

SIP 认证机制的研究和改进*

Research and Improvement of the SIP Certification Mechanism

林霞, 董魁松

LIN Xia, DONG Kui-song

(华中科技大学软件学院, 湖北 武汉 430074)

(School of Software, Huazhong University of Science and Technology, Wuhan 430074, China)

摘要: 本文首先简要介绍了会话初始化协议(SIP)的基本内容, 然后对 SIP 协议中的注册和呼叫流程中的认证机制做了分析, 并提出了改进的方法。

Abstract: This paper briefly introduces the basic contents of the SIP protocol, analyze the registration and the certification mechanism in the call flow, and proposes an improved solution to the registration mechanism.

关键词: SIP; 用户代理; 代理服务器; 注册服务器

Key words: SIP; user agent; proxy server; registrar

中图分类号: TP309

文献标识码: A

1 引言

会话初始化协议 SIP(Session Initiation Protocol, 简称 SIP)是 IETF 提出并主持研究的一个支持多媒体会话的信令控制协议^[1]。SIP 是实现新一代话音通信及多媒体和数据交换的关键技术, 用来创建、修改以及终结一个或多个参与者参加的会话进程。这些会话包括因特网多媒体会议、IP 电话、即时消息等所有因特网上交互两方或者多方多媒体通信活动^[2]。参与会话的成员可以通过多播方式、单播连网方式或两者结合来进行通信。

在 SIP 协议中, 用户认证的主要目的是判断用户是否具有合法性。本文将着重探讨 SIP 协议中的认证机制及其改进方案。

2 SIP 协议

SIP 运用一种分布式的控制模式, 采用 Client/Server 结构的消息机制, 将对语音通信的控制信息封装到消息的头域中, 通过消息的传递来实现^[2]。

SIP 系统主要由两种组件组成: 用户代理(UA)和网络服务器。这是进行通信的两个关键要素。

用户代理(UA)是客户端终端系统的应用程序, 它代表要加入呼叫的用户。用户代理包含两个部分: 用户代理客户端(UAC)用来初始化一个呼叫, 发起 SIP 请求, 并作为该用户的呼叫代理; 用户代理服务器(UAS)用来接收请求, 代表用户发出响应, 并作为被叫用户代理。

SIP 网络服务器一般有四种: (1)代理服务器(Proxy Server)代表其它客户机发起请求, 既充当服务器又充当客户端的媒介程序。其主要作用相当于路由器, 将客户端的请求发送至目标端的代理服务器。(2)注册服务器(Registrar)接收客户机的注册请求, 完成用户地址的注册并将注册信息存入定位服务器。(3)定位服务器(Location Server)保存注册信息, 其作用相当于数据库。(4)重定向服务器(Redirect Server)接收 SIP 请求, 并把请求中的原地址映射成零个或多个新地址, 返回给客户端。以上几种服务器只是 SIP 协议中定义的不同实体, 并不表示它们分布在不同的物理设备上。

SIP 协议的功能主要通过其消息机制实现。SIP 消息有两类: 从客户端到服务器的请求消息(Request)和从服务器到客户端的应答消息(Response)。SIP 的消息共规定了六种基本方法: INVITE、ACK、CANCEL、OPTIONS、BYE、REGISTER。其中, INVITE 和 ACK 用于建立呼叫, 完成三次握手, 或者用于建立以后改变会话属性; BYE 用

* 收稿日期: 2004-08-30; 修订日期: 2004-10-29

作者简介: 林霞(1982-), 女, 江西赣县人, 硕士生, 研究方向为 VoIP 技术的应用; 董魁松, 硕士生, 研究方向为 VoIP 系统和软交换。

通讯地址: 430074 湖北省武汉市华中科技大学东七舍 324; Tel: (027)87546510, 13545216676; E-mail: accountdifficult@sohu.com
Address: School of Software, Huazhong University of Science and Technology, Wuhan, Hubei 430074, P. R. China

以结束会话;OPTIONS用于查询服务器能力;CANCEL用于取消已经发出但未最终结束的请求;REGISTER用于客户端向注册服务器发出注册消息。

SIP中还定义了多种不同的数字状态码来表示不同的信令:1xx代表临时性的消息,2xx表示成功,3xx表示重定向,4xx为客户端错误,5xx为服务器端错误,6xx为全局性错误。

3 SIP 的认证机制的解决方案

3.1 传统的 SIP 流程

SIP协议中,在其建立会话之前必须要求用户具有合法性^[3]。对于非授权用户,SIP系统不予支持。用户代理在发出REGISTER和INVITE的请求消息时,服务器都会要求其发送认证信息,以保证用户代理的合法性。注册服务器发送应答消息401(Unauthorized),而代理服务器发送应答消息407(Proxy-Authentication Required),向用户代理要求各自所需的认证证书。一般情况,401将会在它的WWW-Authentication头域中,407将会在它的Proxy-Authenticate头域中包含认证证书所需的参数。然后,用户代理重发包含头域Authorization和Proxy-Authorization的REGISTER和INVITE请求消息,来分别响应401和407。

