(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2006 年1 月5 日 (05.01.2006)

PCT

(10) 国际公布号
WO 2006/000144 A1

(51) 国际专利分类号[7]: H04L 12/66

(21) 国际申请号: PCT/CN2005/000806

(22) 国际申请日: 2005 年6 月8 日 (08.06.2005)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200410069510.0
2004 年6 月28 日 (28.06.2004) CN

(71) 申请人 (对除美国外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

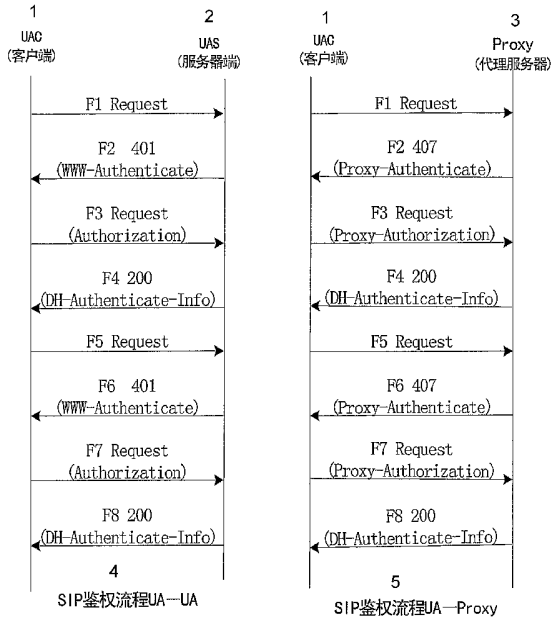
(75) 发明人/申请人 (仅对美国): 周思义(ZHOU, Siyi) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司(UNITALEN ATTORNEYS AT LAW); 中国北京市建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

[见续页]

(54) Title: THE SESSION INITIAL PROTOCOL IDENTIFICATION METHOD

(54) 发明名称: 会话初始协议认证的方法



1 CLIENT-SIDE
2 SERVER-SIDE
3 PROXY SERVER
4 SIP AUTHORIZATION FLOW UA-UA
5 SIP AUTHORIZATION FLOW UA-PROXY

(57) Abstract: The session initial protocol identification method comprises that a client-side sends the request message without identification information to a server and requests to access, and the server sends back the response message with the server-side identification exchange information and the server-side DH identification response information after it received the said request message. The client-side identifies the received response message, and sends the request message with the client-side identification information to the server-side after the identification. The server-side identifies the user based on the received request message, and sendsback he response message with the server-side identification information. The user validates the validity of the server-side from the received response message comprising the server-side identification information. Using this invention can improve the security of the SIP identification effectively.

[见续页]

WO 2006/000144 A1

(81) **指定国**（除另有指明，要求每一种可提供的国家保护）：AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW。

(84) **指定国**（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) 摘要：

本发明公开了一种会话初始协议认证的方法，该方法包括：客户端发送不带认证信息的请求消息到服务器端，请求接入；服务器端收到所述请求消息后回送带有服务器端的认证交换信息及服务器端 DH 认证响应信息的响应消息；客户端对收到的响应消息进行认证，认证通过后，发送带有客户端认证信息的请求消息到服务器端；服务器端根据收到的请求消息对用户进行认证，并回送包含服务器端认证信息的响应消息；用户根据收到的包含服务器端认证信息的响应消息验证服务器端的合法性。利用本发明，可以有效地提高 SIP 认证的安全性。

会话初始协议认证的方法

技术领域

本发明涉及网络安全技术领域，具体涉及一种会话初始协议认证的方法。

背景技术

随着互联网及下一代网络的发展，其方便的接入、逐步提高的接入速度、易于扩展的特性、以及丰富的业务功能，受到了运营商及用户的欢迎，但与此同时其安全性方面也逐步受到人们的关注。SIP（会话初始协议）协议作为下一代网络的核心协议在安全性方面也面临着同样的问题，接入认证是解决这一问题的方式之一，已有的SIP协议（RFC3261）提供了基本的接入认证方式，即所谓的degist（摘要）认证。

SIP协议具有简单、扩展性好及与Internet应用紧密结合的特点，仅用3条消息（INVITE、BYE和ACK）和4个头域（To、From、Call-ID和Cseq）就能实现简单的Internet电话。SIP中有客户机和服务器之分。客户机是指为了向服务器发送请求而与服务器建立连接的应用程序。B2B用户代理（Back to Back User Agent）和代理（Proxy）中含有客户机。服务器是用于向客户机发出的请求提供服务并回送应答的应用程序。共有四类基本服务器:

1. B2B用户代理服务器: 当接到SIP请求时它联系用户，并代表用户返回响应。

2. 代理服务器: 代表其它客户机发起请求，既充当服务器又充当客户机的媒介程序。在转发请 求之前，它可以改写原请求消息中的内容。

3. 重定向服务器: 它接收SIP请求，并把请求中的原地址映射成零个或多个新地址，返回给客户机。

4. 注册服务器: 它接收客户机的注册请求，完成用户地址的注册。 用户终端程序往往需要包括用户代理客户机和用户代理服务器。

SIP的认证过程是一个类似于HTTP（HyperText Transfer Protocol）的无状态的基于Challenge（问询）的机制（RFC2617），基本思路是认证

的双方共享用户名和初始密码。在认证的过程中，认证方向被认证方发送Challenge，被认证方在收到Challenge后，将用户名和初始密码经过加密，形成一个字符串，传递给认证方；认证方将自己知道的用户名和密码通过同样的方式进行加密，得到一个字符串，通过比较该字符串和被认证方传递的字符串是否一致来判断用户的密码是否正确。

