家庭基站设备的快速重认证方法

赖成喆，李 晖，张跃宇，曹 进

(西安电子科技大学通信工程学院 西安 710071)

【摘要】家庭基站是一种室内小型蜂窝基站，由于其设备部署在不可信的环境中，因此接入运营商的核心网时必须进行认证。3GPP组织已提出了使用IKEv2承载EAP-AKA/SIM的家庭基站设备的初始认证方法，该文基于3GPP标准提出一种家庭基站设备的快速重认证方法，在不降低原有安全级别的前提下，对初始认证进行优化，减少了通信开销，加快了认证的速度。对标准中的设施不做任何修改的情况下，使其在实际应用中便于实施。使用AVISPA对方案的安全性进行了分析，并在能量消耗和通信开销方面与初始认证进行了详细的比较，结果表明本方案性能良好。

关 键 词 3GPP; EAP-AKA; 家庭基站; 重认证; 安全

中图分类号 TN918 文献标识码 A doi:10.3969/j.issn.1001-0548.2012.05.007

Fast Re-Authentication Scheme for HeNB

LAI Cheng-zhe, LI Hui, ZHANG Yue-yu, and CAO Jin

(School of Telecommunications Engineering, Xidian University Xi'an 710071)

Abstract Home eNodeB (HeNB) is a small cellular base station, typically designed for use in a home or small business. Deployed in untrusted environments, HeNB must be authenticated when it accesses to operator's core network. 3GPP has presented a method that EAP-AKA runs within IKEv2 between HeNB and security gateway for mutual authentication of HeNB and core network. This paper proposes a fast re-authentication scheme based on 3GPP standard. The proposed procedures reduce significantly the authentication overhand and improve the authentication speed compared with the initial authentication, without compromising the provided security services. Moreover, the proposed method does not modify the infrastructure in 3GPP and can be applied easily to the HeNB system. A detailed analysis of security is made by using AVISPA. In addition, an analysis of energy cost is carried out that compares the energy consumption induced by re-authentication and initial authentication. Finally, an analysis of communication cost analysis is provided that estimates the cost improvement of proposed re-authenitication over the initial authentication procedure.

Key words 3GPP; EAP-AKA; HeNB; re-authentication; security

家庭基站(Femtocell)在3GPP组织(the 3rd Generation Partnership Project)的Rel-10中被定义为HeNB[1]。它是一种小型低功率蜂窝基站，被设计在家庭或小的商业机构中使用。家庭基站的引入带来一些新的安全问题[2]，为此，3GPP组织提出了一系列涉及家庭基站安全方面的解决方案[3]，包括家庭基站的设备鉴权以及移动用户的接入鉴权等。

其中，家庭基站的设备鉴权过程是非常重要的安全机制，它能够向核心网提供家庭基站设备的合法性证明。3GPP组织提出了一种使用IKEv2承载EAP-AKA/SIM的家庭基站设备的初始认证方法，但是没有给出重认证的实施方案。如果家庭基站设备在一台AAA服务器(认证、鉴权、计费服务器)已经进行过初始认证，那么当家庭基站需要再次在同一个AAA服务器下进行设备认证时，为了减少认证过程中的通信开销，需要采用重认证方法。在初始认证过程中会产生一些相关的认证信息，重认证过程正是重用初始认证中的某些认证信息，从而能够执行快速的认证过程，重认证是对初始认证的优化。在以前的工作中，一些方案已经考虑了实施重认证的方法[4-6]，但是这些方案提出了不同的认证框架，从而会对3GPP标准中的基础设施进行比较大的修改，不利于在实际中应用。本文基于家庭基站设备的初始认证过程，提出一种家庭基站设备的快速重认证方法，在不降低原有安全级别的前提下减少认证的信令流程，同时对3GPP标准中相关的设施不进

收稿日期：2011 – 02 – 25； 修回日期：2012 – 01 – 14
基金项目：国家自然科学基金(60772136，61102056)；中央高校基本科研业务费专项资金(JY10000901025)
作者简介：赖成喆(1985 –)，男，博士生，主要从事无线网络方面的研究.

