采用一次交互优化IMS用户注册过程

王晓婧 张奇支 范冰冰
(华南师范大学计算机学院 广州 510631)

摘 要 移动用户向IMS(IP Multimedia Subsystem)网络注册需要经过二次认证过程:GPRS接入认证及IMS对移动终端的认证。两者的认证过程中均采用AKA协议,它们包含很多类似的操作,增加了接入过程的延时,缺乏效率。针对IMS用户注册过程进行研究,在前人研究的基础上,通过SGSN和HSS之间的交互完成用户及网络之间的认证,避免了认证失败造成网络带宽的浪费,对IMS用户的注册过程进行了进一步优化。分析结果显示,改进后的注册过程优于先前所提出的注册过程。

关键词 IMS,注册,认证,优化
中图法分类号 TN915 **文献标识码** A

Optimization in IMS Registration Procedure Using One-pass Interaction

WANG Xiao-jing ZHANG Qi-zhi FAN Bing-bing
(School of Computer, South China Normal University, Guangzhou 510631, China)

Abstract Two authentication procedures are essential when mobile station registers to the IMS network: the GPRS access authentication and the IMS authentication. Both of the authentication procedures perform the protocol AKA. Almost all of the operations are the same, which increase the register procedure delay. As a result, it is very inefficient. This paper investigated the performance of IMS registration procedure and proposed an optimized scheme in IMS registration procedure based on previous study. We through the interaction between SGSN and HSS completed the registration procedure between mobile station and network, which avoids the bandwidth waste when authentication fails. The result of data analysis illustrates that the performance of this optimized registration scheme is better than the primitive one.

Keywords IMS, Registration, Authentication, Optimization

1 引言

IMS(IP Multimedia Subsystem,IP多媒体子系统)[1]是3GPP(Third Generation Partnership Project,第三代合作伙伴项目)在R5版本中首次提出的,随着IETF,ITU-T,TISPAN,OMA等重要标准组织加入到IMS的研究中,IMS在下一代网络中的重要性越来越明显,目前已成为下一代网络的发展方向。

IMS采用了SIP(Session Initiation Protocol,会话初始化协议)[2]作为会话建立和维护的信令协议。IMS的框架结构包括HSS,CSCF,MRF(包括MRFC和MRFP),IMS-MGW,MGCF,BGCF,AS等功能实体,所有的功能在各个实体中完成。其中,HSS(Home Subscriber Server,归属用户服务器)是用于所有用户和IMS业务相关数据的主要数据存储单元。存储在HSS中的主要数据包括用户身份、注册信息、接入参数以及业务触发信息等。CSCF(Call Session Control Function,呼叫会话控制功能)主要控制会话进程,是整个网络的核心。它又分为3个不同实体:P-CSCF(Proxy-CSCF,代理-呼叫会话控制功能),它是IMS网络中MS(Mobile Station,移动终端)的第一个接触点,是系统的入口,执行加密和压缩等功能;I-CSCF(Interrogating-CSCF,问询-呼叫会话控制功能),它是归属网络的入口点,用于隐藏网络内部拓扑结构,负责用户信息的询问并通过和HSS进行交互完成用户S-CSCF的查找;S-CSCF(Serving-CSCF,服务-呼叫会话控制功能),它在IMS中处于核心控制地位,负责记录并控制用户进程状态,执行会话路由功能,根据触发条件选择相应的应用服务器,并不断与应用服务和计费功能进行交互。

IMS可以采用多种接入方式,在通过GPRS(General Packet Radio Service,通用分组无线服务)[3]进行接入时,MS通过UTRAN(UMTS Terrestrial Radio Access Network,UMTS陆地无线接入网)接入到SGSN(Serving GPRS Support Node,服务GPRS支持节点),通过SGSN的认证后,向GGSN(Gateway GPRS Support Node,GPRS网关支持节点)发送一个创建PDP上下文请求的消息,GGSN负责分配一个IP地址,从而实现连接[4]。