在SIP中采用Digest Scheme（摘要机制）的认证方式，具体流程如图1所示。

对于UAS（服务器端），如果需要认证UAC（客户端），则必须发送401 Unauthorized响应，401 Unauthorized响应表示客户试图未经授权访问受密码保护的资源或者客户。401响应中必须携带WWW-Authenticate头域，UAC据此显示用户名字/密码对话框，然后在填写合适的Authorization头后再次发出请求，在Authorization头域中携带认证信息。注册服务器和重定向服务器也可以使用 401 响应来进行认证UAC。

对于Proxy(代理服务器)而言，如果要认证UAC，则必须采用407 Proxy Authentication Required响应，407 Proxy Authentication Required 类似于401，表示客户必须先经过代理服务器的授权，并必须在其中携带Proxy-Authenticate 头域。UAC可以再次发起请求，在Proxy-Authorization头域中携带认证信息。

当UAC因为收到401或者407响应而重新发起请求时，一般应该使用和上一个请求相同的Call-ID，From头域和To头域，但是Cseq头域中的序数必须加一，即有相同Call-ID的请求必须拥有递增的Cseq号。

该认证方式只提供最基本的接入认证功能，在网络安全方面存在以下缺陷:

1、RFC3261中的基本Digest认证机制只能对UAC的Request消息发起认证，对 401或者407响应则没有相应的认证机制，所以很容易导致对UAC发起Plain Text（明文）攻击。

2、由于在RFC3261 Digest所有的认证（只有对UAC的Request消息发起的认证）过程中都使用了初始密钥，所以容易被监听，分析（Authorization 和 Proxy-Authorization）头域，而得出初始密钥，容

易导致字典攻击。

发明内容

本发明的目的是提供一种会话初始协议认证的方法，以提高网络接入的安全性。

本发明的目的是通过以下技术方案实现的：

一种会话初始协议认证的方法，包括：

A、客户端发送不带认证信息的请求消息到服务器端，请求接入；

B、所述服务器端收到所述请求消息后回送带有服务器端的认证交换信息及服务器端DH认证响应信息的响应消息；

C、所述客户端对收到的响应消息进行认证，认证通过后，发送带有客户端认证信息的请求消息到服务器端；

D、所述服务器端根据收到的请求消息对所述用户进行认证，并回送包含服务器端认证信息的响应消息；

E、所述用户根据收到的所述包含服务器端认证信息的响应消息验证所述服务器端的合法性。

所述步骤B包括：服务器端根据用户名和初始密码生成所述服务器端DH认证响应信息。

所述带有客户端认证信息的请求消息包括：可选的客户端的认证交换信息、客户端DH认证响应信息。

所述步骤C包括：

C1、所述客户端根据所述服务器端的认证交换信息及本端的认证交换信息获取共享密钥；

C2、根据所述共享密钥生成所述客户端DH认证响应信息。

所述步骤D包括：

当所述带有客户端认证信息的请求消息的头域中不包括所述用户的认证交换信息时，所述服务器端使用用户名和初始密码对收到的请求消息进行认证；

当所述带有客户端认证信息的请求消息的头域中包括所述用户的认证交换信息时，所述服务器端根据所述用户的认证交换信息以及本端的认

证交换信息获取共享密钥，根据所述共享密钥对收到的请求消息进行认证。

所述步骤D还包括:

当所述带有客户端认证信息的请求消息的头域中不包括所述用户的认证交换信息时，根据所述用户名和初始密码生成所述服务器端DH认证响应信息;

当所述带有客户端认证信息的请求消息的头域中包括所述用户的认证交换信息时，所述服务器端根据所述用户的认证交换信息以及本端的认证交换信息获取共享密钥，根据所述共享密钥生成服务器端DH认证响应信息。

所述包含服务器端认证信息的响应消息包括: 可选的DH认证信息头域。

所述DH认证信息头域包括: 服务器端的验证信息。

所述方法还包括: 在所述客户端和所述服务器端都获取共享密钥后，进行消息交互时，只使用所述共享密钥对所述消息进行加密。

所述服务器端包括: 代理服务器、背靠背服务器、重定向服务器和注册服务器。

由以上本发明提供的技术方案可以看出，本发明在现有 SIP 基本认证基础上，引入 DH（Diffie-Hellman）算法，并对 SIP 头域及字段进行扩展，使初始密钥只在第一次交互中使用，在其他的认证过程中使用共享密钥，使初始密钥得到了充分的保护，可以有效地防止字典攻击; 同时，当任何一方重启后或者希望更换共享密码时，也可以重新启用校验初始密码的方式，通过使用认证次数计数器，有效地防止向 UAS 或者 Proxy 的 replay（重发）攻击。利用本发明，可以大大提高网络的安全性。

附图说明

图1是现有技术中SIP的认证流程;

图2是本发明会话初始协议认证的方法的流程图;

图 3 是本发明方法中用户接入时的消息流程图。

具体实施方式

本发明的核心在于在现有SIP基本认证基础上，引入DH算法，并对SIP头域及字段进行扩展，不仅对用户的请求消息发起认证，而且对服务器端的响应消息也提供相应的认证机制，以便有效地防止对用户发起的Plain Text；同时，在本发明方法中，初始密码只在第一次交互中使用，后续的认证过程都通过共享密码来加密，以便有效地防止字典攻击，而且，当任何一方重启后或者希望更换共享密码时，也可以重新启用校验密码的方式，以便有效地防止replay攻击和兼容异常情况。