行任何修改，以便在实际中部署和应用。

1 背景介绍

1.1 家庭基站系统的网络架构

本文基于3GPP标准中的网络架构[3]进行研究。家庭基站的网络结构如图1所示，其中包括：1) 家庭基站(HeNB)，3GPP标准中的小型低功率蜂窝基站与宏基站兼容，作为移动用户终端的室内无线接入点；2) 安全网关(Se-GW)，代表核心网对家庭基站执行认证操作，确保接入核心网的安全；3) 认证、鉴权、计费服务器(AAA server)，对家庭基站进行接入认证和鉴权；4) 归属用户服务器(HSS)，支持用于处理调用/会话的IMS网络实体的主要用户数据库。它包含用户配置文件，执行用户的身份验证和授权，并可提供有关用户物理位置的信息。

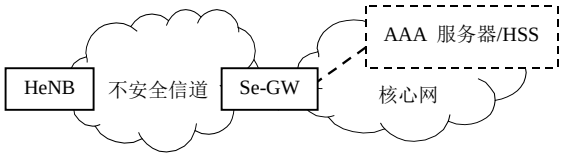

图1　家庭基站系统的网络架构

1.2 完整的家庭基站的设备鉴权流程

完整家庭基站的设备鉴权流程在 3GPP 的 33.820 中已经提出 [3]，采用的是 IPsec 协议中的 IKEv2[7]承载波 EAP-AKA/SIM[8]的方式进行双向认证，针对 IKEv2 的相关操作将在 3.2 节进行介绍，具体步骤如图 2 所示。在初始认证过程中，在 IKEv2 协议开始时，家庭基站和安全网关之间建立一个双向的 IKE 安全关联(IKE_SA)，用于保护接下来的 IKEv2 的消息(图 2 步骤 1～步骤 2)。在 IKE_SA 建立后，家庭基站和 AAA 服务器 [9]执行 IKEv2 承载 EAP-AKA 的流程进行双向认证(图 2 步骤 3～步骤 9)。

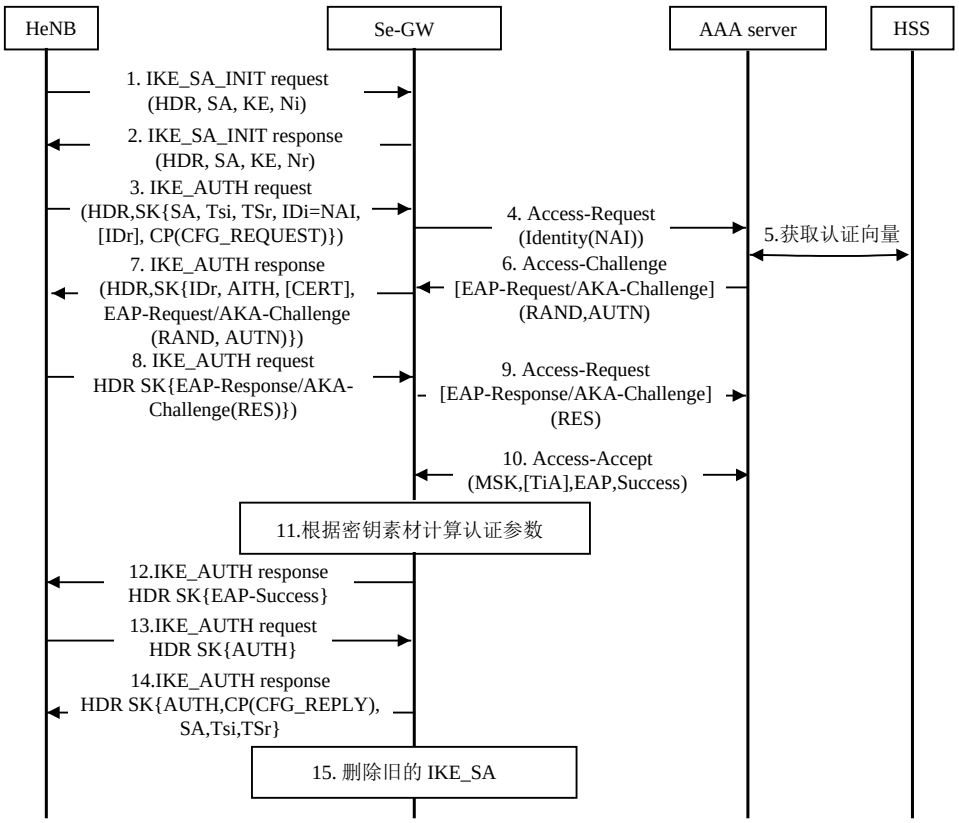

图2　家庭基站设备的初始认证流程

注意安全网关和AAA服务器之间使用的是Diameter协议[10]。在IKEv2协议的最后，一个基于IPsec的虚拟专用网(VPN)在家庭基站和安全网关之间被建立，它使用封装的安全负载(ESP)[11]以保护用户数据的机密性和完整性(图2步骤10～步骤15)。

