(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
2009 年5 月14 日 (14.05.2009)

PCT

(10) 国际公布号
WO 2009/059496 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2008/070686

(22) 国际申请日: 2008 年4 月9 日 (09.04.2008)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200710170309.5
2007 年11 月8 日 (08.11.2007) CN
200710195462.3
2007 年11 月27 日 (27.11.2007) 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): **柴晓前 (CHAI, Xiaoqian)** [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)。 **高洪涛 (GAO, Hongtao)** [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)。 **李克鹏 (LI, Kepeng)** [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)。 **田林一 (TIAN, Linyi)** [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)**; 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

(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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 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。

(54) **Title:** A METHOD, SYSTEM, SERVER AND TERMINAL FOR PROCESSING AN AUTHENTICATION

(54) **发明名称:** 进行认证的方法、系统、服务器及终端

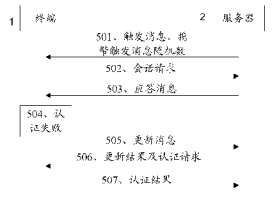

图 5 / Fig. 5

1 TERMINAL
2 SERVER
501 TRIGGER MESSAGE, CARRYING A TRIGGER MESSAGE RANDOM NUMBER
502 SESSION REQUEST
503 RESPONDENCE MESSAGE
504 AUTHENTICATION FAILS
505 UPDATE MESSAGE
506 UPDATE RESULT AND AUTHENTICATION REQUEST
507 AUTHENTICATION RESULT

(57) Abstract: A method for processing an authentication includes: a server generates a trigger message using a trigger message random number, and transmits the trigger message that is generated by using the trigger message random number to a terminal; the terminal can extract the trigger message random number, and when the terminal determines that the trigger message random number is valid, generates a digest using the trigger message random number, and authenticates the trigger message generated by using the trigger message random number; if the authentication is successful, the terminal initiates a session request to the server indicated by the trigger message, the session request contains a session ID. A corresponding system, server, and terminal are also provided. The authentication process of the terminal and server using the DS protocol and DM protocol can be more security by applying this invention.

WO 2009/059496 A1

[见续页]

(57) 摘要：

一种进行认证的方法，包括：服务器使用触发消息随机数生成触发消息，并将所述使用触发消息随机数生成的触发消息发送到终端；以使所述终端可以提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求，所述会话请求中携带会话标识。本发明还公开了相应的系统、服务器、终端。本发明使使用 DS 和 DM 协议的终端和服务器的认证过程更加安全。

进行认证的方法、系统、服务器及终端

本申请要求于 2007 年 11 月 8 日提交中国专利局、申请号为 200710170309.5、发明名称为“进行认证的方法、系统、服务器及终端”、及 2007 年 11 月 27 日提交中国专利局、申请号为 200710195462.3、发明名称为“进行认证的方法、系统、服务器及终端”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术领域，尤其涉及一种使用数据同步（DS，Data Synchronization）协议和设备管理（DM，Device Management）协议进行认证的方法、系统、服务器及终端。

背景技术

同步标记语言（SyncML，Synchronization Mark-up Language）是为了实现多个平台及网络之间个人信息及企业内数据的同步而开发出的协议，其定义了参与操作的实体之间使用的一系列操作，同时定义了承载这些操作的一套消息格式。基于 SyncML，开放行动通讯联盟（OMA，Open Mobile Alliance）开发了 DS 和 DM 协议。

其中，DS 可以在多个平台及网络之间实现个人信息及企业内数据的同步。DS 通常应用于移动设备或应用服务器、与网络服务器之间的数据同步，或两台 PC 之间的数据同步。

DM 是一种通过空中下载技术（OTA，Over The Air）将管理指令数据从网络侧下载到终端设备上，并由终端设备自动运行，进而完成终端软硬件升级、配置、诊断等的低成本远程管理解决方案，同时 DM 还可以将运营商需要的业务信息和终端设备的功能信息等从终端设备传递到服务器侧，以支持其它业务的开展。

在 DS 和 DM 协议中使用了相似的安全认证机制，来实现对服务器（Server）及终端（Client）身份的有效认证，其认证流程如图 1 所示：

步骤 101、服务器发送用于触发会话的触发（Trigger）消息至终端。

该触发消息中携带有：使用服务器随机数（s_nonce）生成的摘要（Digest）、和触发信息（TriggerInfo）。该触发消息可以由 SMS 或其它 Push 消息承载。

s_nonce 为终端生成的随机数（nonce），供服务器使用。

步骤 102、终端发送会话请求消息至服务器。

终端收到 Trigger 消息后，使用保存的 s_nonce 生成 Digest 信息对该 Trigger 消息进行认证，认证通过，则发送会话请求消息至服务器，发起会话。

该会话请求消息中携带有：会话标识（SessionID）、和终端的认证信息（Authenticate），该认证信息为使用终端随机数（c_nonce）生成的 Digest。

c_nonce 为服务器生成的 nonce，供终端使用。

从本步骤开始终端与服务器正式建立会话连接。

步骤 103、服务器返回包含认证结果和认证请求的应答消息。

服务器根据终端发送来的 Authenticate 对终端进行认证，然后向终端返回包含认证结果和服务器认证请求的应答消息。

该应答消息携带有：服务器对终端的身份认证结果、SessionID、服务器的 Authenticate，该 Authenticate 为使用 s_nonce 生成的 Digest。

步骤 104、终端返回包含认证结果的消息至服务器。

终端根据服务器发送来的 Authenticate 对服务器进行认证，然后向服务器返回包含认证结果的消息。

该消息携带有：终端对服务器的身份认证结果、及其他相关信息。

如果服务器对终端的身份认证失败、或终端对服务器的身份认证失败，例如密码错误、或 nonce 值错误，则服务器或者终端可以直接向对方发起质询（challenge）请求重新认证。

当服务器获知其在 Trigger 消息中使用的 s_nonce 错误时，例如服务器发出的多次的 Trigger 消息都没有得到终端的正常回应，则服务器可以认为其使用的 s_nonce 错误，则使用一个值为 0x00000000 的缺省 nonce 生成 Trigger 消息的 Digest，终端在使用 s_nonce 生成的 Digest 对 Trigger 消息进行认证失败后使用缺省 nonce 生成 Digest 对该 Trigger 消息再进行认证，如果认证通过则使用缺省 nonce 进行服务器和终端的身份认证，随后对 s_nonce 和 c_nonce 进行重新更新，更新流程如图 2 所示：

步骤 201、服务器发送用于触发会话的 Trigger 消息至终端。

服务器判断其之前使用的 s_nonce 错误后，使用缺省 nonce 值生成 Trigger

消息发送到终端，该 Trigger 消息中携带有：使用缺省 nonce 值生成的 Digest、和 TriggerInfo。

步骤 202、终端对该 Trigger 消息认证失败，使用缺省 nonce 值重新认证。

终端收到 Trigger 消息后，使用保存的 s_nonce 对该 Trigger 消息进行认证，当由于某种原因认证失败时，终端使用缺省 nonce 值对该 Trigger 消息重新进行认证。

若认证通过，说明服务器之前使用的 s_nonce 错误，终端向服务器发送会话请求消息。

步骤 203、终端发送会话请求消息至服务器。

终端使用缺省 nonce 值认证通过后，发送会话请求消息至服务器，发起会话。

该会话请求消息中携带有：SessionID、使用缺省 nonce 值生成的 Digest。

步骤 204、服务器返回包含认证结果、认证请求和 c_nonce 更新命令的应答消息。

服务器使用缺省 nonce 值对终端进行认证，然后向终端返回包含认证结果和认证请求的应答消息。

该应答消息携带有：服务器对终端的身份认证结果、c_nonce 更新命令、及使用缺省 nonce 值生成的 Digest。

步骤 205、终端返回包含认证结果及 s_nonce 更新命令的消息至服务器。

终端使用缺省 nonce 值对服务器进行认证，认证通过更新 c_nonce，然后向服务器返回包含认证结果及 s_nonce 更新命令的消息。

步骤 206、服务器返回 s_nonce 更新结果至终端。

在对现有技术的研究和实践过程中，发明人发现现有技术存在以下问题：

在处理 s_nonce 错误时使用缺省 nonce 进行认证，由于缺省 nonce 是一个公开的固定不变的值，恶意服务器在截获使用缺省 nonce 的消息后，可以重复发送该消息攻击服务器或终端。

现有技术中的一个会话当中使用了两个 nonce：s_nonce 和 c_nonce，其分别由终端、服务器生成并更新，终端、服务器的管理负担较重。

发明内容

本发明实施例提供一种使用数据同步协议或设备管理协议进行认证的方法、系统、服务器及终端，能够对使用 DS 和 DM 协议的终端和服务器之间的认证过程进行有效优化。

本发明实施例一方面，提供了一种使用数据同步协议或设备管理协议进行认证的方法，所述方法包括:

服务器使用触发消息随机数生成触发消息，并将所述使用触发消息随机数生成的触发消息发送到终端；以使所述终端可以提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求，所述会话请求中携带会话标识。

另一方面，提供了一种使用数据同步协议或设备管理协议进行认证的方法，所述方法包括:

终端获知需要更新服务器随机数;

生成新的服务器随机数，并将所述新的服务器随机数携带在会话请求消息中，发送到所述服务器，以使所述服务器可以在收到所述携带有新的服务器随机数的会话请求消息时，使用所述新的服务器随机数更新自身保存的服务器随机数。

另一方面，提供了一种使用数据同步协议或设备管理协议进行认证的方法，所述方法包括:

终端接收服务器发送的使用缺省随机数生成的触发消息;

所述终端在收到所述触发消息后，首先使用服务器随机数认证所述触发消息，在认证失败后再使用缺省随机数认证触发消息，在认证通过后，使用缺省随机数生成会话请求消息请求会话，在会话中发送新的服务器随机数到所述服务器，使所述服务器更新服务器随机数，并接收服务器发送的使用缺省随机数生成的认证信息以认证服务器身份，并接收服务器发送的更新终端随机数的命令以更新终端随机数;

并在更新所述服务器随机数和终端随机数后更新服务器密码和终端密码。

另一方面，提供了一种使用数据同步协议或设备管理协议进行认证的方法，所述方法包括:

终端向服务器发送使用缺省随机数生成的会话请求消息，以使所述服务器在收到所述会话请求消息后，在确定需要使用缺省随机数进行认证时，使用缺省随机数对所述会话请求消息进行认证，并在认证通过时，向所述终端返回包含认证结果、用缺省随机数生成的认证请求和终端随机数更新命令的应答消息；

终端接收所述应答消息，在确定需要使用缺省随机数进行认证时，使用缺省随机数对所述应答消息进行认证，并在认证通过时，向所述服务器返回包含认证结果和服务器随机数更新命令的应答消息。

另一方面，提供了一种使用数据同步协议或设备管理协议进行认证的方法，所述方法包括：

终端接收服务器发送的使用缺省随机数或会话标识或触发消息标识生成的触发消息；

所述终端在收到所述触发消息后，首先使用服务器随机数认证所述触发消息，在认证失败后再使用缺省随机数或会话标识或触发消息标识认证触发消息，在认证通过后，使用终端随机数生成会话请求消息发送到服务器，以使所述服务器使用终端随机数认证终端。