在IMS中,用户的位置管理和会话管理被尽可能指向归

到稿日期:2010-09-26 返修日期:2010-12-15 本文受国家自然科学基金项目(60703094)资助。
王晓婧(1986-),女,硕士,主要研究方向为下一代网络技术,E-mail:wangxiaojing0603@163.com;张奇支(1976-),男,博士,副教授,主要研究方向为下一代网络技术、移动IP技术,E-mail:Qizhi163@tom.com(通信作者);范冰冰(1962-),男,教授,主要研究方向为下一代网络技术。

属网络，因此，产生注册过程和会话过程都必须经过主叫和被叫的归属网络。在 MS 开始进行注册前，为了和 IMS 进行网络通信，MS 必须找到 IMS 系统的入口点，即发现一个 P-CSCF。之后，MS 通过向其归属网络的 S-CSCF 发送 Register 消息来进行网络注册，生成注册用户的公共用户标识和 MS 的 IP 地址的绑定关系[5]。用户的注册有助于 IMS 准确地定位用户的当前位置。

对于 IMS 而言，GPRS 接入认证同 IMS 用户认证这两个过程都是必要的。在使用 GPRS 接入的过程中，当 MS 发送位置更新请求和附着请求消息到 SGSN 时，SGSN 采用 AKA (Authentication and Key Agreement，认证和密钥协商)[6] 对 MS 进行认证。同样，当 MS 向 IMS 进行注册时，仍然需要使用 AKA 协议进行认证。在实际的应用过程中，这两个认证过程往往前后进行。由于两者都使用 AKA 协议，因此，它们存在很多类似的操作。目前已有很多学者针对这一问题进行了研究。Lin[7] 等人针对规范[5] 中的 IMS 注册过程提出了 GPRS 与 IMS 认证相结合的一种方法，但该方法缺少 MS 对网络的认证，并且忽略了 MS 与 P-CSCF 之间建立安全联盟所需要的密钥，使得整个 IMS 系统的安全性受到很大威胁。Huang [8] 和徐[9] 等人分别在此基础上进行了优化，在提高认证效率的基础上，兼顾了网络安全性能方面的需求。张[10] 等人分析了 IMS 中的重注册过程，并提出一种快速用户重注册的方法。但对于认证失败的情况，文献[8,9]，没有做太多考虑，本文在此基础上进一步对此过程进行改进和优化。

本文第 2 节介绍 IMS 的认证过程及前人对它的改进方法；第 3 节介绍本文提出的 IMS 优化认证过程；第 4 节对优化后的过程进行性能分析；最后进行总结。

2 IMS 认证过程

本节将分别分析基于 AKA 协议的 GPRS 接入认证过程及 IMS 用户认证过程，并介绍前人针对这一过程的改进方法。

2.1 GPRS 接入认证

在 MS 启动 IMS 注册之前，首先需要建立网络连接。图 1 显示了 MS 发起 GPRS 接入认证的详细过程。

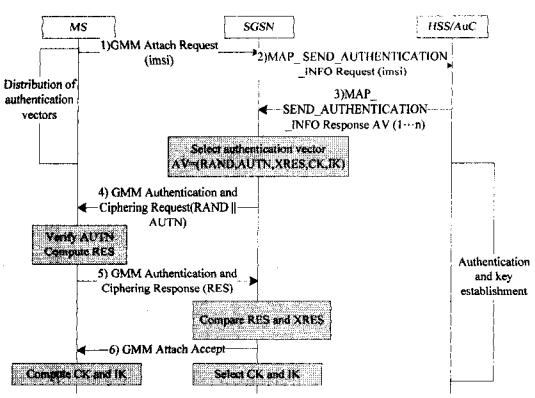


图 1　3GPP GPRS 接入认证过程

在 GPRS 的接入认证过程中：(1)MS 首先携带接入认证参数 IMSI(International Mobile Subscriber Identifier，国际移动用户标识符)(假设值为 imsi)发送附着请求到 SGSN，引发 GPRS 认证过程；(2)如果 SGSN 中已经存在尚未使用的认证向量，则(2)(3)两步可以省略，否则 SGSN 将携带 *imsi* 向 HSS 发送鉴权消息，并请求新的认证向量；(3)收到从 SGSN 发来的请求消息后，HSS 通过参数 *imsi* 得到关于 MS 的信息，并通过共享密钥 K 生成一组新的认证向量，认证向量中的消息包含：网络生成的随机认证挑战 RAND、网络认证令牌 AUTN、期望从终端得到的应答 XRES、加密密钥 CK 及完整性密钥 IK；(4)SGSN 从 HSS 收到认证向量后，会选择一组认证向量，并将 RAND 及 AUTN 发送给 MS；(5)收到 RAND 和 AUTN 之后，MS 会根据 AUTN 的值完成对网络的认证，如果通过认证，则使用自己的密钥和收到的 RAND 来产生一个相应值 RES，并将其发送给 SGSN；(6)SGSN 将收到的 RES 与 XRES 做比较，如果相同，则认证成功。