2 快速重认证方案

2.1 对已有的家庭基站的设备鉴权流程的修改

为了实施重认证方案，需要对已有的家庭基站的设备鉴权流程进行一些修改。在图 2 的步骤 5 中，AAA 服务器收到 HSS 发送来的认证向量时，它将计算：

$$MSK = prf(Identity \mid IK \mid CK) \quad (1)$$

式中，“|”表示比特串的链接；prf是伪随机函数；Identity是家庭基站身份。在2.2节中，MSK仅作为计算认证参数AUTH的密钥素材。在本文方案中，利用MSK作为重认证时的认证参数，当AAA服务器计算出MSK后，进行如下操作：AAA服务器保存MSK，并对该MSK和对应的家庭基站身份进行绑定。在图2的步骤7中，家庭基站使用和网络侧相同的机制生成IK和CK，并使用公式(1)计算同样的MSK并保存。而在网络侧方面，除了AAA服务器需要保存重认证阶段所需的认证参数MSK外，不需要进行其他的修改。

2.2 家庭基站设备接入核心网的快速重认证

假设家庭基站已经在核心网进行过初始认证，需要再次接入核心网时，执行本文方案的重认证流程。

首先 HeNB 和 Se-GW 之间会直接使用 IKEv2 进行认证；随后，在家庭基站和安全网关之间建立一条安全通信信道(VPN)，用于保护它们之间的数据传输。具体步骤如下：

为了发起 IKEv2 协议，HeNB 向 Se-GW 发送 SAi1(定义了用于 IKE_SA 的所支持的密码算法集)、Kei(Diffie-Hellman 值)和 Ni(一个随机数)。其作用是，作为 IKEv2 中所使用的密码函数的输入，以确保密钥素材的新鲜性，防止重放攻击。Se-GW 的响应消息包含 SAr1(它对 SAi1 中的密码算法的选择)，为完成 Diffie-Hellman 选择的自己的 KEr 以及随机数 Nr。这样一来 HeNB 和 Se-GW 通过分享一个双向的 IKE_SA，就能为接下来的 IKEv2 消息提供机密和完整性服务(图 3 步骤 1～步骤 2)。

建立 IKE_SA 后，HeNB 向 Se-GW 发送自己的身份标识，SAi2(包含已经为 IPsec_SA 选择的 HeNB 所支持密码算法)，路径选择 traffic selectors(TSi 和 TSr)，允许通信双方在 IPsec 流程中确认数据包的流向。另外，HeNB 还将计算并向 Se-GW 发送一个认证参数 AUTHi，AUTHi 是使用已经储存的 MSK 所计算的 MAC 值，用于 HeNB 的重认证(图 3 步骤 3)。

随后 Se-GW 将把从 HeNB 收到的身份信息转发给 AAA 服务器，AAA 服务器通过检查建立了绑定关系的 MSK 和家庭基站身份，找到相应的 MSK，并把 MSK 发送给 Se-GW。需要注意的是，MSK 必须在安全的信道中传输。由于 Se-GW 和 AAA 服务器使用 Diameter 协议预先建立的安全信道，因此它们之间存在信任关系 [10](图 3 步骤 4～步骤 5)。

当 Se-GW 收到 MSK 后，将使用 MSK 计算一个 MAC 值和从 HeNB 收到的 AUTHi 进行匹配，从而对 HeNB 进行认证。之后，还将使用 MSK 计算认证参数 AUTHr。Se-GW 将发送 AUTHr、路径选择 traffic selectors(TSi 和 TSr)、SAr2(它对 SAi2 中的密码算法的选择)给 HeNB。为了完成整个认证过程，HeNB 使用自己的 MSK 用同样的方法验证收到的 AUTHr。最后，一条安全的通信信道被建立用于保护 HeNB 和 Se-GW 之间的数据传输安全。至此重认证过程结束(图 3 步骤 6)。