另一方面，提供了一种使用数据同步协议或设备管理协议进行认证的系统，所述系统包括：

服务器，用于使用触发消息随机数生成触发消息，并发送所述使用触发消息随机数生成的触发消息；

终端，用于接收所述使用触发消息随机数生成的触发消息，提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求。

另一方面，提供了一种服务器，所述服务器包括：

第一生成单元，用于使用触发消息随机数生成符合数据同步协议或设备管理协议规范的触发消息；

发送单元，用于发送所述使用触发消息随机数生成的触发消息到终端，以使所述终端可以提取所述触发消息随机数，在确认所述触发消息随机数有效

时，使用所述触发消息随机数对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求。

另一方面，提供了一种终端，所述终端包括：

接收单元，用于接收所述服务器使用触发消息随机数生成的符合数据同步协议或设备管理协议规范的触发消息；

第一认证单元，用于提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求。

另一方面，提供了一种终端，所述终端包括：

获知单元，用于获知需要更新服务器随机数；

第一生成单元，用于生成新的服务器随机数，并将所述新的服务器随机数携带在会话请求消息中，发送到所述服务器，以使所述服务器可以在收到所述携带有新的服务器随机数的会话请求时，使用所述新的服务器随机数更新自身保存的服务器随机数。

另一方面，提供了一种终端，所述终端包括：

接收单元，用于接收服务器发送的使用缺省随机数生成的符合数据同步协议或设备管理协议规范的触发消息；

生成单元，用于在收到所述触发消息后，首先使用服务器随机数认证所述触发消息，在认证失败后再使用缺省随机数认证所述触发消息，在认证通过后，使用终端随机数生成会话请求发送到服务器，以使所述服务器使用终端随机数认证终端。

通过应用以上的技术方案，可以有效提高系统的安全性。

本发明实施例另一方面，提供了一种使用数据同步协议或设备管理协议进行认证的方法，所述方法包括：

终端接收服务器发送的触发消息；

所述终端在收到所述触发消息后，提取其携带的认证信息对所述服务器进行认证；

认证通过后，终端使用服务器及终端共用随机数生成会话请求，并发送到

所述服务器;

以使所述服务器可以在收到所述会话请求后,使用所述共用随机数对所述终端进行认证;

所述终端在收到所述服务器携带有使用所述共用随机数生成的认证信息应答消息后,使用所述共用随机数对所述服务器进行认证。

通过应用以上技术方案,服务器和终端在会话过程中使用共用的 nonce,替代现有技术的 s_nonce 和 c_nonce 完成终端和服务器之间的认证,有效减轻了系统的负担。

附图说明

图 1 是现有技术的认证方法流程图;

图 2 是现有技术在用缺省 nonce 认证并更新 s_nonce 和 c_nonce 时的流程图;

图 3 是本发明实施例提供的进行认证的方法实施例一流程图;

图 4 是加入 nonce 值后的消息格式实施例结构图;

图 5 是 s_nonce 发生错误时本发明实施例提供的进行认证的方法实施例一流程图;

图 6 是本发明实施例提供的进行认证的方法实施例二流程图;

图 7 是本发明实施例提供的进行认证的方法实施例四流程图;

图 8 是本发明实施例提供的进行认证的方法实施例五的流程图;

图 9 是本发明实施例提供的进行认证的方法实施例六的流程图;

图 10 是本发明实施例提供的进行认证的方法实施例七中携带新的 s_nonce 的状态回复消息格式实施例结构图;

图 11 是本发明实施例提供的进行认证的方法实施例八流程图;

图 12 是本发明实施例提供的进行认证的方法实施例九流程图;

图 13 是本发明实施例提供的进行认证的方法实施例十流程图;

图 14 是本发明实施例提供的进行认证的系统实施例一结构图;

图 15 是本发明实施例提供的终端实施例一结构图;

图 16 是本发明实施例提供的终端实施例二结构图;

图 17 是本发明实施例提供的进行认证的系统实施例二结构图。

具体实施方式

本发明实施例提供了一种使用数据同步协议或设备管理协议进行认证的方法、系统、服务器及终端，有效优化了使用 DS 和 DM 协议的终端和服务器之间的认证过程。

本发明中提到的会话中消息的认证均应用的是应用层安全机制。

本发明实施例提供的进行认证的方法实施例一中，服务器为 Trigger 消息生成一个不同于 s_nonce 和 c_nonce 的供 Trigger 消息使用的 nonce，该 nonce 可以被称作 Trigger 消息 nonce，服务器使用该 nonce 生成认证信息，并将该新的 nonce 及认证信息随 Trigger 消息发送到终端，终端使用新的 nonce 对该 Trigger 消息进行认证。

本发明实施例提供的进行认证的方法实施例一流程如图 3 所示：

步骤 301、服务器发送 Trigger 消息至终端，该消息中携带有 Trigger 消息 nonce。

发送前，服务器先生成 Trigger 消息 nonce，并使用该 nonce 生成 Digest，再使用该 Digest 生成 Trigger 消息。

本实施例提供的使用 Trigger 消息 nonce 的方法可以有三种：

第一种、服务器在生成 Trigger 消息时取自身的系统时间 Ts 作为 Trigger 消息 nonce，并把作为 Trigger 消息 nonce 的系统时间 Ts 携带在 Trigger 消息中，使终端在收到 Trigger 消息后可以通过比对本地时间 Tc 与系统时间 Ts 的差值来确定 nonce 的有效性。对于 nonce 而言，其有效性通常被称为该 nonce 的新鲜性（freshness），新鲜即为有效，否则为无效。

终端在收到 Trigger 消息时，计算系统时间 Ts 与终端本地时间 Tc 的时间差值|Ts-Tc|，若时间差值|Ts-Tc|小于预设的阈值 Diff，则该 Trigger 消息 nonce 为有效值，否则，该 Trigger 消息 nonce 为无效值。

阈值 Diff 通常配置在终端，可以是根据网络情况确定的经验值。这是因为移动网络本身并不稳定，容易造成 Trigger 消息的传输延迟，如果阈值设置太小，则容易使得 Trigger 消息的 nonce 值无效；如果阈值设置较大，若有恶意服务器截获了 Trigger 消息，并不断重复发送该消息到终端，只要时间差值|Ts-Tc|在阈值范围内的，都会被终端认为是有效信息，并进行相应处理，随着

阈值的增大，系统被攻击的机会也在增大。

第二种、服务器在生成 Trigger 消息时，先为目标触发的消息生成会话标识（SessionID），该会话标识的生成可以遵循一定的规则，以使得可以从当前的会话标识推导出以前已经使用的会话标识，然后把该会话标识作为 Trigger 消息 nonce，并使用该 nonce 生成 Digest，再使用该 Digest 生成 Trigger 消息。

终端收到该 Trigger 消息后从中提取该 Trigger 消息要触发的会话标识，并使用该 SessionID、服务器标识、服务器密码及 Trigger 消息的其它字段共同生成 Digest 以认证消息的合法性，并在认证通过后发起会话请求以请求该会话标识所标识的会话。服务器提取会话请求消息中的会话标识以识别会话。

进一步，上述终端在提取该 Trigger 消息要触发的会话标识后，可以通过会话标识的编码规则推断该会话标识的新鲜性，或者在终端保存使用过的会话标识，并将该 Trigger 消息的会话标识与保存的会话标识比较以确定其新鲜性。

该方法中的会话标识也可以使用 Trigger 消息标识（NotificationID）代替，该触发消息标识用于将终端回复的触发消息处理结果与该触发消息进行关联。

第三种、服务器在生成 Trigger 消息时，对每个 Trigger 消息进行编号，取该编号作为专用的 Trigger 消息 nonce，并使用该 nonce 生成 Digest，再使用该 Digest 生成 Trigger 消息。

编号的方式可以是累加的方式，也可以是递减的方式。终端在收到 Trigger 消息时，将其携带的 nonce 与上次保存的 nonce 数值进行比较，在使用累加方式编号时，如果新的 nonce 值较大，则认为该 nonce 值是有效的，否则认为该 nonce 值是无效的；在使用递减方式编号时，如果新的 nonce 值较小，则认为该 nonce 值是有效的，否则认为该 nonce 值是无效的。

终端在判断新的 nonce 值有效并认证服务器身份合法后，保存该新的 nonce 值，用于与下一需判断 Trigger 消息 nonce 值进行比较。

使用本方法时，若有恶意服务器截获了 Trigger 消息，并不断重复发送该消息到终端，对终端进行重放攻击，由于该 Trigger 消息使用的 nonce 值已被记录，所有恶意消息都会被判定为无效消息，因此本发明实施例可以有效的防止恶意服务器的攻击。

进一步，由于移动网络的不稳定性，可能会造成后发的消息先到达终端，

服务器先后为不同会话发出的 Trigger 消息，到达终端的顺序有可能会发生变化，造成终端将有效消息判定为无效消息。

例如，服务器先后为 3 个不同会话发出 3 个 Trigger 消息，3 个 Trigger 消息使用的 Trigger 消息 nonce 分别为：30、31、32，但是由于移动网络的不稳定性，终端最先收到了 nonce 为 32 的 Trigger 消息，终端判定该消息有效，并记录下了该 nonce，另外两个 Trigger 消息到达终端与终端的记录比较时，就会由于比记录的值小被判定为无效消息。

为此，本发明实施例提出了三种解决方式：

方式一、终端保存全部或最近收到的 Trigger 消息 nonce，将判断为无效的 Trigger 消息 nonce 与保存的值相比较，如果没有相同的，则重新判定该值有效，并保存该值。

在存储空间有限时，可以设定保存空间，在保存的 nonce 数量到达上限时将保存的最小 nonce 值删除。

方式二、在 Trigger 消息 nonce 编号的方式是累加的方式时，终端保存接收到的最大的值、及小于当前最大值且未收到过的全部或部分的值，将判断为无效的 Trigger 消息 nonce 与保存的值相比较，如果没相同的，则重新判定该值有效，并保存该值；在 Trigger 消息 nonce 编号的方式是递减的方式时，终端保留接收到的最小的值、及大于当前最小值且未收到过的全部或部分的值，将判断为无效的 Trigger 消息 nonce 与保留的值相比较，如果没相同的，则重新判定该值有效，并保存该值。

例如初始值为“1”，编号方式为累加时，终端顺序收到的 Trigger 消息 nonce 的值为“1”“2”“4”“5”“7”，则终端记录下最大值“7”，及小于 7 且未收到的值“3”“6”，若终端收到的 Trigger 消息 nonce 的值为“6”，则首先将其与最大值“7”相比较，结果是小于“7”，为无效值，则再与“3”“6”比较，结果是存在相同的值，因此可以判断该 Trigger 消息 nonce 有效，终端将其记录的“6“删除。在编号方式为递减时，方法与累加相似，在此不再重复描述。