为了使本技术领域的人员更好地理解本发明，下面结合附图和实施方式对本发明作进一步的详细说明。

参照图2，图2是本发明方法的详细流程，包括以下步骤：

步骤201：客户端发送不带认证信息的请求消息到服务器端，请求接入。所述服务器端包括：代理服务器、背靠背服务器、重定向服务器和注册服务器。

步骤202：服务器端收到所述请求消息后根据用户名和初始密码生成服务器端DH认证响应信息。

步骤203：向客户端回送带有服务器端的认证交换信息及服务器端DH认证响应信息的响应消息。

步骤204：客户端根据服务器端的认证交换信息及本端的认证交换信息获取共享密钥。

步骤205：根据所述共享密钥生成客户端DH认证响应信息。

步骤206：客户端对收到的响应消息进行认证，认证通过后，发送带有客户端认证信息的请求消息到服务器端。所述带有客户端认证信息的请求消息包括：可选的客户端的认证交换信息、客户端DH认证响应信息。

步骤207：服务器端根据收到的请求消息对用户进行认证，并回送包含服务器端认证信息的响应消息。所述包含服务器端认证信息的响应消息包括：可选的DH认证信息头域。所述DH认证信息头域包括：服务器端的认证信息。

服务器端收到的请求消息有两种情况：该消息的头域中不包括客户端的认证交换信息；该消息的头域中包括客户端的认证交换信息。

当该消息的头域中不包括客户端的认证交换信息时，服务器端使用用户名和初始密码对收到的请求消息进行认证并根据所述用户名和初始密码生成所述服务器端DH认证响应信息。

当该消息的头域中不包括客户端的认证交换信息时，服务器端根据用户的认证交换信息以及本端的认证交换信息获取共享密钥，根据所述共享密钥对收到的请求消息进行认证，并根据所述共享密钥生成服务器端DH认证响应信息。

步骤208：用户根据收到的包含服务器端认证信息的响应消息验证所述服务器端的合法性。

上述过程结束后，也就是说在客户端和服务器端都获取共享密钥后，进行消息交互时，只使用所述共享密钥对所述消息进行加密。

参照图3，图3示出了本发明方法中用户接入时的消息流程：

对于UAS（服务器端），如果需要认证UAC（客户端），则必须发送401响应，并必须在其中携带WWW-Authenticate头域，在该头域中包含UAS的认证，以防止Middle-In-Man攻击。UAC可以再次发起请求，在Authorization头域中携带认证信息。Registrars（注册服务器）和Redirect server（重定向服务器）也可以使用 401 响应来进行认证UAC。

对于Proxy（代理服务器），如果需要认证UAC，则必须发送407响应，并必须在其中携带Proxy-Authenticate头域，在该头域中包含Proxy的认证，以防止Middle-In-Man攻击。UAC可以再次发起请求，在Proxy-Authorization头域中携带认证信息。

当UAC因为收到401或者407响应而重新发起请求时，一般应该使用相同的Call-ID，From头域和To 头域，但是CSeq头域中的序数必须加一。

但是一个Server（UAS或者Proxy）不能向ACK（确认客户端已经接收到对INVITE的最终响应）请求和CANCEL请求发起认证。对于UAC而言，比较好的方式是在ACK消息中包含一个通过认证的认证信息，该认证信息包括Authorization和Proxy-Authorization头域，它是在和ACK对应的INVITE消息中携带的并已经通过UAS或Proxy认证。

为了防止Plain Text攻击，UAS或者Proxy应在认证的成功响应（200）中包含新增头域DH-Authentication-Info，在该新增头域中包含UAS或者Proxy的验证信息，UAC通过该信息验证UAS或者Proxy的合法性。

这可以是一个可选的特性，如果UAC和UAS或者Proxy间配置了必须包含DH-Authentication-Info，则可以实现UAC验证其接入的服务器的合法性。如果在200响应中没有包含DH-Authentication-Info或者验证失败，且在UAC和UAS或者Proxy间配置了必须要包含DH-Authentication-Info，则UAC可以认为这是某个恶意的服务器接收了消息，可以选择拒绝服务器。

在上述认证过程中，只在初始的认证过程中使用初始密钥Ki，而在以后的认证过程中都使用共享密钥Ks，对于图2中的消息而言，F2-F4所使用的密钥是Ki，而F6-F8使用的密钥是Ks。由于Ki只出现一次，所以可以有效地防止Plain Text和字典攻击。

下面详细说明本发明中的SIP头域中的扩展参数及新增的SIP头域:

本技术领域人员知道，在RFC3261中定义了四个头域，分别为：WWW-Authenticate，Proxy-Authenticate，Authorization，Proxy-Authorization，本发明即是在此基础上，通过对这四个头域中参数的扩展实现DH-Digest认证。

本发明中定义的头域如下:

1. **WWW-Authenticate**="WWW-Authenticate" HCOLON challenge
2. **Proxy-Authenticate**="Proxy-Authenticate" HCOLON challenge

其中:

challenge=("Digest" | LWS digest-cln *(COMMA digest-cln)) / dh-challenge / other-challenge

dh-challenge=("DH-Digest" | LWS digest-cln *(COMMA digest-cln))

other-challenge=auth-scheme LWS auth-param*(COMMA auth-param)

digest-cln=realm / domain / nonce / opaque / stale / algorithm / qop-options / dh-b / dh-response-auth / auth-param

realm="realm" EQUAL realm-value

realm-value=quoted-string
domain="domain" EQUAL LDQUOT URI*(1*SP URI) RDQUOT
URI=absoluteURI / abs-path
nonce="nonce" EQUAL nonce-value
nonce-value=quoted-string
opaque="opaque" EQUAL quoted-string
stale="stale" EQUAL ("true" / "false")
algorithm="algorithm" EQUAL ("MD5" / "MD5-sess" / token)
qop-options="qop" EQUAL LDQUOT qop-value
*("," qop-value) RDQUOT
qop-value="auth" / "auth-int" / token
dh-b= "DH-B" EQUAL dh-b-value
dh-b-value=quoted-string
dh-response-auth = "DH-Rspauth" EQUAL dh-response-digest
dh-response-digest=LDQUOT 32LHEX RDQUOT
其中，带下划线部分为头域中新增的参数。