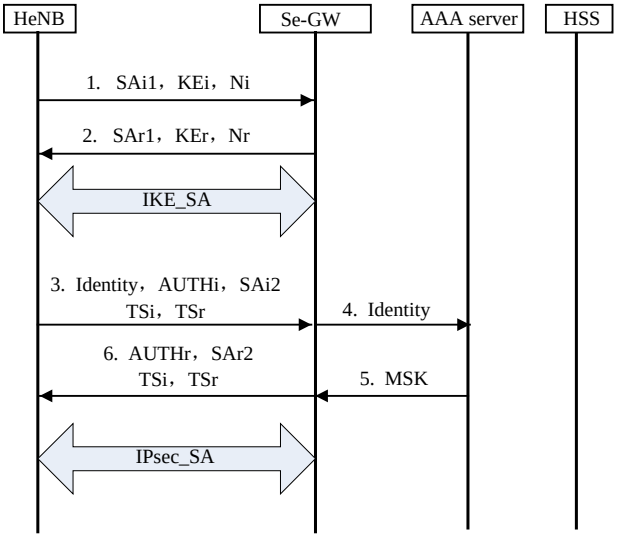

图3 家庭基站设备的重认证流程

3 对重认证方案的分析

3.1 安全性分析

使用 AVISPA[12]对本文方案提出的重认证方法进行安全性分析。由于 AAA 服务器和安全网关之间已经建立信任关系，因此只考虑家庭基站和安全网关之间协议的安全性。AVISPA 是一套建立和分析安全协议模型的工具，融合有 4 种侧重点不同的分析终端。它采用 HLPSL 语言，用户输入安全协议的参与者标识、运行环境、实现目标、攻击者能力等变量，并指定预期的安全属性建立安全协议的分析模型。使用其中两种终端对重认证方案进行分析，即动态模型检验器 OFMC 和基于约束逻辑的攻击搜索器 CL_AtSe。测试的安全目标是确保家庭基站和安全网关之间能够进行成功的双向认证。协议的部分测试代码如下：

```
role henb(A, B: agent, Ka, Kb: public_key,
IK,CK:symmetric_key, MAC: hash_func,
SND, RCV: channel (dy) )
played_by A def=
local
MAC1: hash(text.symmetric_key.symmetric_key),
```

MAC2 :hash(text.symmetric_key.symmetric_key),
$AUTH_{HeNB}$:hash(hash(text.symmetric_key.symmetric_key)),
$AUTH_{SeGW}$:hash(hash(text.symmetric_key.symmetric_key)),
State :nat
const
tsi, tsr, sai2, sar2,
id: text
init State :=0
transition
0. State =0 /\ RCV(start)=|>
State':=2/\MAC1':=MAC(id.IK.CK)/\AUTHHeNB':=MAC(MAC(id.IK.CK))/\SND({id.tsi.tsr.sai2}_Kb.$AUTH_{HeNB}$')
2. State =2 /\ RCV({tsi.tsr.sar2}_Ka.$AUTH_{SeGW}$')
=|>
State' :=4
end role %家庭基站
role segw(A, B: agent, Ka, Kb: public_key
IK,CK:symmetric_key, MAC: hash_func, SND, RCV: channel (dy))
played_by B def=
local
MAC1 :hash(text.symmetric_key.symmetric_key),
MAC2 :hash(text.symmetric_key.symmetric_key),
$AUTH_{HeNB}$:hash(hash(text.symmetric_key.symmetric_key)),
$AUTH_{SeGW}$:hash(hash(text.symmetric_key.symmetric_key)),
State :nat
const
tsi, tsr, sai2, sar2,
id: text
init State :=1
transition
1. State =1 /\ RCV({id.tsi.tsr.sai2}_Kb.$AUTH_{HeNB}$')
=|>
State':=3/\MAC2':=MAC(id.IK.CK)/\AUTHSeGW':=MAC(MAC(id.IK.CK))/\SND({tsi.tsr.sai2}_Ka.$AUTH_{SeGW}$')
end role %安全网关