方式三、在 Trigger 消息 nonce 编号的方式是累加的方式时，保存最大的 nonce 值，所有 nonce 小于该 nonce 的 Trigger 消息均认为是无效的消息；在 Trigger 消息 nonce 编号的方式是递减的方式时，保存最小的 nonce 值，所有

nonce 大于该 nonce 的 Trigger 消息均认为是无效的消息; 服务器在一定时间内没有接到终端的响应消息，则按照编号规则生成新的 nonce，重新发送 Trigger 消息携带此新的 nonce。

以上为本发明实施例提供的使用 Trigger 消息 nonce 的方法的描述。

若使用系统时间或 Trigger 消息编号作为 Trigger 消息的 nonce 时，该 Trigger 消息 nonce 值可以携带在 Trigger 消息的消息头或消息体中。以消息头中携带为例，加入 nonce 值后的消息格式实施例如图 4 所示，包括：摘要（Digest）、触发消息头（trigger-hdr）、触发消息体（trigger-body）。

其中，trigger-hdr 包括：版本（version）、用户交互模式（ui-mode）、会话发起方（initiator）、随机数（nonce）、保留字段（future-use）、会话标识（sessionid）、服务器标识符长度（length-identifier）、服务器标识符（server-identifier）等字段。

同时，本发明实施例还提供了两种使用 Trigger 消息 nonce 生成 Digest 的方法:

方法一、设定：H=MD5 哈希函数（hashing function），b64 = Base64 编码函数，则 Digest 使用公式可以表述为:

Digest= H(B64(H(server-identifier:password)):nonce:B64(H(trigger)))

其中，server-identifier 字段 为服务器标识，password 字段为服务器的密码，nonce 字段为 Trigger 消息随机数（即：前述系统时间 Ts 或者会话标识或者 Trigger 消息编号），trigger 字段为 Trigger 消息的 trigger-hdr 与 trigger-body。

终端收到 Trigger 消息并判断该 Trigger 消息携带的 Trigger 消息 nonce 有效后，在终端管理树上查找该服务器对应的密码，使用查找的密码、及 Trigger 消息中的 server-identifier、nonce、trigger 生成 Digest，比较终端生成的 Digest 与消息中携带的 Digest 是否相同，相同则认证通过，否则认证失败。

方法二、设定：H=MD5 哈希函数（hashing function），b64 = Base64 编码函数。

由于 Trigger 消息 nonce 是携带在消息头或消息体中的，nonce 就成为了 Trigger 消息的 trigger-hdr 与 trigger-body 字段的一部分，因此计算 Digest 可以只使用 Trigger 消息的 trigger-hdr 与 trigger-body 字段，则 Digest 使用公式可以

表述为:

Digest = H(B64(H(server-identifier:password)):B64(H(trigger)))

其中，server-identifier 字段为服务器标识，password 字段为服务器的密码，trigger 字段为 Trigger 消息的 trigger-hdr 与 trigger-body。

终端收到 Trigger 消息并判断该 Trigger 消息携带的 Trigger 消息 nonce 有效后，在终端管理树上查找该服务器对应的密码，使用查找的密码、及 Trigger 消息中的 server-identifier、trigger 生成 Digest，比较终端生成的 Digest 与消息中携带的 Digest 是否相同，相同则认证通过，否则认证失败。

步骤 302、终端判断该信息有效，且对该信息认证通过后，发送会话请求消息至服务器。

终端收到 Trigger 消息后，首先判断该 Trigger 消息携带的 Trigger 消息 nonce 是否有效，判断方法见上文描述，若有效则在终端管理树上查找该服务器对应的密码，使用查找的密码、及 Trigger 消息中的 server-identifier、trigger 生成 Digest，对该 Trigger 消息进行认证，详细认证方法可参考步骤 301 中的描述，根据不同的生成 Digest 的方法，终端生成 Digest 认证的方法也会不同。

若认证通过，则发送会话请求消息至服务器，发起会话。

该会话请求消息中携带有：SessionID、包含使用 c_nonce 生成的 Digest 的 Authenticate。

从本步骤开始终端与服务器正式建立会话连接。

步骤 303、服务器返回包含认证结果和认证请求的应答消息。

服务器根据终端发送来的 Authenticate 对终端进行认证，然后向终端返回包含认证结果和认证请求的应答消息。

该应答消息携带有：服务器对终端的身份认证结果、SessionID、包含使用 s_nonce 生成的 Digest 的 Authenticate。

步骤 304、终端返回包含认证结果的消息至服务器。

终端根据服务器发送来的 Authenticate 对服务器进行认证，然后向服务器返回包含认证结果的消息。

该消息携带有：终端对服务器的身份认证结果、及其他相关消息。

进一步，在使用累加的方式进行 Trigger 消息 nonce 编号时，随着 Trigger

消息的增多，nonce 的值会越来越大；在使用递减的方式进行 Trigger 消息 nonce 编号时，nonce 的值会递减到“0”；在这些时候，可能需要对 nonce 进行调整，例如调整计数起点，因此本发明实施例提供了在需要时对 nonce 的值进行调整的几种方法：

方法一、服务器每隔一段时间都会更新其在终端的账号密码，可以在服务器更新其在终端的账号密码时，服务器和终端双方自动重置 nonce 计数值。

方法二、在需要对 nonce 的值进行调整时，例如预定的时间到了、计数达到预定的值，服务器下发命令直接重置 nonce 值，该命令可以是警告（Alert）命令，例如：

<Alert>

<CmdID>1</CmdID>

<Data>1227</Data> <!-- nonce 计数重置 -->

</Alert>

服务器在对 nonce 的值进行调整后，下发命令，更改其在终端的账号密码，以防止恶意服务器截获消息后进行攻击。

方法三、由于服务器可以直接对终端的终端管理树进行操作，因此服务器可以在终端管理树上的其账号信息中增加一节点，用以保存终端收到并保留的 nonce 值，该节点可以为：

<X>/AppAuth/<X>/SNAAuthCount

然后在需要对 nonce 的值进行调整时，例如预定的时间到了、计数达到预定的值，对该节点下发重置（Replace）命令进行重置。命令实例如下：

<Replace>

<CmdID>4</CmdID>

<Item>

<Target>

<LocURI>./DMAcc/serverA/AppAuth/1/SNAAuthCount</LocURI>

</Target>

<Data>1</Data>

</Item>

</Replace>

服务器在对 nonce 的值进行调整后，下发命令，更改其在终端的账号密码，以防止恶意服务器截获消息后进行攻击。

方法四、在需要对 nonce 的值进行调整时，例如预定的时间到了、计数达到预定的值，终端向服务器发送重置请求，在接收到服务器的确认后双方对 nonce 进行调整。在调整完成后服务器更新终端其在终端的账号密码，以防止恶意服务器截获消息后进行攻击。

在本发明实施例提供的进行认证的方法实施例一中，提供了一个不同于 s_nonce 和 c_nonce 的供 Trigger 消息使用的 nonce，每次发起新的会话，服务器都会生成 Trigger 消息专用的 nonce，用于触发会话，终端使用该 nonce 对 Trigger 消息进行认证，即使服务器保存的 s_nonce 是错误的，终端仍然可以发起会话，此时若 s_nonce 或 c_nonce 发生了错误，都可以通过交互方式更新 s_nonce 或 c_nonce，以完成认证。

以 s_nonce 发生错误为例，本发明实施例提供的进行认证的方法实施例一流程如图 5 所示:

步骤 501、服务器发送 Trigger 消息至终端，该消息中携带有 Trigger 消息 nonce。

发送前，服务器先生成 Trigger 消息 nonce，并使用该 nonce 生成 Digest，再使用该 Digest 生成 Trigger 消息。

步骤 502、终端判断该 Trigger 消息携带的 Trigger 消息 nonce 有效，且对该信息认证通过后，发送会话请求消息至服务器。

终端收到 Trigger 消息后，首先判断该 Trigger 消息携带的 Trigger 消息 nonce 是否有效，判断方法见上文描述，若有效则在终端管理树上查找该服务器对应的密码，使用查找的密码、及 Trigger 消息的 server-identifier、trigger 生成 Digest，对该 Trigger 消息进行认证，详细认证方法可参考步骤 301 中的描述，根据不同的生成 Digest 的方法，终端生成 Digest 认证的方法也会不同。

若认证通过，则发送会话请求消息至服务器，发起会话。

该会话请求消息中携带有：SessionID、包含使用 c_nonce 生成的 Digest 的 Authenticate。

从本步骤开始终端与服务器正式建立会话连接。

步骤 503、服务器返回包含认证结果和认证请求的应答消息。

服务器根据终端发送来的 Authenticate 对终端进行认证，然后向终端返回包含认证结果和认证请求的应答消息。

该应答消息携带有：服务器对终端的身份认证结果、SessionID、包含使用 s_nonce 生成的 Digest 的 Authenticate。

步骤 504、终端使用自身保存的 s_nonce 对服务器进行认证，认证失败。

步骤 505、终端发送质询及 s_nonce 更新消息至服务器。

步骤 506、服务器使用新的 s_nonce 生成认证信息并重发认证请求至终端。

服务器收到更新消息后，根据终端的指示更新自身保存的 s_nonce，并使用更新后的 s_nonce 生成新的认证请求，并将更新结果及新的认证请求发送到服务器。

步骤 507、终端返回包含认证结果的消息至服务器。

终端根据服务器发送来的使用更新后的 s_nonce 生成新的认证请求对服务器进行认证，然后向服务器返回包含认证结果的消息。

该消息携带有：终端对服务器的身份认证结果、及其他相关消息。

在本发明实施例提供的进行认证的方法实施例一中，每次发起新的会话，服务器都会生成 Trigger 消息专用的 nonce，用于触发会话，在本发明实施例提供的进行认证的方法实施例二中，则可以只在服务器认为 s_nonce 错误时，生成 Trigger 消息专用的 nonce，用于触发会话。

本发明实施例提供的进行认证的方法实施例二流程如图 6 所示：

步骤 601、服务器发送 Trigger 消息至终端，该消息中携带有 s_nonce。

步骤 602、服务器发现认证失败。

在一定时间内服务器没有收到终端返回的消息，可以认为是认证失败了。

步骤 603、服务器发送新的 Trigger 消息至终端，该消息中携带有 Trigger 消息 nonce。

发送前，服务器先生成 Trigger 消息 nonce，并使用该 nonce 生成 Digest，再使用该 Digest 生成 Trigger 消息。

步骤 604、终端判断 Trigger 消息携带的 Trigger 消息 nonce 有效，且对该

Trigger 消息认证通过后，发送会话请求消息至服务器。

终端收到 Trigger 消息后，可以通过判断 Trigger 消息是否使用了 Trigger 消息 nonce，来决定使用 s_nonce 还是使用 Trigger 消息 nonce 进行认证。

判断的方法，可以是通过判断 Trigger 消息中是否有 nonce 字段来判断 Trigger 消息是否使用了 Trigger 消息 nonce，即含有 nonce 字段时说明 Trigger 消息使用了 Trigger 消息 nonce; 或者可以通过判断 Trigger 消息的 version 字段信息来判断 Trigger 消息是否使用了 Trigger 消息 nonce，这是因为从消息的 version 可以获知该消息是否使用了 Trigger 消息 nonce。