对上述WWW-Authenticate和Proxy-Authenticate头域中的参数说明如下:

realm：realm-value必须是一个全局唯一的字符串，并且全部由可显示的字符组成，用来呈现给用户，指示用户输入用户名及密码。

Domain: 由双引号包含的一个或多个URI列表，表明在这些domain域中，可以使用同样的认证信息。该参数对Proxy-Authenticate头域无意义。

Nonce: nonce是由server提供的一串以16进制或base64表示的随机字符串。

Opaque: opaque是由server提供的一串以16进制或base64表示的随机字符串，客户端应不作任何改变，返回给server。

Stale: 该参数是一个标志，有TRUE和FALSE两个值，用来指示前一

个请求，由于nonce过期而导致的认证失败。当客户端收到的401/407中，该参数值为TRUE时，只需使用新的nonce，重新计算一次摘要即可，不需再要求用户输入用户名及密码。只有当server收到的request中nonce是过期的，但是该过期的nonce对应的摘要正确时（也就是说用户名和密码是正确的），才可将该参数设置为TRUE。

Algorithm: 用于指示两边计算摘要的算法，当没有该参数时，缺省为MD5算法。

qop-options: 为了兼容RFC2069而引入的任选参数，用于指示server所能支持的"quality of protection"，可以带多个值，目前有两个取值："auth" 、"auth-int"（取值不同在加密算法上稍有不同）。具体使用方法参见后面的摘要计算方法。

dh-b: 为了实现DH Digest而特别引入的一个参数，代表了UAS或者Proxy的DH交换数；通过此参数，UAC可以用来计算出共享密钥。

当 scheme 为 DH-Digest ， 而 且 WWW-Authentication 和 Proxy-Authentication中不包含此dh-b时，则意味着UAS或者Proxy已经将db-b在以前的消息中发送给UAC了，当前的这次认证可以直接采用共享密钥，而不需要采用初始密钥（如果UAC不记得共享密钥，如重启后，也可以使用初始密钥进行认证）。当其中包含dh-b时，则表示UAS或者Proxy希望重新发起一次共享密钥的协商。

dh-response-auth: 为了防止恶意服务器发起的401或者407响应，UAC需要对UAS或者Proxy发起的401或者407响应进行认证。UAS或者Proxy在发送401或者407响应时，必须采用初始密钥（当dh-b参数存在时）或者采用共享密钥（当不存在dh-b参数时）进行认证。

auth-param: 该参数是为了将来扩展引入的。

3. **Proxy-Authorization**="Proxy-Authorization" HCOLON credentials
4. **Authorization**="Authorization" HCOLON credentials

其中：

credentials = ("Digest" LWS digest-response) / dh-digest-response
/other-response
digest-response=dig-resp *(COMMA dig-resp)
dh-digest-response= dig-resp *(COMMA dig-resp)
dig-resp=username / realm / nonce / digest-uri
/ dresponse / algorithm / cnonce
/ opaque / message-qop
/ nonce-count / dh-a / auth-param
username="username" EQUAL username-value
username-value=quoted-string
digest-uri="uri" EQUAL LDQUOT digest-uri-value RDQUOT
digest-uri-value=rquest-uri ; Equal to request-uri as specified
by HTTP/1.1
message-qop="qop" EQUAL qop-value
cnonce="cnonce" EQUAL cnonce-value
cnonce-value=nonce-value
nonce-count="nc" EQUAL nc-value
nc-value=8LHEX
dresponse="response" EQUAL request-digest
request-digest=LDQUOT 32LHEX RDQUOT
dh-a= "DH-A" EQUAL dh-a-value
dh-a-value= quoted-string
auth-param=auth-param-name EQUAL (token / quoted-string)
auth-param-name=token
other-response=auth-scheme LWS auth-param*(COMMA auth-param)
auth-scheme=token

其中，带下划线部分为头域中新增的参数。

对上述Authorization和Proxy-Authorization头域中的参数说明如下:

response: 一个128比特的，由32个16进制数表示的字符串，它是由后面的公式计算而来的。

username: 在指定的realm范围内的用户名。

digest-uri: 与最初的Request-Line的 Request-URI相同，之所以不直接使用请求消息中的Request-URI，是因为中间的proxy可能会修改Request-URI。

message-qop: 为了兼容RFC2069而引入的任选参数，用于指示客户端所能支持的“quality of protection（保护质量）”，只能带一个值，且只能是server 过来的qop中的一个值。它将影响对摘要的计算。WWW-Authenticate或Proxy-Authenticate头域中如果包含了qop参数，那么在Authorization或Proxy-Authorization头域中必须带此参数。

cnonce: 如果WWW-Authenticate或Proxy-Authenticate头域中带了qop参数，那么在Authorization或Proxy-Authorization头域中必须带此参数，否则不需要带此参数。该参数由客户端给出，用于避免plain text攻击、提供message integrity protection、以及提供相互的认证。

cnonce-count: 如果WWW-Authenticate或Proxy-Authenticate头域中带了qop参数，那么在Authorization或Proxy-Authorization头域中必须带此参数，否则不需要带此参数。该参数是一个16进制的计算器，用于计数客户端发出的包含nonce的请求消息个数。例如，对于server给定的一个nonce，客户端发出的第一个请求消息，该参数为“nc=00000001”，server会保存自己的一份nc拷贝，这样server能对客户端发过来的该参数的值与自己保存的值进行比较，这样就可以判断是否受到了replay 攻击。

dh-a: 为了实现DH Digest而特别引入的一个参数，代表了UAC的DH交换数；通过此参数，UAS或者Proxy可以用来计算出共享密钥。

当 Authorization 和 Proxy-Authorization 头域中的 scheme 为“DH-Digest”，此时如果头域中包含了dh-a参数，则当前的这次认证是使用初始密钥进行加密的，此时不管Challenge（WWW-Authentication和Proxy-Authentication）中是否包含了dh-b参数，都应该使用初始密钥和

dh-a的算法进行验证（这种情况可能发生在 UAC重启后，发送新的请求，但是UAS或者Proxy并不知道UAC重启了，而仍然希望UAC使用共享密钥来进行验证，此时UAC可以忽略UAS或者Proxy希望通过共享密钥来加密的请求，而通过初始密钥来实现验证）；如果不包含dh-a参数，则意味着在以前的消息中UAC已经将dh-a发送给UAS或者Proxy了，当前的这次认证是使用共享密钥加密的。