采用OFMC对重认证测试的消息输出结果如图4所示；采用CL_AtSe对重认证测试的消息输出结果如图5所示。

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  D:\SPAN\testsuite\results\test.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  ParseTime: 0.00s
  SearchTime: 0.04s
  VisitedNodes: 45 modes
  Depth: 5 plies
```

图4 使用OFMC对重认证测试的消息输出

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  D:\SPAN\testsuite\results\test.if

GOAL
  As_specified

BACKEND
  CL_AtSe

STATISTICS

  Analysed: 0 states
  Reachable: 0 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

图5 使用CL_AtSe对重认证测试的消息输出

从两个测试结果可以看出，结果显示为安全，说明本文方案的重认证过程和初始认证相比，都能够为家庭基站设备和核心网提供正确的相互认证。

除了重认证功能外，本文方案同样能够在家庭基站设备和移动运营商的核心网之间使用IPsec建立一条安全的虚拟专用网，从而为接下来的数据传输提供保密和完整性服务。IPsec的隧道模式(tunnel mode)可以对包括IP头在内的完整的数据包进行安全性保护，从而有效避免源IP数据包交换遭受流量分析攻击。此外，家庭基站设备还可以通过运行IKEv2协议获得前向安全性，这样，即使攻击者获得一个已经泄露的密钥，也不能据此计算出新鲜的会话密钥。最后，使用IKE_SA传输家庭基站设备的身份能够提供匿名性保护。因此，本文方案的重认证过程提供了和初始认证同样的安全服务，没有降低原有的安全级别。

3.2 能量消耗分析

对全认证和本文提出的重认证进行能量消耗的比较分析。能量的消耗大致可分为两个部分：通信中的能量消耗以及采用的安全方案所产生的消耗。

安全方案包括：1) IKEv2消息的传送和应答；2) 在使用对称密码的方案中，为了产生或者验证一个MAC(消息验证码)，会使用预先分享的密钥进行认证参数的计算；3) 在使用公钥密码的方案中，为了产生或者验证一个证书，会使用PKI进行认证参数的计算；4) 使用EPS-AKA算法进行相关密钥的计算；5) 使用Diffie-Hellman算法进行相关密钥的计算；6) 一条IKEv2消息的加密和解密。具体的符号定义如表1所示。

表1 能量损耗参数

符号	说明
E_{M}	发送和接收一条IKEv2消息的能量消耗
E_{MAC}	使用一个预先分享的密钥生成或验证一个消息验证码MAC的能量消耗
E_{PKI}	使用一个公钥算法生成或验证一个证书的能量消耗
$E_{\mathrm{KEY-EPS}}$	使用EPS-AKA算法进行密钥计算的能量消耗
$E_{\mathrm{KEY-DH}}$	使用Diffie-Hellman算法进行密钥计算的能量消耗
E_{ENC}	对IKEv2消息进行加密或解密的能量消耗

在初始认证中，家庭基站和核心网之间的认证中仍然使用完整的IKEv2承载EAP-AKA的流程(具体步骤见1.2节)。能量消耗如下：1) 使用一个公钥算法对安全网关的证书进行验证；2) AUTHi和RES的生成以及AUTHr和AUTH负载的验证；3) 和安全网关间的8条IKEv2消息的交换；4) 6条IKEv2消息的加解密（IKE_SA）；5) IKEv2中为IPsec SA使用Diffie-Hellman算法的所生成的密钥；6) EPS-AKA中会话密钥的生成。因此，初始认证的能量消耗为：

$$E_{\mathrm{ini}} = E_{\mathrm{PKI}} + 4E_{\mathrm{MAC}} + 8E_{\mathrm{M}} + 6E_{\mathrm{ENC}} + E_{\mathrm{KEY-DH}} + E_{\mathrm{KEY-EPS}} \tag{2}$$

在本文提出的重认证方法中，能量消耗如下：1) AUTHi的生成和AUTHr的验证；2) 和安全网关间的4条消息的交换，3) 2条IKEv2消息的加解密(IKE_SA)；4) 使用Diffie-Hellman算法生成IPsec会话密钥。本文提出方法的能量消耗为：

$$E_{\mathrm{re}} = 2E_{\mathrm{MAC}} + 4E_{\mathrm{M}} + 2E_{\mathrm{ENC}} + E_{\mathrm{KEY-DH}} \tag{3}$$

根据文献[13]，E_{M}、E_{MAC}、$E_{\mathrm{KEY-EPS}}$消耗的能量可以忽略，因此重认证和初始认证消耗能量的比值为：