终端收到 Trigger 消息后，首先判断该 Trigger 消息携带的 Trigger 消息 nonce 是否有效，判断方法见上文描述，若有效则在终端管理树上查找该服务器对应的密码，使用查找的密码、及 Trigger 消息中的 server-identifier、trigger 生成 Digest，对该 Trigger 消息进行认证，详细认证方法可参考步骤 301 中的描述，根据不同的生成 Digest 的方法，终端生成 Digest 认证的方法也会不同。

若认证通过，则发送会话请求消息至服务器，发起会话。

该会话请求消息中携带有：SessionID、包含使用 c_nonce 生成的 Digest 的 Authenticate。

从本步骤开始终端与服务器正式建立会话连接。

步骤 605、服务器返回包含认证结果和认证请求的应答消息。

本步骤与步骤 503 基本类似，在此不再详细描述。

步骤 606、终端使用自身保存的 s_nonce 对服务器进行认证，认证失败。

步骤 607、终端发送包含质询及新的 s_nonce 的消息至服务器。

步骤 608、服务器返回更新结果及新的认证请求至终端。

本步骤与步骤 506 基本类似，在此不再详细描述。

步骤 609、终端返回包含认证结果的消息至服务器。

本步骤与步骤 507 基本类似，在此不再详细描述。

在本发明实施例提供的进行认证的方法实施例二中，在服务器认为 s_nonce 错误时，生成 Trigger 消息专用的 nonce，用于触发会话，终端依然按照本发明实施例提供的进行认证的方法实施例一的方式对该 Trigger 消息进行处理。在本发明实施例提供的进行认证的方法实施例三中，终端可以通过判断

该 Trigger 消息是否使用了 Trigger 消息专用的 nonce，确定是否需要更新 s_nonce，在该 Trigger 消息使用了 Trigger 消息专用的 nonce 时，直接进行 s_nonce 更新，使服务器可以直接使用更新后的 s_nonce 进行会话中的认证。

使用本发明实施例提供的进行认证的方法实施例一、二提供的技术方案，在认证失败时，将不再需要使用缺省 nonce 完成认证，提高了系统的安全性。

同时，本发明实施例提供的进行认证的方法实施例三，在现有技术的基础上，更新过 s_nonce 和 c_nonce 后，相应的更新服务器密码和终端密码，更新服务器密码可以使得使用缺省 nonce 生成的服务器的 Digest 不同，可以防止对终端的消息重放攻击，更新终端密码可以使得使用缺省 nonce 生成的终端的 Digest 不同，可以防止对服务器的消息重放攻击，可以提高系统的安全性。

进一步，本发明实施例提供的进行认证的方法实施例四，在现有技术的基础上，强化步骤之间的关联，以前一步骤作为后一步骤的认证基础，以提高系统的安全性，其流程如图 7 所示:

步骤 701、终端接收到用于触发会话的 Trigger 消息，并对其进行认证。

步骤 702、终端对该 Trigger 消息认证失败，使用缺省 nonce 值重新认证。

步骤 703、终端向服务器发送使用缺省 nonce 生成的会话请求消息

若用缺省 nonce 认证通过，则终端向 Trigger 消息指示的服务器发送会话请求消息，在会话使用应用层安全时在该消息中携带使用缺省 nonce 生成的认证信息，进入步骤 704。若用缺省 nonce 认证失败，则终端忽略该 Trigger 消息，无会话发起，流程结束。

步骤 704、服务器认证终端发送的会话请求消息。

服务器通过两种方式进行认证，分述如下:

方法一、服务器首先使用 c_nonce 生成认证信息进行认证，如果认证通过，则按现有技术方法正常处理。如果认证失败，则使用缺省 nonce 生成认证信息重新认证，若认证通过则使用缺省 nonce 生成服务器认证请求，进入步骤 705。

方法二、服务器在确定会话使用了应用层安全机制，且该服务器发送过使用缺省 nonce 生成的 Trigger 消息给终端，且该 Trigger 消息为触发该会话请求消息的 Trigger 消息时，使用缺省 nonce 对该会话请求消息进行认证，认证通过后进入步骤 705。

判断某会话请求消息是否是被某 Trigger 消息触发的方法为：每个会话请求消息会有一个唯一的会话标识，比较该会话请求消息所携带的会话标识和该 Trigger 消息所携带的会话标识是否相同，若相同则表示该会话是由该 Trigger 消息触发。

判断服务器是否发送过使用缺省 nonce 生成的 Trigger 消息给终端，且该 Trigger 消息为触发该会话请求消息的 Trigger 消息，可以发生在使用缺省 nonce 对该会话请求消息进行认证之后，在认证通过后进行判断，判断通过进入步骤 705。

本步骤的意义在于，若服务器未发送过使用缺省 nonce 生成的用以触发该会话的 Trigger 消息给终端，却收到了终端发送的使用缺省 nonce 生成的会话请求消息，则说明该消息不是一个正常安全的消息，有很大几率是恶意第三方发送的欺骗性消息，可以丢弃处理，因此，采用本步骤后，可以提高系统的安全性。

步骤 705、服务器向终端返回应答消息。

服务器向终端返回包含认证结果、认证请求和 c_nonce 更新命令的应答消息。

步骤 706、终端认证服务器发送的应答消息。

在会话使用了应用层安全机制时，终端使用缺省 nonce 认证服务器，具体认证方法为：终端首先使用 s_nonce 生成认证信息进行认证，如果认证通过，则按现有技术方法正常处理。如果认证失败，则使用缺省 nonce 生成认证信息重新认证，认证通过并更新 c_nonce 后进入步骤 707。

进一步，本步骤也可以在会话使用应用层安全机制，且终端发送过使用缺省 nonce 生成的会话请求消息给服务器时，终端使用缺省 nonce 认证该消息，认证通过并更新 c_nonce 后进入步骤 707。

该步骤中判断终端是否发送过使用缺省 nonce 生成的会话请求消息给服务器，可以发生在使用缺省 nonce 对该消息进行认证之后，在认证通过后进行判断，判断通过进入步骤 707。

步骤 707、终端向服务器返回应答消息。

终端向服务器返回包含认证结果、c_nonce 更新结果及 s_nonce 更新命令

的应答消息。

步骤 708、服务器返回 s_nonce 更新结果至终端。

在完成上述步骤后，为了防止重放攻击，可以选择更新服务器密码，或者同时更新服务器密码及终端密码。

进一步，上述步骤中可以把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 代替缺省 nonce，可以避免使用一个不变的公知的 nonce，进而达到更好的安全性。

通过应用本发明实施例提供的进行认证的方法实施例三、四，可以有效提高系统的安全性。

现有技术中，在 s_nonce 错误需要更新时，需要进行 4 次交互命令才能完成更新，如图 2 的步骤 203 到步骤 204，由于在更新完成前，都需要使用缺省 nonce，安全风险较大，消息在移动网络中的交互次数过多，也加大了网络负担。

本发明实施例提供的进行认证的方法实施例还提供了在终端发送的会话请求消息中携带新的 s_nonce 的技术方案，这样服务器就可以直接进行 s_nonce 更新，并使用新的 s_nonce 进行认证，既减少了信令交互的次数，也减少了使用缺省 nonce 的次数，增加了系统的安全性，也减轻了网络负担。

本发明实施例提供的进行认证的方法实施例五流程如图 8 所示：

步骤 801、终端获知需要更新 s_nonce。

终端判断出 s_nonce 已经过期，或者发现服务器保存的 s_nonce 与终端保存的不一致时，可以获知需要更新 s_nonce。

终端发现服务器保存的 s_nonce 与终端保存的不一致的方法可以为：

终端收到 Trigger 消息后，使用保存的 s_nonce 对该 Trigger 消息进行认证，当由于某种原因认证失败时，终端使用缺省 nonce 值或者会话标识作为 nonce 或者使用 Trigger 消息 ID 作为 nonce 生成 Digest 对该 Trigger 消息重新认证。

若认证通过，则说明服务器之前使用的 s_nonce 错误，服务器保存的 s_nonce 与终端保存的不一致。

步骤 802、终端发送包含更新信息的会话请求消息至服务器。

终端在获知需要更新 s_nonce 时，生成新的 s_nonce，并将该 s_nonce 携带

在会话请求消息中发送至服务器请求发起会话，并使服务器更新 s_nonce。

该会话请求消息中携带有: SessionID、新生成的 s_nonce、包含使用 c_nonce 值生成的 Digest 的 Authenticate。此会话请求消息中，也可以使用缺省 nonce 值或者会话标识作为 nonce 或者使用 Trigger 消息 ID 作为 nonce 生成的 Digest。

新生成的 s_nonce 可以携带在会话请求消息(SyncML)的消息头(SyncHdr)或消息体 (SyncBody)。

以下以携带在消息头中为例说明携带方法。

为了携带 s_nonce，对消息头的定义进行如下修改:

SyncHdr (VerDTD, VerProto, SessionID, MsgID, Target, Source, RespURI?, NoResp?, Cred? , Chal?, Meta?)>

则携带 s_nonce 的 SyncML 消息为:

<SyncML xmlns='SYNCML:SYNCML1.2'>

<SyncHdr>

…

<Chal>

<Meta>

<NextNonce xmlns=’syncml:metinf’>LG3iZQhhdmKNHg==</NextNonce>

</Meta>

</Chal>

</SyncHdr>

<SyncBody>

…

</SyncBody>

</SyncML>

步骤 803、服务器返回包含认证结果、更新结果、及认证请求的应答消息。

服务器收到该会话请求消息后，使用 c_nonce 值对终端进行认证，并使用该会话请求消息携带的更新后的 s_nonce 更新其保存的 s_nonce; 认证通过，更新成功后，再使用更新过的 s_nonce 生成认证请求，并向终端返回包含认证结果、更新命令及认证请求的应答消息。优选的，服务器首先使用 c_nonce 认

证会话请求消息，在认证通过后进行 s_nonce 更新，以保持服务器保存的 s_nonce 和终端保持的 s_nonce 同步。

该应答消息携带有：服务器对终端的身份认证结果、s_nonce 更新结果、及包含使用更新后 s_nonce 值生成的 Digest 的 Authenticate。

步骤 804、终端返回包含认证结果的消息至服务器。

终端使用更新后 s_nonce 值对服务器进行认证，认证通过后，向服务器返回认证结果。

进一步本发明实施例提供的进行认证的方法实施例五也可以应用在本发明实施例提供的进行认证的方法实施例二中，以减少信令交互的次数。

本发明实施例提供的进行认证的方法实施例六的流程图如图 9 所示：

步骤 901、服务器发送 Trigger 消息至终端，该消息中携带有 s_nonce。

步骤 902、服务器发现认证失败。

例如，在一定时间内服务器没有收到终端的会话请求，则可以认为是认证失败了。

步骤 903、服务器发送 Trigger 消息至终端，该消息中携带有 Trigger 消息 nonce。

发送前，服务器先生成 Trigger 消息 nonce，并使用该 nonce 生成 Digest，再使用该 Digest 生成 Trigger 消息。

步骤 904、终端发现需要更新 s_nonce。

终端收到该 Trigger 消息后，判断该 Trigger 消息是否使用了 Trigger 消息专用的 nonce，确定是否需要更新 s_nonce，发现在该 Trigger 消息使用了 Trigger 消息专用的 nonce，需要进行 s_nonce 更新。