2.2 IMS 用户认证

IMS 用户认证过程如图 2 所示。在 IMS 中采用 IMPI(IP Multimedia Private Identity，私有用户标识)来唯一标识用户，同样，在 HSS 中，也根据用户的 IMPI 值来保存用户信息。当 MS 通过 GPRS 接入认证及 PDP 上下文激活后，如果需要进行业务之间的访问，首先需要进行注册。在初始的注册过程中，移动终端和 S-CSCF 通过运行 IMS AKA[6] 协议来进行相互之间的认证。IMS AKA 使用了与私有用户标识相关的在 ISIM 和 HSS 之间共享的长期密钥。其认证过程已在文献[7-9]中进行了详细说明，本文不再阐述。值得注意的是，当 S-CSCF 收到从 I-CSCF 转发的 Register 注册消息(图 2 中的 I18)之后会比较 RES 与 XRES：如果不同，则返回 403 Forbidden 消息，认证失败，参见图 2 中的 I21a－I24a；如果相同，S-CSCF 返回 200 OK 消息，通知用户通过认证，参见图 2 中的 I21b－I24b。

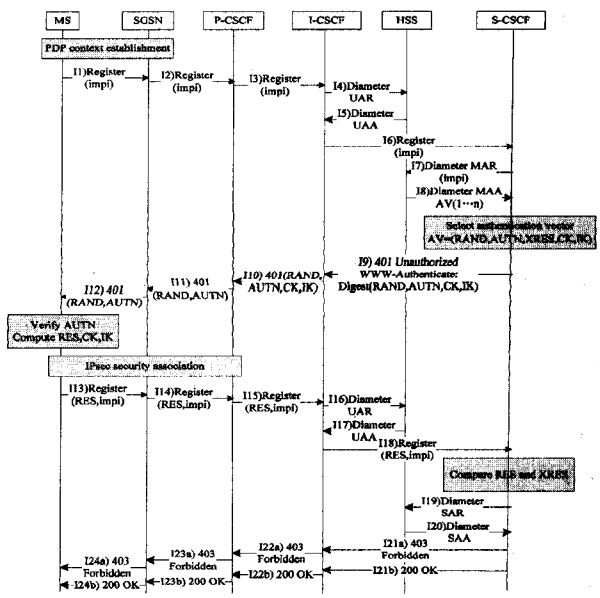


图 2　IMS 注册认证及密钥分配

2.3 前人的改进

从图 2 可以发现，MS 在通过 GPRS 认证之后，继续进行 IMS 注册及密钥分配，仍需要进行两回合的交互。徐[9] 等人针对 IMS 的注册及密钥分配过程进行了改进，所提出的方法实现了 MS 与 IMS 网络的双向认证，并正确分配了密钥，只需要进行一个回合的认证，减少了信令的开销，如图 3 所示。