$$\eta = \frac{E_{\mathrm{re}}}{E_{\mathrm{ini}}} = \frac{2E_{\mathrm{ENC}} + E_{\mathrm{KEY-DH}}}{E_{\mathrm{PKI}} + 6E_{\mathrm{ENC}} + E_{\mathrm{KEY-DH}}} \tag{4}$$

设E_{PKI}=270 mJ，$E_{\mathrm{KEY-DH}}$=875 mJ，E_{ENC}=270 mJ，则η=0.5，和初始认证过程相比，由于减少了认证过程的计算量，提出的重认证方案中家庭基站设备的能量消耗降低为初始认证的50%。首先，由于提出的重认证方案不需要执行EAP-AKA的认证流程，而是利用初始认证中计算好的MSK作为认证参数，从而避免了EAP-AKA认证流程带来的认证参数的计算。其次，由于本文方案中没有采用安全网关的证书对其进行认证，因此家庭基站避免了使用公钥算法计算相应的认证参数，从而大大降低了能量的消耗[13]。同时，和初始认证相比，重认证减少了认证向量的计算和使用。

3.3 通信开销分析

对家庭基站设备的初始认证和重认证流程的通信开销[14]进行分析。假设家庭基站和AAA服务器之间一条消息的传输代价是一个单位(1 unit)，家庭基站和Se-GW之间是a个单位(a unit)，a<1，因为家庭基站和Se-GW之间的通信距离比家庭基站和AAA服务器的要小。同样，假设AAA服务器和HSS之间一条消息的传输代价是x个单位，x<1，理由同上。

如图3所示，本文方案的重认证方法中，包含了家庭基站和Se-GW之间的两条消息的传送，Se-GW和AAA服务器之间两条消息的传送。注意在本文方案中AAA服务器和HSS之间没有通信过程。因此得到的通信开销为：

$$C_{\mathrm{re}} = 2a + 2 \tag{5}$$

为了得到初始认证的通信开销，考虑以下两种情况：1) AAA服务器必须去HSS获取新鲜的认证向量；2) AAA服务器已经拥有一组新鲜的认证向量，因此不需要和HSS再进行通信。

第一种情况下包含的认证过程有：a) 家庭基站和Se-GW之间交换的4条消息；b) 家庭基站和AAA服务器之间交换的4条消息；c) AAA服务器和HSS之间为获取认证向量进行的2条消息的交换。通信开销为：

$$C_{\mathrm{ini1}} = 4a + 2x + 4 \tag{6}$$

第二种情况下，AAA服务器已经拥有一组新鲜的认证向量，因此不需要和HSS再进行通信。通信开销为：

$$C_{\mathrm{ini2}} = 4a + 4 \tag{7}$$

注意，初始认证中AAA服务器会要求从HSS中获得n组认证向量。因此，从式(6)和式(7)可以得到初始认证的通信开销为：

$$C_{\mathrm{ini}} = \frac{1}{n}C_{\mathrm{ini1}} + \frac{n-1}{n}C_{\mathrm{ini2}}$$

从而有：

$$C_{\mathrm{ini}} = \frac{1}{n}(4a + 2x + 4) + \frac{n-1}{n}(4a + 4) = \frac{n(4a+4) + 2x}{n} \tag{8}$$

从式(5)和式(8)可以得到重认证方法相比于初始认证的通信开销的改善率为：

$$I=\frac{C_{\text{ini}}-C_{\text{re}}}{C_{\text{ini}}}=\frac{4an+4n+2x-2an-2n}{4an+4n+2x}=\frac{2n+2x+2an}{4an+2n+2x}=\frac{n+x+an}{2an+2n+x} \tag{9}$$

I值越大则重认证相比于初始认证的通信开销越小。

图6中画出了以n和x为自变量的I函数，n代表认证向量组的数量，x代表AAA服务器和HSS之间的消息的传输代价。当n=1，x=0时，通信开销改善率为$\frac{1+a}{2+2a}$；当n=1，x=1时，通信开销改善率为$\frac{2+a}{3+2a}$，为了便于分析，把a固定设置为0.5。可以从图中观察到，随着n值的减少，通信开销的改善率I值增大。这是因为，如果每次接入认证都运行完整的认证流程，则AAA服务器就要频繁地和HSS进行通信以获取新鲜的认证向量。此外，还可以看到随着x值的增大，通信开销的改善率I值也会增大，这是由于重认证避免了为获得认证向量而产生的通信开销，因为重认证中AAA服务器不需要和HSS交换信息。

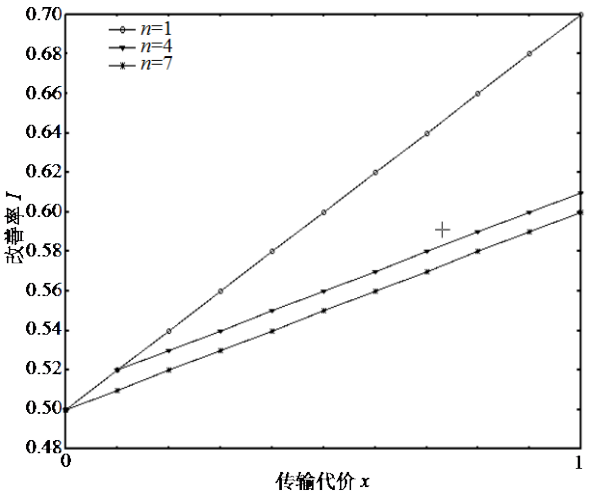

图6　重认证相比于初始认证的通信开销改善率

4　结束语

本文提出了一种家庭基站设备的快速重认证方法，能够大大降低初始认证的认证开销，同时不改变3GPP标准中的基础设施。本文方案利用初始认证过程中产生的参数MSK和重认证建立了安全绑定关系，因此在重认证中不需要再执行完整的IKEv2承载EAP-AKA/SIM的认证流程，从而减少了认证信令的交换和认证参数的计算。本文对重认证方案的安全性进行了分析，保证了和初始认证同样的安全级别，并且在能量消耗和信令开销方面和初始认证进行了详细的比较，结果表明本方案性能良好。

参　考　文　献