判断该 Trigger 消息是否使用了 Trigger 消息专用的 nonce 的方法，可以是通过判断 Trigger 消息中是否有 nonce 字段来判断 Trigger 消息是否使用了 Trigger 消息 nonce，即含有 nonce 字段时说明 Trigger 消息使用了 Trigger 消息 nonce；或者可以通过判断 Trigger 消息的 version 字段信息来判断 Trigger 消息是否使用了 Trigger 消息 nonce，这是因为 version 字段信息中包含有 Trigger 消息是否使用了 Trigger 消息 nonce 的消息。

若发现在该 Trigger 消息使用的不是 Trigger 消息 nonce 时，则说明不需要

进行 s_nonce 更新，直接进入普通处理流程即可。

步骤 905、终端发送包含更新信息的会话请求消息至服务器。

终端收到 Trigger 消息，且确定其使用了 Trigger 消息专用的 Trigger 消息 nonce 后，首先判断该 Trigger 消息携带的 Trigger 消息 nonce 是否有效，判断方法见上文描述，若有效则在终端管理树上查找该服务器对应的密码，使用查找的密码、server-identifier、trigger 生成 Digest，对该 Trigger 消息进行认证，详细认证方法可参考步骤 301 中的描述，根据不同的生成 Digest 的方法，终端生成 Digest 认证的方法也会不同。

终端对该 Trigger 信息认证通过后，生成新的 s_nonce，并将该 s_nonce 携带在会话请求消息中，作为包含更新信息的会话请求消息发送至服务器，发起会话，并使服务器更新 s_nonce。

该会话请求消息中携带有: SessionID、更新后的 s_nonce、包含使用 c_nonce 值生成的 Digest 的 Authenticate。

其中，新生成的 s_nonce 可以携带在会话请求消息的消息头（SyncHdr）或消息体（SyncBody）。

步骤 906、服务器返回包含认证结果、更新结果、及认证请求的应答消息。

服务器收到该会话请求消息后，使用 c_nonce 值对终端进行认证，并使用该会话请求消息携带的更新后的 s_nonce 更新其保存的 s_nonce；认证通过，更新成功后，使用更新过的 s_nonce 生成认证请求，并向终端返回包含认证结果、更新结果、及认证请求的应答消息。

该应答消息携带有：服务器对终端的身份认证结果、s_nonce 更新结果、及包含使用更新后 s_nonce 值生成的 Digest 的 Authenticate。

步骤 907、终端返回包含认证结果的消息至服务器。

终端使用更新后 s_nonce 值对服务器进行认证，认证通过后，向服务器返回认证结果。

该消息携带有：对服务器的身份认证结果、及其他相关消息。

在现有技术中有些时候，终端在认证服务器通过后，可能决定不发起会话，此时若已经发现 s_nonce 过期或错误，需要更新，将无法更新 s_nonce，无法有效维护 s_nonce。

因此，本发明实施例提供的进行认证的方法实施例七中，提供了相应的解决方案。

在本发明实施例提供的进行认证的方法实施例七中，终端在认证服务器通过后，并决定不发起会话时，会向服务器发送一个状态回复消息，当终端判断出 s_nonce 已经过期，或服务器保存的与终端保存的不一致时，生成新的 s_nonce，在该状态回复消息中携带新的 s_nonce、使用 c_nonce、终端用户名、密码、回复消息体等计算出的 Digest，使服务器收到该状态回复消息后，可以根据使用 c_nonce、终端用户名、密码、回复消息体等计算出的 Digest 对该信息进行认证，在认证通过后根据该状态回复消息中携带新的 s_nonce 更新其自身保存的 s_nonce。

该携带新的 s_nonce 的状态回复消息格式实施例如图 10 所示，包括：摘要（Digest）、通知消息头（notification-hdr）、通知消息体（notification -body）。

其中，notification-hdr 包括：版本（version）、状态码（status-code）、对应的通知消息标识（Notification-ID）、新随机数（Next-nonce）、保留（future-use）、会话标识（sessionid）、认证标识长度（length-authname）、认证标识（authname）。

其中的 NextNonce 即携带的新 s_nonce。

在现有技术中，s_nonce 出现问题后，s_nonce 和 c_nonce 都不再使用，终端和服务器都使用缺省 nonce 生成认证信息，这样就造成恶意服务器截获任何一个消息都有可能攻击服务器或终端。

而 s_nonce 和 c_nonce 是两个不同的值，分别由服务器和终端生成，供对方使用，所以一个出现问题并不影响另外一个，本发明实施例提供的进行认证的方法实施例八、及九中，在 s_nonce 出现问题时，提供了单独更新 s_nonce 的解决方案。

s_nonce 出现问题的状况包括：终端判断出 s_nonce 已经过期，或者发现服务器保存的 s_nonce 出了问题，例如终端判断出服务器保存的 s_nonce 与终端的 s_nonce 不一致、不同步。

其中，判断服务器保存的 s_nonce 与终端的 s_nonce 不一致、不同步的方法包括：服务器使用 s_nonce 发出触发消息后，一定时间内没有收到终端回复的信息；或者是终端发现服务器发送的 Trigger 消息中使用缺省 nonce 生成

Digest; 或者是终端发现服务器发送的 Trigger 消息中没有使用 nonce 等。

终端在发现 s_nonce 出现问题，并对服务器身份认证通过后，发起会话请求，会话请求消息中认证终端身份的认证信息用 c_nonce 生成或者使用基础（basic）认证方式，即用户名加密码的认证方式，进一步进行 s_nonce 的更新。

本实施例提供了两种更新 s_nonce 的方法：进行认证的方法实施例七、与进行认证的方法实施例八。

本发明实施例提供的进行认证的方法实施例八中，以服务器使用缺省 nonce 值生成 Trigger 消息为例进行描述，其流程如图 11 所示：

步骤 1101、服务器发送用于触发会话的 Trigger 消息至终端。

服务器判断其之前使用的 s_nonce 错误后，使用缺省 nonce 值生成 Trigger 消息发送到终端，该 Trigger 消息中携带有：使用缺省 nonce 值生成的 Digest、TriggerInfo、及其他相关消息。

步骤 1102、终端对该 Trigger 消息认证失败，使用缺省值重新认证。

终端收到 Trigger 消息后，使用保存的 s_nonce 生成 Digest 对该 Trigger 消息进行认证，当由于某种原因认证失败时，终端使用缺省 nonce 值生成 Digest 对该 Trigger 消息重新进行认证。

若认证通过，则说明服务器之前使用的 s_nonce 错误，服务器保存的 s_nonce 与终端保存的不一致。

步骤 1103、终端发送包含更新信息的会话请求消息至服务器。

终端使用缺省 nonce 值认证通过后，生成新的 s_nonce，并将该 s_nonce 携带在会话请求消息中，作为包含更新信息的会话请求消息发送至服务器，发起会话，并使服务器更新 s_nonce。

该会话请求消息中携带有：SessionID、更新后的 s_nonce、包含使用 c_nonce 值生成的 Digest 的 Authenticate。

进一步，上述步骤中可以把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 代替缺省 nonce，可以避免使用一个不变的公知的 nonce，进而达到更好的安全性。

在会话请求消息中携带更新后的 s_nonce 的方法与实施例三及四基本相同，此处不再赘述。

步骤 1104、服务器返回包含认证结果、更新结果及认证请求的应答消息。

服务器收到该会话请求消息后，使用 c_nonce 值对终端进行认证，并使用该会话请求消息携带的更新后的 s_nonce 更新其保存的 s_nonce；认证通过，更新成功后，再使用更新过的 s_nonce 生成认证请求，向终端返回包含认证结果、更新结果及认证请求的应答消息。

该应答消息携带有：服务器对终端的身份认证结果、s_nonce 更新结果、及包含使用更新后 s_nonce 值生成的 Digest 的 Authenticate。

步骤 1105、终端返回包含认证结果的消息至服务器。

终端使用更新后 s_nonce 值对服务器进行认证，认证通过后，向服务器返回认证结果。

本发明实施例提供的进行认证的方法实施例九中，以服务器使用缺省 nonce 值生成 Trigger 消息，但不在会话请求中携带更新信息为例进行描述，其流程如图 12 所示：

步骤 1201、服务器发送用于触发会话的 Trigger 消息至终端。

服务器判断其之前使用的 s_nonce 错误后，使用缺省 nonce 值生成 Trigger 消息发送到终端，该 Trigger 消息中携带有：使用缺省 nonce 值生成的 Digest、TriggerInfo、及其他相关消息。

步骤 1202、终端对该 Trigger 消息认证失败，使用缺省 nonce 重新认证。

终端收到 Trigger 消息后，使用保存的 s_nonce 生成 Digest 对该 Trigger 消息进行认证，当由于某种原因认证失败时，终端使用缺省 nonce 值生成 Digest 对该 Trigger 消息重新进行认证。

若认证通过，则说明服务器其之前使用的 s_nonce 错误，服务器保存的 s_nonce 与终端保存的不一致。

步骤 1203、终端对该信息认证通过后，发送会话请求消息至服务器。

若认证通过，则发送会话请求消息至服务器，发起会话。

该会话请求消息中携带有：SessionID、包含使用 c_nonce 生成的 Digest 的 Authenticate。

从本步骤开始终端与服务器正式建立会话连接。

步骤 1204、服务器返回包含认证结果和认证请求的应答消息。

服务器根据终端发送来的 Authenticate 对终端进行认证，认证通过，使用缺省 nonce 生成 Authenticate，然后向终端返回包含认证结果和认证请求的应答消息。

该应答消息携带有：服务器对终端的身份认证结果、SessionID、包含使用缺省 nonce 生成的 Digest 的 Authenticate。

步骤 1205、终端返回更新命令、及认证结果到服务器。

终端使用缺省 nonce 对服务器进行认证，认证通过后，生成新的 s_nonce，并发送 s_nonce 更新命令、及对服务器的认证结果到服务器

步骤 1206、服务器返回更新结果至终端。

服务器收到更新消息后，根据终端的指示更新自身保存的 s_nonce，并将更新结果返回给终端。

进一步，上述步骤中可以把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 代替缺省 nonce，可以避免使用一个不变的公知的 nonce，进而达到更好的安全性。

此时为了提供系统的可靠性，可对服务器密码进行更新。

本发明提供的进行认证的方法的又一实施例中，以服务器使用缺省 nonce 值生成 Trigger 消息，但不在会话中携带缺省 nonce 为例进行描述，具体方法说明如下：

