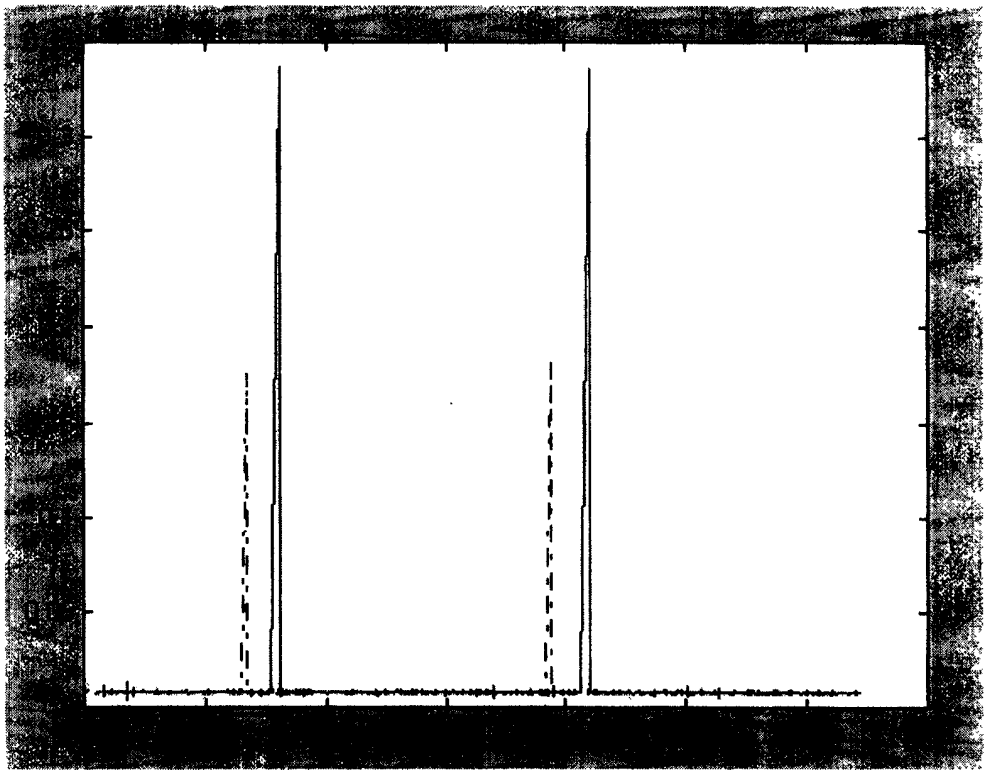


图 4