[1] THOMAS H. 3GPP TR 25.820, 3G Home NodeB study item technical report[S]. 2008.

[2] 赖成喆, 李晖, 张跃宇, 等. 一种移动用户通过家庭基站接入核心网的快速认证方法[C]//2010年全国通信安全学术会议论文集. 云南: 国防工业出版社, 2010: 61-65.
LAI Cheng-zhe, LI Hui, ZHANG Yue-yu, et al. A fast authentication method for mobile user accessing to core network via home NodeB/eNodeB[C]//2010 China Conference on Communication Security. Yunnan: National Defense Industry Press, 2010: 61-65.

[3] YANG Y M. 3GPP TR 33.820, Security of H(e)NB[S]. 2009.

[4] Aura T, Roe M. Reducing reauthentication delay in wireless networks[C]//Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks. Washington DC: IEEE Computer Society, 2005: 139-148.

[5] GANZ A, PARK S H, GANZ Z. Robust re-authentication and key exchange protocol for IEEE 802.11 wireless LANs[C]//Proceedings of the International Conference on Military Communications. Boston: IEEE, 1998: 1018-1022.

[6] NARAYAN V, DONETI L. Eap extensions for eap re-authentication protocol (erp)[EB/OL]. [2011-11-30]. http://tools.ietf.org/html/rfc5296.

[7] KAUFMAN C. The internet key exchange (IKEv2) protoco[EB/OL]. [2011-11-30]. http://www.ietf.org/rfc/rfc4306.txt.

[8] ARKKO J, HAVERINEN H. EAP-AKA authentication [EB/OL]. [2011-11-30]. http://tools.ietf.org/html/rfc5448.

[9] LIANG W, WANG W. A local authentication control scheme based on AAA architecture in wireless networks[C]// In IEEE 60th Vehicular Technology Conference (VTC). Los Angeles: IEEE, 2004: 5276-5280.

[10] CALHOUN P, LOUGHNEY J, GUTTMAN, et al. Diameter base protocol [EB/OL]. [2011-11-30]. http://www.ietf.org/rfc/rfc3588.txt

[11] KENT S, ATKINSON R. IP encapsulating security payload (ESP)[EB/OL]. [2011-11-30]. http://www.ietf.org/rfc/rfc4303.txt.

[12] AVISPA project. Automated validation of internet security protocols and applications[EB/OL]. [2011-11-30]. http://www.avispa-project.org.

[13] POTLAPALLY N R, RAVI S, Raghunathan A, et al. Analyzing the energy consumption of security protocols [C]//In International Symposium on Low Power Electronics and Design. Seoul, Korea: IEEE, 2003: 30-35.

[14] LIN, Y B, CHANG M F, HSU M T, et al. One-pass GPRS and IMS authentication procedure for UMTS[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(6): 1233-1239.

编　辑　张　俊