服务器在判断其之前使用的 s_nonce 错误后，使用缺省 nonce 值或把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 生成 Trigger 消息发送到终端，该 Trigger 消息中携带有：使用缺省 nonce 值或把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 生成的 Digest、TriggerInfo、及其他相关消息。

终端收到 Trigger 消息后，使用保存的 s_nonce 生成 Digest 对该 Trigger 消息进行认证，当由于某种原因认证失败时，终端使用缺省 nonce 值或把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 生成 Digest 对该 Trigger 消息重新认证，若认证通过，则发送会话请求消息至服务器，发起会话，该会话请求消息中携带有：SessionID、包含使用 c_nonce 生成的 Digest 的 Authenticate。

服务器使用 c_nonce 认证该会话请求消息，认证失败后发起挑战（challenge）以更新 c_nonce 并要求重新认证，认证通过后服务器发送使用

s_nonce 生成的认证请求，终端同样使用 s_nonce 进行认证，认证失败后发起挑战（challenge）以更新 s_nonce 并要求重新认证，认证通过后返回结果。

进一步，上述步骤中终端可以在会话请求消息中携带更新的 s_nonce 给服务器，服务器发送的认证请求使用该新的 s_nonce。

由以上描述可以看出，在 s_nonce 出现问题时只更新 s_nonce，不更新 c_nonce，即使系统在处理 s_nonce 错误时使用缺省 nonce 或把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 进行认证，但由于不需要更新 c_nonce，终端可以使用 c_nonce 生成会话请求，减少了使用缺省 nonce 或把会话标识作为 nonce 或者把 Trigger 消息标识作为 nonce 的次数，系统的安全性得到了提高。

另外，由于一个会话当中使用的 s_nonce 和 c_nonce，分别由终端、服务器生成并更新，因此造成终端、服务器的管理负担较重。

在本发明实施例提供的进行认证的方法实施例十中，一个会话当中使用相同的 nonce，替代现有技术的 s_nonce 和 c_nonce 完成终端和服务器之间的认证，这是由于在同一会话中，有传输层安全或应用层安全认证保证，所以可以使用相同的 nonce 完成终端和服务器之间的认证。

该 nonce 可以由服务器生成，也可以由终端生成，下面将以由服务器生成为例对本发明实施例提供的进行认证的方法实施例十进行详细描述。

本发明实施例提供的进行认证的方法实施例十提供了两种更新 nonce 值的两种方法，分述如下：

方法一、由服务器进行 nonce 值的更新。

首先由服务器下发更新随机数命令（NextNonce），在 NextNonce 命令中携带新 nonce。

终端接收到该 NextNonce 命令后，使用该 NextNonce 命令中携带的新 nonce 更新自身保存的 nonce 值。

该更新命令可以携带在认证消息中，即在该消息中携带了更新命令和服务器的认证信息；或其它管理消息中，即在该消息中没有携带服务器的认证信息。若该更新命令携带在认证消息中，则终端收到该消息后，根据 NextNonce 命令先更新 nonce，再使用更新后的 nonce 生成 Digest 对该信息进行认证，认证必

然会通过，此时若有其它恶意服务器截获了该消息，就可以在任何时间对终端进行重放攻击。为了防止这种情况的出现，在认证消息中携带 NextNonce 命令时，使用未更新前的 nonce 生成的 Digest，终端在收到消息后，先使用更新前的 nonce 生成的 Digest 进行认证，在认证通过后，再根据 NextNonce 命令对自身保存的 nonce 值进行更新；若在其它管理消息中携带 nonce 更新命令，则由于新 nonce 和认证信息分开在两个不同的消息中发送给对方，所以不存在重放攻击风险。

以使用应答消息携带 NextNonce 命令为例，流程如图 13 所示：

步骤 1301、服务器发送用于触发会话的 Trigger 消息至终端。

该触发消息中携带有：使用共用 nonce 生成的 Digest、TriggerInfo。

共用 nonce 为服务器生成，供服务器与终端使用。

在实际使用时，本步骤中的共用 nonce 也可以是触发消息 nonce、或缺省 nonce，在有些时候服务器也可以不使用 nonce，直接使用服务器 ID 和密码生成用于触发会话的 Trigger 消息，而终端也直接使用服务器 ID 和密码生成 Digest 该 Trigger 消息进行认证。

步骤 1302、终端发送会话请求消息至服务器。

终端收到 Trigger 消息后，使用保存的 s_nonce 生成 Digest 对该 Trigger 消息进行认证，认证通过，则发送会话请求消息至服务器，发起会话。

该会话请求消息中携带有：SessionID、包含使用共用 nonce 生成的 Digest 的 Authenticate。

从本步骤开始终端与服务器正式建立会话连接。

步骤 1303、服务器返回包含认证结果和认证请求的应答消息，并在该应答消息中携带 NextNonce 命令。

服务器根据终端发送来的 Authenticate 对终端进行认证，认证通过，并发现共用 nonce 需要更新时，生成新的共用 nonce，然后向终端返回包含认证结果和认证请求的应答消息，并在该应答消息中携带 NextNonce 命令。

该应答消息携带有：服务器对终端的身份认证结果、SessionID、包含使用更新前 nonce 生成的 Digest 的 Authenticate、包含新的 nonce 的 NextNonce 命令。

步骤 1304、终端收到该应答消息后，使用更新前的 nonce 对该消息进行认证。

步骤 1305、认证通过，终端根据 NextNonce 命令的指示，使用 NextNonce 命令携带的新的 nonce 更新自身保存的共用 nonce。

步骤 1306、终端返回包含认证结果、更新结果的消息至服务器。

该消息携带有：终端对服务器的身份认证结果、共用 nonce 的更新结果、及其他相关消息。

由于服务器和终端对共用 nonce 有效时间的定义可能不同，服务器判断共用 nonce 有效时，可能对于终端而言已经到达有效时限了，因此为了保持共用 nonce 对终端的有效性，本发明实施例提供的进行认证的方法实施例十中，提供了终端请求服务器更新共用 nonce 的技术方案。

终端可以使用 DM 命令中的提醒（Alert）命令向服务器请求更新共用 nonce，为了使得服务器可以理解该命令，为其增加一个 Alert 类型以表示请求服务器更新 nonce。

终端在认为共用 nonce 需要更新的时候，通过该 Alert 命令向服务器发送共同 nonce 更新请求，该消息可以携带在认证消息中或其它管理消息中，服务器收到该消息后，根据具体情况决定是否更新。

Alert 类型可以定义为：org.openmobilealliance.NextNonce。

该 Alert 类型的消息实例可以为：

```
<Alert>
<CmdID>2</CmdID>
<Data>1226</Data> <!-- Generic Alert -->
<Item>
  <Meta>
    <Type xmlns="syncml:metinf">
org.openmobilealliance.NextNonce
    </Type>
  </Meta>
<Data/>
```

</Item>

</Alert>

由终端进行 nonce 值更新的方法与由服务器进行 nonce 值的更新的方法类似，这里不再赘述。

方法二、由服务器和终端共同进行 nonce 的更新。

服务器判断共用 nonce 需要更新时，生成一个新的 nonce 进行更新，终端也可以在判断共用 nonce 需要更新时，生成一个新的 nonce 进行更新。

该更新 nonce 的方法可以是：通过 NextNonce 命令进行，实例如下：

<Chal>

<Meta>

<NextNonce xmlns='syncml:metinf'>LG3iZQhhdmKNHg==</NextNonce>

</Meta>

</Chal>

该 NextNonce 命令可以携带在会话过程中的消息中，例如，终端可以将该 NextNonce 命令携带在会话请求中，发送到服务器，请求服务器更新共用 nonce；也可以使用其它消息发送 NextNonce 命令。

不管是服务器进行共同 nonce 的更新还是终端进行共同 nonce 的更新，若该更新命令携带在认证消息中，则对端收到该消息后，先更新 nonce，再使用更新后的 nonce 生成 Digest 对该信息进行认证，认证必然会通过，此时若有其它恶意服务器截获了该消息，就可以在任何时间对终端进行重放攻击。为了防止这种情况的出现，在认证消息中携带 NextNonce 命令时，可以使用更新前的 nonce 生成 Digest 对该信息进行认证，在认证通过后，再根据 NextNonce 命令对自身保存的 nonce 值进行更新；若使用其它管理消息携带该 nonce 更新命令，则由于新 nonce 和认证信息分开在两个不同的消息中发送给对方，所以不存在攻击风险。

在本发明实施例提供的进行认证的方法实施例十中，服务器和终端使用共用的 nonce 进行认证，此时如果共用 nonce 出错，可以使用以上所述的任何一种方式进行处理，在使用本发明实施例提供的进行认证的方法实施例五时，步骤 803 中将携带新的 nonce、及用该 nonce 生成的 Digest，此时若有恶意服务

器截获了该消息，就可以向服务器或终端不断重复发送该消息，进行重放攻击，服务器或终端将无法识别，均认为是有效信息，并进行相应操作，为了防止这种情况，可以使用未更新前的 nonce 生成 Digest，这样服务器在接收到消息后首先使用未更新前的 nonce 计算 Digest 以认证消息发送者，即终端，在认证通过后，再根据 NextNonce 命令对自身保存的 nonce 值进行更新。

使用本发明实施例提供的进行认证的方法实施例十可以有效的减轻系统的负担。

本发明实施例提供的进行认证的系统实施例一结构如图 14 所示，包括:

服务器 1410，用于使用触发消息随机数生成触发消息，并发送所述使用触发消息随机数生成的触发消息;

终端 1420，用于接收所述使用触发消息随机数生成的触发消息，并使用所述触发消息随机数对所述使用触发消息随机数生成的触发消息进行认证，认证所述使用触发消息随机数生成的触发消息的有效性。

其中，服务器 1410 内又包括:

第一生成单元 1412，用于使用触发消息随机数生成触发消息;

发送单元 1411，用于发送所述使用触发消息随机数生成的触发消息;

第二生成单元 1417，用于使用服务器随机数生成触发消息，并将所述使用服务器随机数生成的触发消息发送到所述终端;

判断单元 1413，用于在确定终端对所述使用服务器随机数生成的触发消息认证失败时，控制所述第一生成单元 1412 使用触发消息随机数生成触发消息;

时间单元 1414，用于在所述第一生成单元 1412 使用触发消息随机数生成触发消息时，取所述服务器的系统时间，并将所述系统时间携带在所述使用触发消息随机数生成的触发消息中;

编码单元 1415，用于对所述第一生成单元 1412 使用触发消息随机数生成的触发消息进行编号，使用所述编号作为所述触发消息随机数;

随机数重置单元 1416，用于根据需要对所述编码单元 1415 生成的触发消息随机数进行调整。

会话标识转随机数单元 1418，用于将触发消息所触发会话的会话标识作

为触发消息随机数，以使终端在收到该触发消息时，使用该触发消息随机数对该触发消息进行认证，并在认证通过后发起会话请求以请求该会话标识标识的会话。

其中，编码单元 1415 内又包括:

累加编码单元 14151，用于使用累加的方式对所述使用触发消息随机数生成的触发消息进行编号;