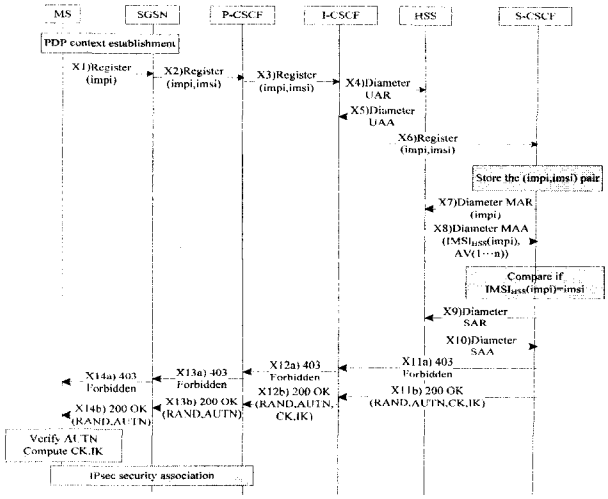


图 3　前人改进后的 IMS 注册过程

在改进后的过程中：(X1)－(X3) MS 与 SGSN 通过 PDP 上下文激活后，携带认证参数 IMPI(假设值为 *impi*)发送 Register 注册消息到 SGSN。经过 GPRS 认证后，SGSN 了解 MS 的 IMSI 值(假设值为 *imsi*)，SGSN 将注册消息并携带参数(*impi*，*imsi*)经过 P-CSCF 后转发至 I-CSCF；(X4)－(X6) I-CSCF 通过和 HSS 交互，得到 S-CSCF 地址，并将注册消息发送至 S-CSCF；(X7)－(X8) S-CSCF 在本地保存(*impi*，*imsi*)的对应关系，并使用参数 *impi* 向 HSS 发送 MAR 消息，请求 IMSI 的值，这里用 $IMSI_{HSS}(impi)$ 表示 IMPI 值为 *impi* 的 MS 的 IMSI 值。HSS 收到请求消息后会基于共享密钥及序列号计算得到一组认证向量，通过 MAA 消息连同 $IMSI_{HSS}(impi)$ 的值返回给 S-CSCF。S-CSCF 检查 $IMSI_{HSS}(impi)$ 与 *imsi* 是否相同，如果相同，则 MS 通过认证；(X9)－(X10) S-CSCF 通过 SAR 消息和 HSS 交互，HSS 返回 SAA 消息作为响应。同样，如果 MS 没有通过认证：(X11a)－(X14a) S-CSCF 返回 403 Forbidden 消息通知 MS 认证失败；如果 MS 通过认证：(X11b)－(X12b) S-CSCF 选择一个未使用的认证向量，将 RAND，ATUN，CK 和 IK 的值通过 I-CSCF 转发到 P-CSCF；(X13a)－(X14a) P-CSCF 去掉 CK 和 IK 后将消息发送到 SGSN，最后到达 MS；随后，MS 利用共享密钥验证 AUTN，从而完成对网络的认证，最后与 P-CSCF 建立安全关联。在徐[9]所提出的优化方法中，没有分析 X11a－X14a 认证失败的情况，为了方便后文的性能分析，本文加入了这一过程。

从上述的优化过程来看，徐等人提出的 GRPS 与 IMS 认证与密钥分发的优化集成方法实现了对移动终端的认证，并且满足移动终端对 IMS 网络的认证需求及双方的密钥分配需求。但需要注意的是，经过了上述过程的(X1)－(X8)，S-CSCF 要检查 $IMSI_{HSS}(impi)$ 与 *imsi* 是否相同，如果相同，则 MS 通过认证；如果不相同，则认证失败。需要注意的是，IMS 中使用基于文本的 SIP 信令作为会话建立和维护的信令协议，而该方法仍然需要经过一个比较复杂的过程才能验证用户和网络双方是否通过认证(认证用户需要 X1－X8，认证网络需要 X1－X14)。因此，如果出现认证失败的情况，无疑在一定程度上浪费了网络中有限的带宽资源。本文将在下一节对优化过程提出进一步的改进。

3　优化

上一节提到前人采用 GPRS 与 IMS 认证与密钥分发的优化集成方法在一定程度上对原始的 IMS 用户注册进行了改进。本节针对其出现认证失败情况下所造成的网络资源浪费的情况进行进一步改进，其改进后的流程如图 4 所示。