根据Authentication-Info的ABNF定义不能扩展参数，所以在本发明中还新增加了一个头域DH-Authentication-Info。

5. **DH-Authentication-Info** = "DH-Authentication-Info" HCOLON dh-ainfo*(COMMA dh-ainfo)

其中：

dh-ainfo=nextnonce / message-qop / response-auth
/ cnonce / nonce-count / dh-a

nextnonce="nextnonce" EQUAL nonce-value

response-auth="rspauth" EQUAL response-digest

response-digest=LDQUOT *LHEX RDQUOT

对上述新增头域 DH-Authentication-Info 中的参数说明如下：

UAS或者Proxy可以利用该头域：

A、改变nonce，客户端收到带nextnonce参数的该头域后，如果要发送下一个请求，则应使用新的nonce进行计算，否则如果客户端仍使用老的nonce计算摘要，server会要求重新认证，并且带指示TRUE的stale参数。此时不需要包含dh-a参数。

B、UAS或Proxy向UAC认证自己，需要携带response-digest参数；此时如果包含了dh-a参数，则此response-digest是采用初始密钥进行加密的；如果没有携带dh-a参数，则此response-digest是采用的共享密钥进行加密的。

Nextnonce：该参数是server给出的客户端下一次发送请求消息时用

的新nonce。

message-qop: 该参数应与客户端发来的qop参数取相同的值，指示server计算response摘要时的"quality of protection"。

为了防止replay攻击，本发明方法规定在上述头域WWW-Authenticate，Proxy-Authenticate，Authorization，Proxy-Authorization使用中必须携带qop参数。

上述参数中涉及的加密算法如下:

1、dh-response-digest（DH响应摘要）的算法如下:

因为在 WWW-Authenticate和Proxy-Authenticate中的qop是一个选项，可以包含auth或者auth-int等多种选择。所以在此强制规定，qop-value为只使用auth。

dh-response-digest = <"> < MD5 (MD5(A1), unq(nonce-value) ":" unq(qop-value)":" MD5(A2)) <">

其中，A1 的算法如下:

如果"algorithm"指示 "MD5" 或没有带该参数，并且没有 dh-b 参数，则 A1 = unq(username-value) ":" unq(realm-value) ":" shared-key

其中，shared-key = < shared key calculated by dh-a and dh-b >

如果"algorithm"指示 "MD5" 或没有带该参数，并且有 dh-b 参数，则 A1 = unq(username-value) ":" unq(realm-value) ":" passwd ":" unq(dh-b)

其中，passwd= < user's password >

dh-b= < dh-b-value >

如果 "algorithm" 指示 "MD5-sess"， 并且没有 dh-b 参数，则 A1=MD5(unq(username-value) ":" unq(realm-value) ":" shared-key) ":" unq(nonce-value))

如果"algorithm"指示 "MD5" 或没有带该参数，并且有 dh-b 参数，则 A1= MD5(unq(username-value) ":" unq(realm-value) ":" passwd ":" unq(dh-b))

A2 的算法如下:

A2= Method ":" digest-uri-value

2、request-digest（请求摘要）的算法如下:

如果 "qop"值为 "auth" 或 "auth-int"，则

request-diges=<">< MD5 (MD5(A1),unq(nonce-value)":" nc-value":" unq(cnonce-value) ":" unq(qop-value) ":" MD5(A2)) <">

其中，A1 的算法如下:

如果"algorithm"指示 "MD5" 或没有带该参数，并且没有 dh-a 参数，则 A1= unq(username-value) ":" unq(realm-value) ":" shared-key

其中，shared-key= < shared key calculated by dh-a and dh-b >

如果"algorithm"指示 "MD5" 或没有带该参数，并且有 dh-a 参数，则 A1 = unq(username-value) ":" unq(realm-value) ":" passwd ":" dh-a

其中，passwd= < user's password >

dh-a= < dh-a-value >

如果 "algorithm" 指示 "MD5-sess"，并且没有 dh-a 参数，则

A1 = MD5(unq(username-value) ":" unq(realm-value) ":" shared-key) ":" unq(nonce-value) ":" unq(cnonce-value)

如果"algorithm"指示 "MD5" 或没有带该参数，并且有 dh-a 参数，则

A1= MD5(unq(username-value) ":" unq(realm-value) ":" passwd ":" dh-a) ":" unq(nonce-value) ":" unq(cnonce-value)

A2 的算法如下:

如果 "qop" 指示 "auth" ，则 A2 = Method ":" digest-uri-value

如果 "qop" 指示"auth-int"，则 A2 = Method ":" digest-uri-value ":" MD5(entity-body)

如果 SIP 的消息体为空，则在 RFC2617 中定义的 A2 中使用的 H(entity-body) 采用如下的定义:

H(entity-body) =MD5("")= "d41d8cd98f00b204e9800998ecf8427e"

3、response-digest（响应摘要）的算法:

response-digest 的算法与前面的 request-digest 算法相似，区别在于 A2 的计算:

如果 Authorization 和 Proxy-Authorization 头域中的 "qop"指示 "auth"，则 A2 = ":" digest-uri-value

如果 Authorization 和 Proxy-Authorization 头域中的 "qop"指示 "auth-int"，则 A2 = ":" digest-uri-value ":" MD5(entity-body)

如果 SIP 的消息体为空，则在 RFC2617 中定义的 A2 中使用的 H(entity-body) 采用如下的定义:

H(entity-body) =MD5("")= "d41d8cd98f00b204e9800998ecf8427e"

虽然通过实施例描绘了本发明，本领域普通技术人员知道，本发明有许多变形和变化而不脱离本发明的精神，希望所附的权利要求包括这些变形和变化而不脱离本发明的精神。

权 利 要 求

1、一种会话初始协议认证的方法，其特征在于包括:

A、客户端发送不带认证信息的请求消息到服务器端，请求接入;

B、所述服务器端收到所述请求消息后回送带有服务器端的认证交换信息及服务器端DH认证响应信息的响应消息;

C、所述客户端对收到的响应消息进行认证，认证通过后，发送带有客户端认证信息的请求消息到服务器端;

D、所述服务器端根据收到的请求消息对所述用户进行认证，并回送包含服务器端认证信息的响应消息;

E、所述用户根据收到的所述包含服务器端认证信息的响应消息验证所述服务器端的合法性。

2、根据权利要求1所述的会话初始协议认证的方法，其特征在于，所述步骤B包括：服务器端根据用户名和初始密码生成所述服务器端DH认证响应信息。

3、根据权利要求1所述的会话初始协议认证的方法，其特征在于，所述带有客户端认证信息的请求消息包括：可选的客户端的认证交换信息、客户端DH认证响应信息。

4、根据权利要求3所述的会话初始协议认证的方法，其特征在于，所述步骤C包括:

C1、所述客户端根据所述服务器端的认证交换信息及本端的认证交换信息获取共享密钥;

C2、根据所述共享密钥生成所述客户端DH认证响应信息。

5、根据权利要求3所述的会话初始协议认证的方法，其特征在于，所述步骤D包括:

当所述带有客户端认证信息的请求消息的头域中不包括所述客户端的认证交换信息时，所述服务器端使用用户名和初始密码对收到的请求消息进行认证;

当所述带有客户端认证信息的请求消息的头域中包括所述客户端的认证交换信息时，所述服务器端根据所述客户端的认证交换信息以及本端

的认证交换信息获取共享密钥，根据所述共享密钥对收到的请求消息进行认证。

6、根据权利要求3所述的会话初始协议认证的方法，其特征在于，所述步骤D还包括:

当所述带有客户端认证信息的请求消息的头域中不包括所述客户端的认证交换信息时，根据所述用户名和初始密码生成所述服务器端DH认证响应信息;

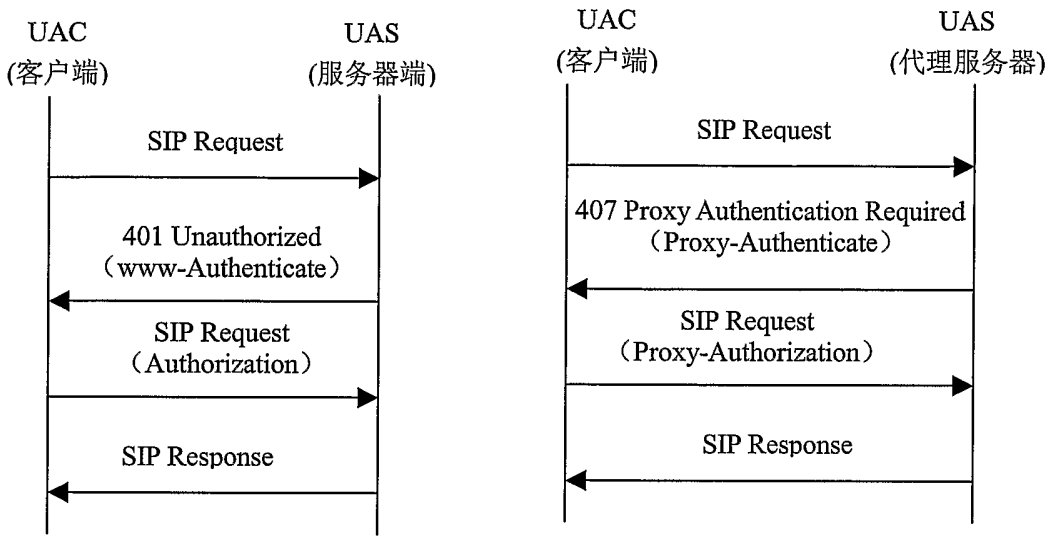
当所述带有客户端认证信息的请求消息的头域中包括所述客户端的认证交换信息时，所述服务器端根据所述客户端的认证交换信息以及本端的认证交换信息获取共享密钥，根据所述共享密钥生成服务器端DH认证响应信息。

7、根据权利要求1或3所述的会话初始协议认证的方法，其特征在于，所述包含服务器端认证信息的响应消息包括: 可选的DH认证信息头域。

8、根据权利要求7所述的会话初始协议认证的方法，其特征在于，所述DH认证信息头域包括: 服务器端的认证信息。

9、根据权利要求6所述的会话初始协议认证的方法，其特征在于，所述方法还包括: 在所述客户端和所述服务器端都获取共享密钥后，进行消息交互时，只使用所述共享密钥对所述消息进行加密。