递减编码单元 14152，用于使用递减的方式对所述使用触发消息随机数生成的触发消息进行编号。

其中，终端 1420 内又包括:

接收单元 1421，用于接收所述使用触发消息随机数生成的触发消息;

第一认证单元 1422，用于使用所述触发消息随机数对所述使用触发消息随机数生成的触发消息进行认证，认证所述使用触发消息随机数生成的触发消息的有效性。

第二认证单元 1425，用于在收到所述触发消息时，使用所述服务器随机数对所述触发消息进行认证，并在认证失败后使用触发消息随机数进行重认证。

第一有效判断单元 1423，用于在所述接收单元 1421 收到所述使用触发消息随机数生成的触发消息时，取所述终端的本地时间，以所述本地时间与所述系统时间差值的绝对值与预设的值进行比较，在小于所述预设的值时，判断所述触发消息随机数为有效值，并控制所述第一认证单元 1422 使用所述触发消息随机数对所述使用触发消息随机数生成的触发消息进行认证。

第二有效判断单元 1424，用于在所述接收单元 1421 收到所述使用触发消息随机数生成的触发消息，根据自身保存的触发消息随机数，判断所述触发消息携带的触发消息随机数有效时，保存所述触发消息携带的触发消息随机数，并控制所述第一认证单元 1422 使用所述触发消息随机数对所述使用触发消息随机数生成的触发消息进行认证。

会话标识转随机数单元 1428，用于将所述触发消息所触发会话的会话标识作为所述触发消息随机数，并使用所述触发消息随机数对所述触发消息进行认证，并在认证通过后发起会话请求以请求所述会话标识标识的会话。

所述第二有效判断单元 1424 包括:

第一编码判断单元 14241，用于以所述终端保存的触发消息随机数与所述触发消息携带的触发消息随机数进行比较，在所述触发消息携带的触发消息随机数大于所述保存的最大的触发消息随机数时，或在终端保存的已接收过的触发消息随机数中不包含所述触发消息携带的触发消息随机数时，或在终端保存的未收到过的数值中包含所述触发消息携带的触发消息随机数时，判断所述触发消息携带的触发消息随机数有效。

第二编码判断单元 14242，用于以所述终端保存的触发消息随机数与所述触发消息携带的触发消息随机数进行比较，在所述触发消息携带的触发消息随机数小于所述保存的最小的触发消息随机数时，或在所述保存的已接收过的触发消息随机数中不包含所述触发消息携带的触发消息随机数时，或在终端保存的未收到过的数值中包含所述触发消息携带的触发消息随机数时，判断所述触发消息携带的触发消息随机数有效。

本发明实施例提供的进行认证的系统实施例一的具体运行方式，可参考上文描述的本发明实施例提供的进行认证的方法实施例一、二，在此不再重复描述。

使用本发明实施例提供的进行认证的系统实施例一提供的技术方案，在认证失败时，将不再需要使用缺省 nonce 完成认证，提高了系统的安全性。

本发明实施例提供的服务器实施例一，与上文描述的本发明实施例提供的进行认证的系统实施例一中的服务器基本一致，在此不再重复描述。

本发明实施例提供的终端实施例一结构如图 15 所示，包括:

接收单元 1501，用于接收服务器发送的触发消息;

第一生成单元 1502，用于在收到所述触发消息后，判断服务器随机数需要更新时，生成新的服务器随机数，并将所述新的服务器随机数携带在会话请求中，发送到所述服务器，以使所述服务器可以在收到所述携带有新的服务器随机数的会话请求时，使用所述新的服务器随机数更新自身保存的服务器随机数。

第二生成单元 1503，用于在收到触发消息后，决定不发起会话，判断服务器随机数需要更新时，生成新的服务器随机数，并将所述新的服务器随机数

携带在状态回复消息中，发送到所述服务器，以使所述服务器可以在收到所述携带有新的服务器随机数的状态回复消息时，使用所述新的服务器随机数更新自身保存的服务器随机数。

本发明实施例提供的终端实施例一的具体运行方式，可参考上文描述的本发明实施例提供的进行认证的方法实施例四、五、六，在此不再重复描述。

使用本发明实施例提供的终端实施例一提供的技术方案，在 s_nonce 需要更新时，直接在会话请求消息中携带更新命令，可以减少信令交互的次数，有效减轻系统的负荷，并且可以减少使用缺省 nonce 完成认证的次数，提高了系统的安全性。

本发明实施例提供的终端实施例二，结构如图 16 所示:

终端 1600 包括:

接收单元 1601，用于接收服务器发送的触发消息;

生成单元 1602，用于在收到所述触发消息后，首先使用服务器随机数认证该触发消息，在认证失败后再使用缺省随机数认证该触发消息，在认证通过后，使用终端随机数生成会话请求发送到服务器，以使服务器使用终端随机数认证终端。

密码修改单元 1603，用于在使用所述新的服务器随机数更新服务器随机数完成后，修改服务器密码和终端密码。

本发明实施例提供的终端实施例二的具体运行方式，可参考上文描述的本发明实施例提供的进行认证的方法实施例七、八，在此不再重复描述。

使用本发明实施例提供的终端实施例二提供的技术方案，在 s_nonce 需要更新时，只更新 s_nonce，不更新 c_nonce，即使系统在处理 s_nonce 错误时使用缺省 nonce 进行认证，但由于不需要更新 c_nonce，终端可以使用 c_nonce 生成会话请求，减少了使用缺省 nonce 的次数，系统的安全性得到了提高。

本发明实施例提供的进行认证的系统实施例二结构如图 17 所示，包括:服务器 1710、及终端 1720。

其中，服务器 1710 内又包括:

触发单元 1711，用于使用服务器及终端共用随机数生成触发消息，并发送到终端，以使所述终端在收到所述触发消息后，使用所述共用随机数对所述

触发消息进行认证;

接收单元 1712，用接收终端返回的使用所述共用随机数生成的会话请求;

认证单元 1713，用于使用所述共用随机数对所述会话请求进行认证;

生成单元 1714，用于在对所述会话请求认证通过后，使用所述共用随机数生成应答消息，并发送到所述终端，以使所述终端在收到所述应答消息后，使用所述共用随机数对所述应答消息进行认证。

更新单元 1715，用于生成所述共用随机数，在需要更新所述共用随机数时，生成新的共用随机数，并发送包含所述新的共用随机数的更新随机数消息到所述终端，以使所述终端在收到所述更新随机数消息时，使用所述新的共用随机数更新共用随机数。

请求单元 1716，用于在判断需要更新所述共用随机数时，发送请求更新随机数消息至所述终端，以使所述终端在收到所述请求更新随机数消息，且决定更新后，生成所述新的共用随机数，并发送包含所述新的共用随机数的更新随机数消息。

其中，终端 1720 内又包括:

接收单元 1721，用于接收服务器发送的使用服务器及终端共用随机数生成的触发消息;

第一认证单元 1722，用于在收到所述触发消息后，使用所述共用随机数对所述触发消息进行认证;

生成单元 1723，用于在认证通过后，使用所述共用随机数生成会话请求，并发送到所述服务器，以使所述服务器可以在收到所述会话请求后，使用所述共用随机数对所述会话请求进行认证，认证所述会话请求的有效性;

第二认证单元 1724，用于在收到所述服务器使用所述共用随机数生成的应答消息后，使用所述共用随机数对所述应答消息进行认证。

更新单元 1725，用于生成所述共用随机数，在需要更新所述共用随机数时，生成新的共用随机数，并发送包含所述新的共用随机数的更新随机数消息到所述服务器，以使所述服务器在收到所述更新随机数消息时，使用所述新的共用随机数更新共用随机数。

请求单元 1726，用于在判断需要更新所述共用随机数时，发送请求更新

随机数消息至所述服务器，以使所述服务器在收到所述请求更新随机数消息，且决定更新后，生成所述新的共用随机数，并发送包含所述新的共用随机数的更新随机数消息。

本发明实施例提供的进行认证的系统实施例二的具体运行方式，可参考上文描述的本发明实施例提供的进行认证的方法实施例九，在此不再重复描述。

在本发明实施例提供的进行认证的系统实施例二提供的技术方案中，服务器和终端在会话过程中使用共用的 nonce，替代现有技术的 s_nonce 和 c_nonce 完成终端和服务器之间的认证，有效减轻了系统的负担。

本发明实施例提供的服务器实施例二、及本发明实施例提供的终端实施例三，与本发明实施例提供的进行认证的系统实施例二种描述的服务器及终端基本一致，在此不再重复描述。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上对本发明所提供的一种使用数据同步协议或设备管理协议进行认证的方法、系统、服务器及终端进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权 利 要 求

1、一种使用数据同步协议或设备管理协议进行认证的方法，其特征在于，包括:

服务器使用触发消息随机数生成触发消息，并将所述使用触发消息随机数生成的触发消息发送到终端；以使所述终端可以提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求，所述会话请求中携带会话标识。

2、如权利要求 1 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，在所述服务器使用触发消息随机数生成触发消息之前，所述方法还包括:

所述服务器使用服务器随机数生成触发消息，并将所述使用服务器随机数生成的触发消息发送到终端;

在确定终端对所述使用服务器随机数生成的触发消息认证失败时，所述服务器再使用触发消息随机数生成触发消息。

3、如权利要求 1 或 2 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，所述服务器使用触发消息随机数生成触发消息包括:

所述服务器取所述服务器的系统时间作为触发消息随机数，并将所述系统时间携带在所述使用触发消息随机数生成的触发消息中;

以使所述终端可以在收到所述使用触发消息随机数生成的触发消息时，取所述终端的本地时间与所述触发消息随机数进行比较，判断所述触发消息随机数是否为有效值，在判断所述触发消息随机数为有效值时，使用所述触发消息随机数生成的摘要对所述使用触发消息随机数生成的触发消息进行认证。

4、如权利要求 1 或 2 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，所述服务器使用触发消息随机数生成触发消息包括:

所述服务器使用所述触发消息所触发会话的会话标识作为所述触发消息随机数，以使所述终端在收到所述触发消息时，使用所述触发消息随机数对所述触发消息进行认证，并在认证通过后发起会话请求以请求所述会话标识标识的会话。

5、如权利要求 1 或 2 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，所述服务器使用触发消息随机数生成触发消息包括:

所述服务器使用所述触发消息的标识作为所述触发消息随机数，以使所述终端在收到所述触发消息时，使用所述触发消息随机数对所述触发消息进行认证，所述触发消息标识用于将终端回复的所述触发消息的处理结果与所述触发消息进行关联。

6、如权利要求 1 或 2 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，还包括:

服务器使用累加的方式对所述使用触发消息随机数生成的触发消息进行编号，使用所述编号作为所述触发消息随机数;

以使所述终端可以在收到所述使用触发消息随机数生成的触发消息，根据自身保存的触发消息随机数判断，当所述触发消息携带的触发消息随机数大于所述保存的最大的触发消息随机数时，或在所述保存的已接收过的触发消息随机数中不包含所述触发消息携带的触发消息随机数时，或在所述保存的未收到过的数值中包含所述触发消息携带的触发消息随机数时，确定为所述触发消息携带的触发消息随机数有效，并保存所述触发消息携带的触发消息随机数，并使用所述触发消息随机数生成的摘要对所述使用触发消息随机数生成的触发消息进行认证。