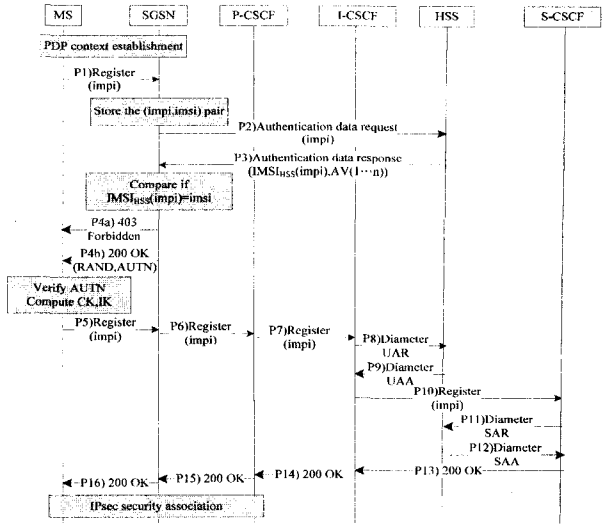


图 4　改进后的 IMS 注册过程

(P1) MS 与 SGSN 通过 PDP 上下文激活后，携带认证参数 IMPI(假设值为 *impi*)发送 Register 注册消息到 SGSN；(P2)经过 GPRS 认证后，SGSN 了解 MS 的 IMSI 值(假设值为 *imsi*)，因此，SGSN 首先在本地保存(*impi*，*imsi*)的对应关系，并携带认证参数 *impi* 向 HSS 发送认证请求消息，请求认证向量 AVs 及 $IMSI_{HSS}(impi)$，这里仍用 $IMSI_{HSS}(impi)$ 表示 IMPI 值为 *impi* 的 MS 的 IMSI 值；(P3) HSS 在应答消息中，将认证向量及 $IMSI_{HSS}(impi)$ 返回至 SGSN，SGSN 根据收到的应答消息判断 $IMSI_{HSS}(impi)$ 与 *imsi* 是否相同；(P4a)如果不相同，则 SGSN 返回 403 Forbidden 消息通知 MS 认证失败；(P4b)如果相同，则用户通过认证，SGSN 提取认证向量中的 RAND 和 AUTN 参数并连同应答消息发送至 MS，MS 收到应答消息后计算出 CK 及 IK，并根据收到的 AUTN 的值完成对网络的认证；(P5)－(P7)如果网络通过认证，MS 携带参数向 SGSN 发送 Register 注册消息。SGSN 将收到的注册消息经过 P-CSCF 转发后至 I-CSCF；(P8)－(P12) I-CSCF 通过和 HSS 交互，得到 S-CSCF 地址，并将注册消息发送至 S-CSCF。S-CSCF 发送 SAR 消息到 HSS，请求 HSS 记下为之提供服务的 SIP 服务器的对应关系，HSS 发送 SAA 消息至 S-CSCF，作为 SAR 的响应；(P13)－(P16)由 S-CSCF 发送 200 OK 消息，依次经过 I-CSCF，P-CSCF，SGSN，最后达到 MS。MS 通过计算出的 CK 及 IK 的值，与 P-CSCF 建立安全联盟，注册结束。应该注意的是，SGSN 向 HSS 请求认证向量后会在本地进行保存，因此(P2)(P3)两步并非每次注册都要进行。

从上述过程中，我们可以看到如果用户认证失败，则改进后的认证过程到第(P4)步结束；同样，如果网络认证失败，则在完成第(P4)步后结束。因此，从直观上看，改进后的认证过程在网络带宽占用上有更大的优势，以下我们将对其进行性能分析。

4 性能分析

本节将对改进后的注册过程进行性能分析，主要针对改进后的优化方法与 IMS AKA 认证以及徐等人的优化方法进行费用比较。

为方便分析，将由 MS 出发的 SIP 信令经过 SGSN，P-CSCF，I-CSCF 最后到达 S-CSCF 的费用开销作为整体考虑，假设将其整体开销归为 1（其中从 MS 到 SGSN 的开销为 0.25，从 SGSN 到 S-CSCF 的开销为 0.75），而其它实体（I-CSCF，S-CSCF）同 HSS 之间的一次信令传输的开销为 α，SGSN 同 HSS 之间的一次信令传输的开销为 β。由于 I-CSCF，S-CSCF，SGSN 与 HSS 的信令交互属于整体开销的一部分，而 I-CSCF，S-CSCF 同 HSS 通常属于归属地，SGSN 属于漫游地，因此 $0<\alpha<\beta<1$。考虑到在认证过程中，认证失败也是不可避免的，因此定义认证成功的概率为 P_1，用户被网络认证失败的概率为 P_2，网络被用户认证失败的概率为 P_3，不难看出 $P_1+P_2+P_3=1$。并且，假设 S-CSCF 同 HSS 交互一次会得到 $n(n\geqslant 1)$个认证向量。