10、根据权利要求1所述的会话初始协议认证的方法，其特征在于，所述服务器端包括: 代理服务器、背靠背服务器、重定向服务器和注册服务器。



SIP 鉴权流程 UA—UA　　SIP 鉴权流程 UA—Proxy

图 1

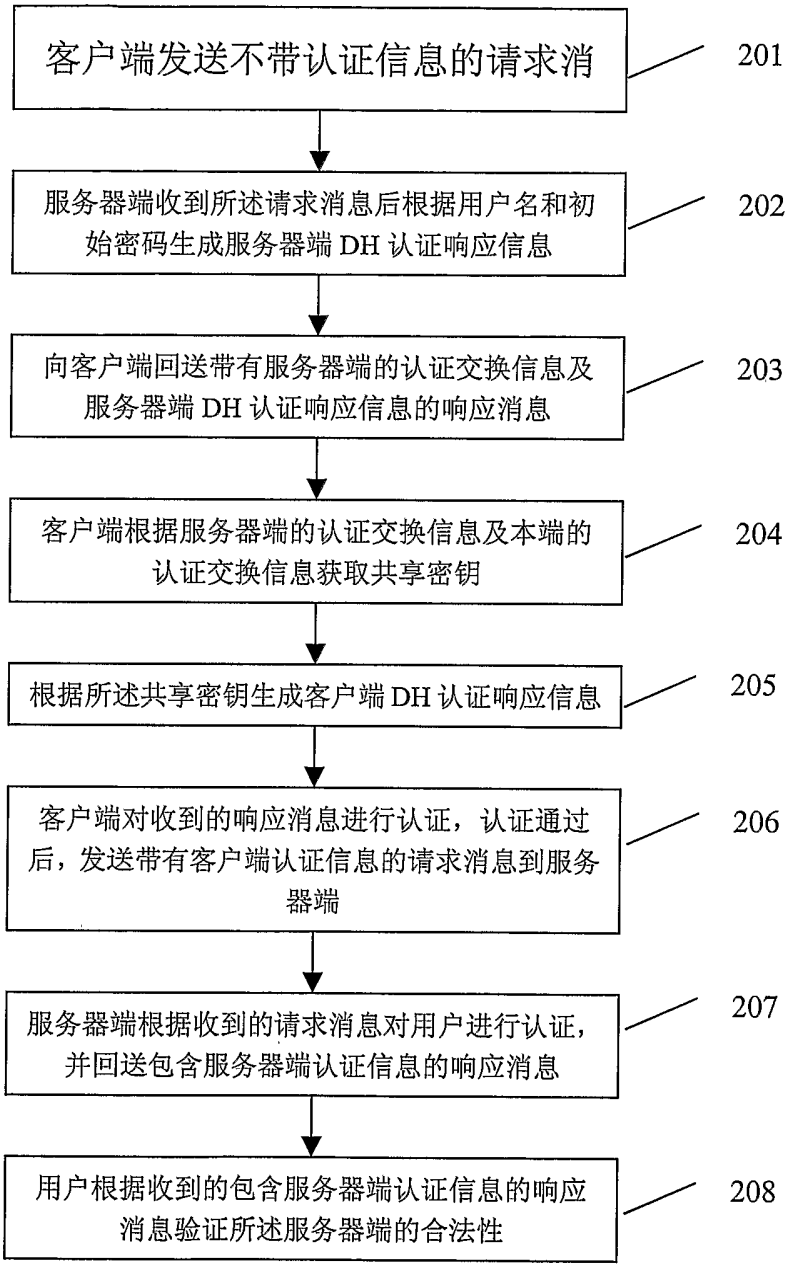

客户端发送不带认证信息的请求消
201
服务器端收到所述请求消息后根据用户名和初始密码生成服务器端 DH 认证响应信息
202
向客户端回送带有服务器端的认证交换信息及服务器端 DH 认证响应信息的响应消息
203
客户端根据服务器端的认证交换信息及本端的认证交换信息获取共享密钥
204
根据所述共享密钥生成客户端 DH 认证响应信息
205
客户端对收到的响应消息进行认证，认证通过后，发送带有客户端认证信息的请求消息到服务器端
206
服务器端根据收到的请求消息对用户进行认证，并回送包含服务器端认证信息的响应消息
207
用户根据收到的包含服务器端认证信息的响应消息验证所述服务器端的合法性
208