为了便于说明问题,本文只将代理服务器和注册服务器在图1中进行标示。图1便是一个完整的注册和呼叫过程。

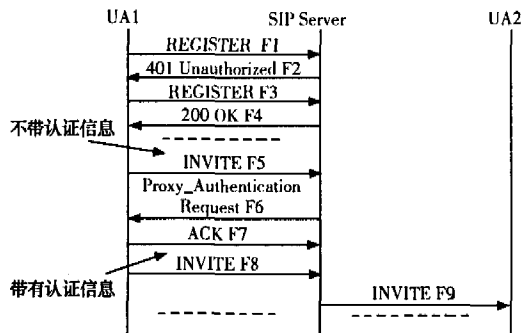


图1 传统的 SIP 流程

在图1中,UA1第一次发送的注册请求REGISTER(F1)中不带有认证信息。因此,注册服务器返回应答消息401 Unauthorized(F2),表示UA1未经授权,并且在消息中包含注册服务器所需要的认证信息。UA1重发包含认证信息的请求,注册服务器验证通过并返回OK(F4)。至此,注册过程结束。

当UA1试图呼叫UA2时,向代理服务器发出INVITE的请求,请求中不带有认证信息,因此代理服务器返回应答消息407 Proxy-Authentication Request(F6)拒绝UA1的请求,同时在消息中包含代理服务器所需要的认证信息。UA1收到407之后马上返回ACK,并且在之后重发包含代理服务器所需认证信息的INVITE请求。代理服务器验证信息正确之后向UA2发送INVITE请求并建立连接。

3.2 改进后的方案

在现实的应用中,一种普遍的做法是将注册服务器和代理服务器这两个实体放置在同一物理设备上,本文暂且称之为SIP Server,此服务器承担所有的注册服务器和代理服务器的功能。如果在这种情况下还采用上述传统的流程则是不必要的,因为用户代理发送的认证证书的格式是通过一项称为“realm”的参数来区分的,不同的realm使用不同的认证证书。401(Unauthorized)或407(Proxy-Authentication Required)的头域中都包含此参数。当注册服务器和代理服务器用同一服务器来实现时,它们拥有相同的realm值,因此所需的认证证书也是相同的。用户代理在发送REGISTER请求成功之后,可以将realm所需的证书及其参数值记录下来。当用户代理希望建立呼叫时,便可以将认证证书包含在INVITE请求的头域中,省去了图1中的F5和F6两个步骤。改进后的流程如图2所示。

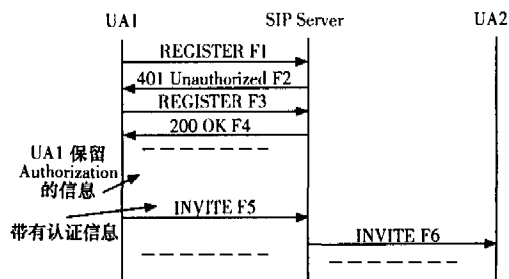


图2 改进后的 SIP 流程

数据结构设计如下:

```
struct SIPAuthorization Item{
    bool isSIPServer;
    string realm;
    string nonce;
};
```

首先用isSIPServer来判断注册服务器和代理服务器是否在同一服务器上,如果isSIPServer为True才执行拷贝的工作;否则按原流程进行。当服务器向用户代理返回401(Unauthorized)时,解析并提取出头域WWW-Authenticate及其参数,将对应的realm和nonce拷贝到结构体当中。用户代理在发起INVITE请求时,就可以直接将结构体当中相应的参数复制到Proxy-Authorization中去。

如果此方案的实现必须要求服务器对用户代理的注册请求发出回应,则在200(OK)中带上包括参数nextnonce的头域Authentication-Info。如果服务器使用后者,则每次注册成功后,都要将结构体中的nonce更新,用nextnonce的值代替原先的nonce值,以便用户代理和服务器可以正确地进行加密和解密。

改进后的方案减少了用户代理和服务器之间的对话,缩短了呼叫建立的流程。在网络资源有限的情况下,此方案可以有效地在最短时间建立会话,能够减轻服务器的处理量,对于注册用户较多的服务器会有很大的帮助。

4 分析与测试结果

为了性能测试少受其他网络因素的影响,我们建立了

(下转第18页)

5 实验结果

在实验中,我们选取四种学科中邓小平理论、计算机人工智能技术、经济学、图书情报学、计算机网络五个个性化的专题,每个专题选取了一定数量的训练文档组成训练数据集,具体的数量如表 1 所示。对训练数据集我们分别采用 LSI 方法和简单的关键词选取的方法来摘要每个个性化类的特征向量,形成每个类对应用户的兴趣模型,而且都采用 KNN 分类算法作为新的个性化文本或信息的识别算法。

表 1 实验结果

Index	Categories	Num train.	Precision	
			LSI	keyword
1	邓小平理论研究	270	86%	67%
2	人工智能技术	189	90%	78%
3	经济学	354	93%	87%
4	图书情报学	253	89%	90%
5	计算机网络	107	92%	88%