对于原始的 IMS AKA 认证，定义 C_I 为总的信令费用，需要注意在图 2 中，S-CSCF 和 HSS 的交互（I7－I8）有两方面的作用：一方面是从 HSS 中下载认证向量，另一方面 S-CSCF 将自己的 SIP URI 记录在 HSS 中，使得其它实体可以通过向 HSS 询问来得到分配给某个用户的 S-CSCF 的 URI。因此，在原始的 IMS 认证过程中，即使当 S-CSCF 中存在未使用的认证向量时 I7－I8 也是不能跳过的：

$$C_I=P_1(4+8\alpha)+P_2(4+8\alpha)+P_3(2+4\alpha)$$
$$=(P_1+P_2)(4+8\alpha)+P_3(2+4\alpha) \quad (1)$$

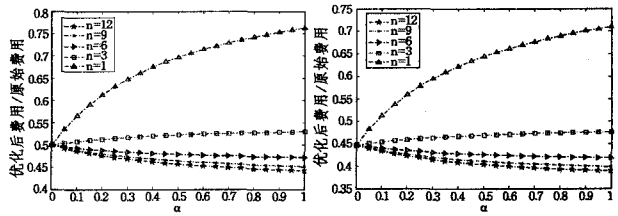
同理，对于徐等人提出的优化方案，定义 C_X 为总的信令费用，根据图 3，当 S-CSCF 中存在未使用的认证向量时 X7－X8 可跳过，因此：

$$C_X=P_1[\frac{1}{n}(2+6\alpha)+\frac{n-1}{n}(2+4\alpha)]+P_2[\frac{1}{n}(2+6\alpha)+\frac{n-1}{n}(2+4\alpha)]+P_3[\frac{1}{n}(2+6\alpha)+\frac{n-1}{n}(2+4\alpha)]$$
$$=\frac{1}{n}(2+6\alpha)+\frac{n-1}{n}(2+4\alpha) \quad (2)$$

对于改进的优化方案，定义 C_P 为总的信令费用，为了便于分析，令 $\beta=2\alpha$。根据图 4，当 SGSN 中存在未使用的认证向量时 P2－P3 可跳过，因此：

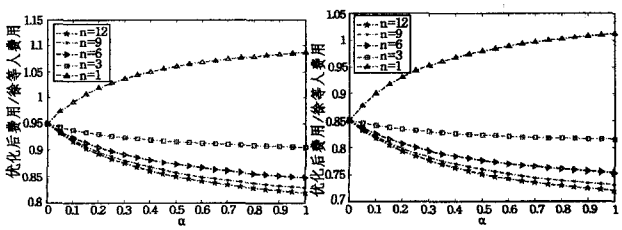
$$C_P=P_1[\frac{1}{n}(2.5+4\alpha+2\beta)+\frac{n-1}{n}(2.5+4\alpha)]+P_2[\frac{1}{n}(0.5+2\beta)+\frac{n-1}{n}\times 0.5]+P_3[\frac{1}{n}(0.5+2\beta)+\frac{n-1}{n}\times 0.5]$$
$$=P_1[\frac{1}{n}(2.5+8\alpha)+\frac{n-1}{n}(2.5+4\alpha)]+(P_2+P_3)[\frac{1}{n}(0.5+4\alpha)+\frac{n-1}{n}\times 0.5] \quad (3)$$

当 $P_1=0.7$，$P_2=0.2$，$P_3=0.1$ 时，图 5(a)和图 6(a)分别显示了改进后的认证过程和 IMS AKA 原始认证过程费用的对比情况，及改进后的认证过程和徐等人提出的集成方法费用的对比情况。从图 5(a)，我们可以发现，通过对认证向量的个数 n 的不同取值，随着一次取得的认证向量个数逐渐增大，性能优化也逐渐显著。当 $n=12$，$\alpha=1$ 时，性能优化效果最好，约为原始费用的 44.15%。尽管当 $n=1$，$\alpha=0$ 时，性能优化的效果最不好，但优化后的总费用仍然只占原始费用的 76.32%。同时，在图 6(a)中，当 $n=1$ 时，本文提出的优化方法的费用代价略高于徐等人提出的方法，这是由于当认证成功的概率非常高时（$P_1=0.7$）。随着 α 值的增大，SGSN 与 HSS 的交互增加了费用。但从整体上分析，本文提出的优化方法的费用代价要小于徐等人提出的集成方法的费用代价。图 5(b)和图 6(b)显示了当 $P_1=0.6$，$P_2=0.3$，$P_3=0.1$ 时的费用对比情况。可以发现，当用户认证失败的概率由 0.2 上升到 0.3 时，性能优化有了进一步提高，本文提出的改进方法的优势也更加明显。