图 2

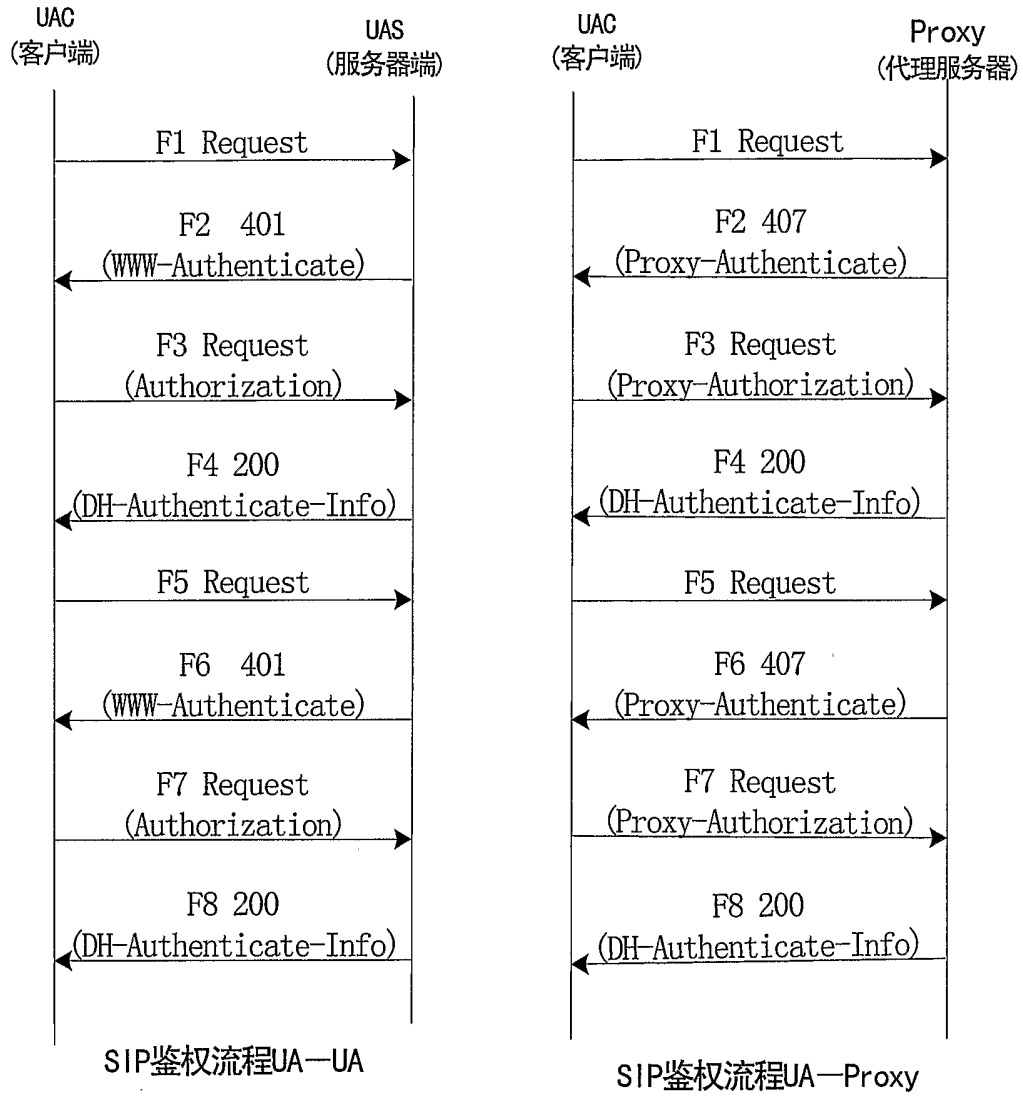

UAC
(客户端)
UAS
(服务器端)
F1 Request
F2 401
(WWW-Authenticate)
F3 Request
(Authorization)
F4 200
(DH-Authenticate-Info)
F5 Request
F6 401
(WWW-Authenticate)
F7 Request
(Authorization)
F8 200
(DH-Authenticate-Info)
SIP鉴权流程UA—UA
UAC
(客户端)
Proxy
(代理服务器)
F1 Request
F2 407
(Proxy-Authenticate)
F3 Request
(Proxy-Authorization)
F4 200
(DH-Authenticate-Info)
F5 Request
F6 407
(Proxy-Authenticate)
F7 Request
(Proxy-Authorization)
F8 200
(DH-Authenticate-Info)
SIP鉴权流程UA—Proxy

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/000806

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7]: H04L12/66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: H04L12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, PAJ(SIP, session initial protocol, identification, authentication, request, server, client, response)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SIP-based media communication system security technology, Tongji University, "data communication", 04.2004, No.2, see the whole document	1—10
A	SIP protocol-based network security analysis, Wuhan University, "computer engineering and design", 03.2004, see the whole document	1—10
A	WO03091891 A1 (- (OYNO) NOKIA CORP - (ISOM-I) ISOMAEKI M - (OYNO) NOKIA INC), 06.Nov 2003 (06.11.2003), see the whole document	1—10
A	WO2004021655 A1 (- (OYNO) NOKIA CORP - (NIEM-I) NIEMI A), 11.Mar 2004(11.03.2004), see the whole document	1—10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05.Sep 2005 (05.09.2005)	22 · SEP 2005 (22 · 09 · 2005)

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer
ZHU Qi
Telephone No. 86-10-62084554

TERNATIONAL SEARCH REPORT
Information patent family members

Search request No.
PCT/CN2005/000806

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO03091891 A1	06.11.2003	US2003204608 A1	30.10.2003
		AU2003215815 A1	10.11.2003
		EP1514194 A1	16.03.2005
WO2004021655 A1	11.03.2004	EP1540907 A1	15.06.2005
		US2004137887 A1	15.07.2004
		AU2003256000 A1	19.03.2004

国际检索报告

国际申请号 PCT/CN2005/000806

A. 主题的分类

IPC[7]: H04L12/66

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[7]: H04L12/66

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,中国期刊全文库, WPI, EPODOC, PAJ(会话初始协议，SIP，认证，请求，服务器，客户，响应，session initial protocol, identification, authentication, request, server, client, response)

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	基于 SIP 的多媒体通信系统安全技术，同济大学交通信息工程及控制研究所，《数据通信》，2004 年 4 月，参见全文	1－10
A	基于 SIP 协议的网络安全性分析，武汉大学，《计算机工程与设计》，2004 年 3 月，参见全文	1－10
A	WO03091891 A1 (- (OYNO) NOKIA CORP - (ISOM-I) ISOMAEKI M - (OYNO) NOKIA INC), 2003 年 11 月 6 日 (06.11.2003), 参见全文	1－10
A	WO2004021655 A1 (- (OYNO) NOKIA CORP - (NIEM-I) NIEMI A) , 2004 年 3 月 11 日(11.03.2004)，参见全文	1－10

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
05.9 月 2005(05.09.2005)	22・9月 2005 (22・09・2005)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 朱琦 电话号码：(86-10)－62084554

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2005/000806

检索报告中引用的专利文件	公布日期	同族专利	公布日期
WO03091891 A1	06.11.2003	US2003204608 A1	30.10.2003
		AU2003215815 A1	10.11.2003
		EP1514194 A1	16.03.2005
WO2004021655 A1	11.03.2004	EP1540907 A1	15.06.2005
		US2004137887 A1	15.07.2004
		AU2003256000 A1	19.03.2004