通过实验我们发现:如果具有足够数量洁净的训练数据集,基于 LSI 的 KNN 分类算法比简单的关键词选取的兴趣模型方法具有更高的分类和识别精度。潜在语义索引是一种更有效的个性化特征选择算法。

6 结束语

结果表明,由于简单的关键词匹配忽略了词和类之间的内在语义关系,LSI 和 KNN 的结合提高了约 10%~20% 分类识别的精度,基于 LSI 的个性化文本和信息识别具有更高的精度。同时,由于向量空间维数的减少,所以也降低了计算的复杂度,LSI 是一种更有效的个性化特征选择方法。

参考文献:

- [1] 杨清,游星雅,蒋向红. 基于智能信息处理的数字图书馆知识服务系统的研究与设计[J]. 计算机工程与科学, 2004, 26(10):11-14.
- [2] 陈丽群. 个性化服务:高校图书馆服务的新理念[J]. 情报杂志, 2003, 22(7):101-102.
- [3] 魏争光,于迎娣. 个性化服务—图书馆人性化服务的新形式[J]. 图书馆学研究, 2005, (2):43-45.
- [4] Tao Liu, Zheng Chen, Benyu Zhang, et al. Improving Text Classification Using Local Latent Semantic Indexing[A]. Proc of ICDM2004[C]. 2004. 162-169.
- [5] Mingwen Wang, Jianyun Nie. A Latent Semantic Structure Model for Text Classification[EB/OL]. http://www.dcs.vcu.edu/CIR/cikkek/NIE_MFIR2003.pdf, 2004-05.
- [6] H Parry, H Simon, D Chris. On the Use of the Singular Value Decomposition for Text Retrieval[EB/OL]. <http://www.lbl.gov/CS/html/reports.html>, 2000-05.
- [7] S Dumais. Latent Semantic Indexing (LSI): TREC-3 Report [A]. Proc of the 3rd Text Retrieval Conf on NIST Special Publication[C]. 1995. 219-230.
- [8] S Deerwester, S T Dumais, T K Landauer, et al. Indexing by Latent Semantic Analysis[J]. Journal of the Society for Information Science, 1990, 41(6):391-407.
- [9] K J Maschho, D C Sorensen. A Portable Implementation of

ARPACK for Distributed Memory Parallel Computers[A]. Proc of the Copper Mountain Conf on Iterative Methods. Vol 1[C]. 1996.

- [10] 游星雅. 高校网络数字图书馆建设中的知识服务[J]. 湘潭师范学院学报(社科版), 2003, 25(1):141-144.
- [11] 庞剑锋,卜东波,白硕,等. 基于向量空间模型的文本自动分类系统的研究与实现[J]. 计算机应用研究, 2001, 18(9):23-26.

(上接第 14 页)

一个局域网测试环境,将 UA1、UA2 与 SIP Server 放在同一局域网内。测试时使用的 SIP Server 为 Radvision 公司的 Prolab 服务器,各响应时间都是通过 ethereal 抓包计算得出的。

如图 1,定义 UA1 从发送 F5 至接收到 F6 的时间为 t_1 ,接收到 F6 至发送 F7 的时间为 t_2 ,发送 F7 到发送 F8 的时间为 t_3 ;SIP 服务器从接收到 F8 至发送 F9 的时间为 t_4 。则 UA1 从第一次发出 INVITE 的请求至服务器转发其请求的总时间为 $t = t_1 + t_2 + t_3 + t_4$ 。而在图 2 中,定义 UA1 从第一次发出 INVITE 请求至服务器转发其请求的时间为 t' 。测试结果如表 1 所示。

表 1 测试结果

时间	传统的流程	改进后的流程
t_1	2.2	—
t_2	8.0	—
t_3	3.0	—
t_4	1.3	—
t'		4.3
总计	14.5	4.3

从表 1 可看出,对于 UA1 从第一次发出 INVITE 请求至服务器转发其请求的时间,改进后的流程所花费的时间大于传统的流程;但是,对于整个过程的建立,改进后的流程所需时间远小于传统的流程。由于 Prolab 服务器支持标准的 SIP 协议,因此可以看出改进后的流程并没有导致与服务器不兼容。

5 结束语

本文首先介绍了 SIP 的基本内容,然后对 SIP 协议中注册和呼叫流程中的认证机制做出了分析,并提出了改进的方案。改进后的方案缩短了 SIP 的呼叫建立流程,使得服务器免于处理大量重复的认证请求。这对于在 SIP 协议基础上开发商用的 SIP 服务器会有一定的参考价值。

参考文献:

- [1] J Rosenberg, H Schulzrinne, M Handley, et al. SIP: Session Initiation Protocol[R]. RFC 3261, 2002.
- [2] S Zeadally, F Siddiqui. Design and Implementation of a SIP-Based VoIP Architecture[A]. Proc of the 18th Int'l Conf on Advanced Information Networking and Application (AINA) [C]. 2004. 156-158.
- [3] Stefano Salsano, Luca Veltri, Danald Papalilo. The SIP Authentication Procedure and Its Processing Load[J]. IEEE Network, 2002, 16(6):38-44.