$P_1=0.7, P_2=0.2, P_3=0.1$ (a)　　$P_1=0.6, P_2=0.3, P_3=0.1$ (b)

图 5　改进后的认证过程和 IMS AKA 原始认证过程费用对比



$P_1=0.7, P_2=0.2, P_3=0.1$ (a)　　$P_1=0.6, P_2=0.3, P_3=0.1$ (b)

图 6　改进后的认证过程和徐等人集成方法费用对比

结束语　以 IMS 为核心的下一代网络是未来融合网络发展的方向。本文通过分析 IMS 网络中的注册过程及前人对该问题的改进方法，在前人研究的基础上，提出了对 IMS 用户注册过程的进一步优化方法，从而避免了认证失败时出现的复杂的注册过程，减少了信令的迂回，从而减少了用户注册的费用。数据分析表明，本文提出的改进方法确实对原始的注册过程进行了优化，并在一定程度上对前人的研究成果进行了进一步优化。

参 考 文 献

[1] 3GPP TS 23.228, V.8.2.0. IP Multimedia Subsystem (IMS) [S]. Sep. 2007

[2] Rosenberg J, Schulzrinne H, Camarillo G, et al. SIP: Session Initiation Protocol, IETF RFC 3261[S]. June 2002

[3] 3GPP TS 23.060 V10.0.0. "General Packet Radio Service (GPRS); Service description; Stage 2", Release 10, June 2010

[4] 3GPP TS 33.102 V9.2.0. "3G Security; Security architecture", Release 9, Mar. 2010

[5] 3GPP TS 33.203 V9.3.0. "3G security; Access security for IP-based services", Release 9, Dec. 2009

（下转第 87 页）

①计算两资源管理树的树根结点中包含的 *Key* 相似度，利用 Wordnet 中词语的关系结构标识对应结点的位置关系；

②根据 *Key* 相似度，调整结点中 *Key* 的集合，使得两结点的 *Key* 集合映射到同一个 Wordnet 词集合中；

③由于资源管理树被存储为 RDF/RDFS 格式，利用 Lucene 对文本的搜索能力，利用 Jena 的推理，使用 Jena API 进行判断；

④判断对应两树结点的关系 R，若 $R \in$ {Attribute-of, Part-of, Instance-of, Kind-of}，则建立两树结构点的关系映射说明，形成树结构结点关系映射集 RelSet；

⑤根据关系映射集 RelSet，通过树的深度遍历判断两资源管理树的相似度；

⑥返回相似度大于可信度阈值的分支结构及关系映射集 RelSet。算法结束。

4.3 RDF/RDFS 文件的管理

资源管理应用中，用户通过管理 RDF/RDFS 文件实现了资源应用和共享，也实现了资源存储及使用的虚拟化。在实现资源语义标注的过程中，使用 Protégé 作为建模工具，得到 Doc 本体、Wr 本体和 Dt 本体的 OWL 文件，完成了对资源信息元核心属性的建立，然后配合文本标注和 XML Schema 使用 Jena RDF API 完成了利用 RDF/RDFS 对资源管理树的描述并形成相应的文件，并以 RDF 三元组的形式存储在数据库中。

通过 Lucene 读取文件的接口，为描述资源管理树的 RDF/RDFS 建立关键字标识号的排列索引，根据该排列索引中的关键字，调整 RDF/RDFS 对应的资源管理树中从根结点到各叶子结点路径所包含的各结点的关键字集，以完成资源管理树的初始化工作。

先按需求完成资源本体的相似度计算，通过 Jena RDF API 以及基于 XML 操作的控件的功能，实现调整、插入、合并结点的过程，即完成对资源管理树（RDF/RDFS 文件）的管理。

结束语 如上所述，本文主要研究了 Web 资源的多粒度语义标注，并给出了基于粒度匹配计算的搜索应用技术的相关算法。从以上分析可知：这种处理方法的效率是肯定的。然而，至于如何考虑标注的开销，和在“查准”与“查全”两方面做出权衡，限于文章篇幅留待下一步探讨。

参 考 文 献

[1] Pirro G, Mastroianni C, Talia D. A Framework for distributed knowledge management: Design and implementation[J]. Future Generation Computer Systems, 2010, 26: 38-49

[2] Han K H, Park J W. Process-centered knowledge model and enterprise ontology for the development of knowledge management system[J]. Expert Systems with Applications, 2009, 36: 7441-7447

[3] Jung J J. Ontology mapping composition for query transformation on distributed environments[J]. Expert Systems with Applications, 2010, 37: 8401-8405

[4] Kiryakov A, Popov B, Terziev I, et al. Semantic annotation, indexing, and retrieval[J]. Journal of Web Semantics, 2004, 2(1): 49-79

[5] Dean M, Schreiber G, Bechhofer S, et al. OWL web ontology language reference[EB/OL]. W3C Recommendation. http://www.w3.org/TR/2004/REC-owl-ref-20040210/, 2004

[6] Alani H, Kim S, Millard D, et al. Automatic ontology-based knowledge extract ionfrom Web documents[J]. Intelligent Systems, 2003, 18(1): 14-21

[7] Jane M, Christopher M, Fernando G, et al. Semantic Annotation of Aerospace Problem Reports to Support Text Mining[J]. IEEE Intelligent Systems, 2010, 25(5): 20-26

[8] Alcaraz Calero J M, Marín Pérez J M, Bernabé J B, etal. Detection of semantic conflicts in ontology and rule-based information systems[J]. Data and Knowledge Engineering, 2010, 69: 1117-1137

[9] Jung J J. Reusing ontology mappings for query routing in semantic peer-to-peer environment[J]. Information Sciences, 2010, 180: 3248-3257

[10] Ahn J W, Brusiloysky P, Grady J, et al. Semantic annotation based exploratory search for information analysts[J]. Information Processing and Management, 2010, 46(4): 383-402

[11] 陈叶旺，李文，彭鑫，等. 基于本体的文档语义标注改进方法[J]. 东南大学学报：自然科学版，2009，39(6)：1109-1113

[12] 杨艳萍，谭庆平. 一种有效的服务资源自动语义标注方法[J]. 计算机研究与发展，2007，44(1)：37-43

[13] Popov B, Kiryakov A, Ognyanoff D, et al. KIM: a Semantic Platform for Information Extraction and Retrieval[J]. Natural Language Engineering, 2004, 10(3/4): 375-392

[14] Kopecky J, Vitvar T, Bournez C, et al. SAWSDL: Semantic Annotation for WSDL and XML Schema[J]. IEEE Internet Computing, 2007, 11(6): 60-67

[15] 白伟华，李吉桂. 基于 SOA 的多边多议题协商模型的研究[J]. 计算机科学，2008，35(1)：151-153，175

[16] Zhu Jia-xian, Bai Wei-hua, Li Ji-gui. The mediation data services application model based on web resource ontology[C]// 1st International Conference on E-Business and E-Government. Guangzhou China, 2010: 1468-1472

（上接第 64 页）

[6] Arkko J, Haverinen H. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)[M]. RFC 4187, January 2006

[7] Lin Yi-bing, Chang Ming-feng, Hsu M, et al. One-pass GPRS and IMS authentication procedure for UMTS [J]. IEEE Journal on Selected Areas in Communications, 2005, 23(6): 1233-1239

[8] Huang Chung-ming, Li Jian-wei. One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS[C]// IEEE 21st International Conference on Advanced Networking and Applications (AINA'07). Niagara Falls. ON, Canada, May 2007: 482-489

[9] 徐鹏，廖建新，朱晓民，等. GPRS 与 IMS 认证与密钥分发的一种优化集成方法[J]. 北京邮电大学学报，2006(05)

[10] 张奇支，黄兴平，范冰冰. IMS 中一种快速的用户注册过程[J]. 计算机科学，2010，37(9)：117-120