7、如权利要求 6 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，还包括:

对触发消息随机数进行调整。

8、如权利要求 1 或 2 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，所述服务器使用触发消息随机数生成触发消息包括:

所述服务器将所述触发消息随机数携带在所述触发消息的消息头或消息体中，并使用所述触发消息随机数、所述触发消息的消息头和消息体生成摘要，使用所述摘要生成所述触发消息;

或所述服务器将所述触发消息随机数携带在所述触发消息的消息头或消息体中，使用所述触发消息的消息头和消息体生成摘要，使用所述摘要生成所述触发消息。

9、一种使用数据同步协议或设备管理协议进行认证的方法，其特征在于，包括:

终端获知需要更新服务器随机数;

生成新的服务器随机数，并将所述新的服务器随机数携带在会话请求消息中发送到服务器，以使所述服务器可以在收到所述携带有新的服务器随机数的会话请求消息时，使用所述新的服务器随机数更新自身保存的服务器随机数。

10、如权利要求 9 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，所述服务器更新自身保存的服务器随机数具体为:

所述服务器在收到所述会话请求消息时，首先认证所述终端，并在认证通过后使用所述新的服务器随机数更新自身保存的服务器随机数。

11、如权利要求 9 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，将所述新的服务器随机数携带在会话请求中包括:

所述终端将所述新的服务器随机数携带在所述会话请求消息的消息头或消息体中。

12、一种使用数据同步协议或设备管理协议进行认证的方法，其特征在于，包括:

终端接收服务器发送的使用缺省随机数生成的触发消息;

所述终端在收到所述触发消息后，首先使用服务器随机数认证所述触发消息，在认证失败后再使用缺省随机数认证触发消息，在认证通过后，使用缺省随机数生成会话请求消息请求会话，在会话中发送新的服务器随机数到所述服务器，使所述服务器更新服务器随机数，并接收服务器发送的使用缺省随机数生成的认证信息，认证服务器身份，接收服务器发送的更新终端随机数的命令以更新终端随机数;

并在更新所述服务器随机数和终端随机数后更新服务器密码和终端密码。

13、一种使用数据同步协议或设备管理协议进行认证的方法，其特征在于，包括:

终端向服务器发送使用缺省随机数生成的会话请求消息，以使所述服务器在收到所述会话请求消息后，在确定需要使用缺省随机数进行认证时，使用缺省随机数对所述会话请求消息进行认证，并在认证通过时，向所述终端返回包

含认证结果、用缺省随机数生成的认证请求和终端随机数更新命令的应答消息;

终端接收所述应答消息，在确定需要使用缺省随机数进行认证时，使用缺省随机数对所述应答消息进行认证，并在认证通过时，向所述服务器返回包含认证结果和服务器随机数更新命令的应答消息。

14、如权利要求 13 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，所述服务器确定需要使用缺省随机数进行认证具体为:

若服务器发送过使用缺省随机数的用以触发所述会话的触发消息给所述终端，则确定为需要使用缺省随机数进行认证; 或者

服务器首先使用终端随机数生成认证信息进行认证，在认证失败时确定为需要使用缺省随机数进行认证;

所述终端确定需要使用缺省随机数进行认证具体为:

若终端发送过使用缺省随机数的会话请求消息给所述服务器，则确定为需要使用缺省随机数进行认证; 或者

终端首先使用服务器随机数生成认证信息进行认证，在认证失败时确定为需要使用缺省随机数进行认证。

15、一种使用数据同步协议或设备管理协议进行认证的方法，其特征在于，包括:

终端接收服务器发送的使用缺省随机数或会话标识或触发消息标识生成的触发消息;

所述终端在收到所述触发消息后，首先使用服务器随机数认证所述触发消息，在认证失败后再使用缺省随机数或会话标识或触发消息标识认证触发消息，在认证通过后，使用终端随机数生成会话请求消息发送到服务器，以使所述服务器使用终端随机数认证终端。

16、如权利要求 15 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，还包括:

终端发送新的服务器随机数到所述服务器，使所述服务器使用所述新的服务器随机数更新服务器随机数，所述终端将所述新的服务器随机数携带在所述会话请求消息中发送到所述服务器，或者携带在所述服务器发送的挑战消息的

回复消息中发送到所述服务器。

17、如权利要求 15 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，在所述终端使用终端随机数生成会话请求消息并发送到服务器之后，所述方法还包括:

所述终端收到所述服务器返回的使用缺省随机数或会话标识或触发消息标识生成的应答消息后，对服务器进行认证，并认证通过后，发送所述新的服务器随机数到所述服务器，使所述服务器使用所述新的服务器随机数更新服务器随机数。

18、如权利要求 15 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，在所述终端使用终端随机数生成会话请求消息并发送到服务器之后，所述方法还包括:

所述终端接收所述服务器返回的携带使用服务器随机数生成的服务器认证请求的应答消息，并使用服务器随机数对所述服务器进行认证。

19、如权利要求 15、16、17 或 18 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，还包括:

在使用所述新的服务器随机数更新服务器随机数完成后，更新服务器密码。

20、一种使用数据同步协议或设备管理协议进行认证的方法，其特征在于，包括:

终端接收服务器发送的触发消息;

所述终端在收到所述触发消息后，提取其携带的认证信息对所述服务器进行认证;

认证通过后，终端使用服务器及终端共用随机数生成会话请求，并发送到所述服务器;

以使所述服务器可以在收到所述会话请求后，使用所述共用随机数对所述终端进行认证;

所述终端在收到所述服务器携带有使用所述共用随机数生成的认证信息应答消息后，使用所述共用随机数对所述服务器进行认证。

21、如权利要求 19 所述的使用数据同步协议或设备管理协议进行认证的

方法，其特征在于，还包括:

在需要更新所述共用随机数时，生成新的共用随机数，并发送包含所述新共用随机数的更新命令;

收到所述更新命令，使用所述新的共用随机数更新所保存的共用随机数。

22、如权利要求 21 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，还包括:

将所述新的共用随机数携带在会话过程中的认证消息中发送，收到所述认证消息后，使用更新前的随机数生成摘要进行认证;

或者将所述新的共用随机数携带在会话过程中的管理消息中发送。

23、如权利要求 21 或 22 所述的使用数据同步协议或设备管理协议进行认证的方法，其特征在于，还包括:

在判断需要更新所述共用随机数时，发送随机数更新请求;

收到所述随机数更新请求，生成所述新的共用随机数，并发送包含所述新的共用随机数的消息。

24、一种使用数据同步协议或设备管理协议进行认证的系统，其特征在于，包括:

服务器，用于使用触发消息随机数生成触发消息，并发送所述使用触发消息随机数生成的触发消息;

终端，用于接收所述使用触发消息随机数生成的触发消息，提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求。

25、一种服务器，其特征在于，包括:

第一生成单元，用于使用触发消息随机数生成符合数据同步协议或设备管理协议规范的触发消息;

发送单元，用于发送所述使用触发消息随机数生成的触发消息到终端，以使所述终端可以提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求。

26、如权利要求 25 所述的服务器，其特征在于，还包括:

第二生成单元，用于使用服务器随机数生成触发消息，并将所述使用服务器随机数生成的触发消息发送到所述终端，以使所述终端可以使用所述服务器随机数对所述使用服务器随机数生成的触发消息进行认证;

判断单元，用于在确定所述终端对所述使用服务器随机数生成的触发消息认证失败时，控制所述第一生成单元使用触发消息随机数生成触发消息。

27、如权利要求 26 所述的服务器，其特征在于，所述编码单元包括:

累加编码单元，用于使用累加的方式对所述使用触发消息随机数生成的触发消息进行编号，以使所述终端以保存的触发消息随机数与所述触发消息携带的触发消息随机数进行比较，判断所述触发消息携带的触发消息随机数是否有效，有效则使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，并保存所述触发消息携带的触发消息随机数。

28、如权利要求 26 所述的服务器，其特征在于，还包括:

随机数重置单元，用于对所述编码单元生成的触发消息随机数进行调整。

29、如权利要求 26 所述的服务器，其特征在于，还包括:

会话标识转随机数单元，用于将所述触发消息所触发会话的会话标识作为所述触发消息随机数，以使所述终端在收到所述触发消息时，使用所述触发消息随机数对所述触发消息进行认证，并在认证通过后发起会话请求以请求所述会话标识标识的会话。

30、一种终端，其特征在于，包括:

接收单元，用于接收服务器使用触发消息随机数生成的符合数据同步协议或设备管理协议规范的触发消息;

第一认证单元，用于提取所述触发消息随机数，在确认所述触发消息随机数有效时，使用所述触发消息随机数生成摘要对所述使用触发消息随机数生成的触发消息进行认证，在认证通过后，向所述触发消息指示的服务器发起会话请求。

31、如权利要求 30 所述的终端，其特征在于，还包括:

第二认证单元，用于在收到所述触发消息时，使用所述服务器随机数对所述触发消息进行认证，并在认证失败后使用触发消息随机数进行重认证。

32、如权利要求 30 或 31 所述的终端，其特征在于，还包括:

第二有效判断单元，用于在所述接收单元收到所述服务器使用触发消息编号作为触发消息随机数生成的触发消息，根据自身保存的触发消息随机数判断，当所述触发消息携带的触发消息随机数大于终端保存的最大的触发消息随机数时，或在终端保存的已接收过的触发消息随机数中不包含所述触发消息携带的触发消息随机数时，或在终端保存的未收到过的数值中包含所述触发消息携带的触发消息随机数时，确定为所述触发消息携带的触发消息随机数有效，并保存所述触发消息携带的触发消息随机数，并控制所述第一认证单元使用所述触发消息随机数对所述使用触发消息随机数生成的触发消息进行认证。

33、如权利要求 30 或 31 所述的终端，其特征在于，还包括:

会话标识转随机数单元，用于将所述触发消息所触发会话的会话标识作为所述触发消息随机数，并使用所述触发消息随机数对所述触发消息进行认证，并在认证通过后发起会话请求以请求所述会话标识标识的会话。

34、一种终端，其特征在于，包括:

获知单元，用于获知需要更新服务器随机数;

第一生成单元，用于生成新的服务器随机数，并将所述新的服务器随机数携带在会话请求消息中，发送到所述服务器，以使所述服务器可以在收到所述携带有新的服务器随机数的会话请求时，使用所述新的服务器随机数更新自身保存的服务器随机数。

35、一种终端，其特征在于，包括:

接收单元，用于接收服务器发送的使用缺省随机数生成的符合数据同步协议或设备管理协议规范的触发消息;

生成单元，用于在收到所述触发消息后，首先使用服务器随机数认证所述触发消息，在认证失败后再使用缺省随机数认证所述触发消息，在认证通过后，使用终端随机数生成会话请求发送到服务器，以使所述服务器使用终端随机数认证终端。

36、如权利要求 35 所述的终端，其特征在于，还包括:

密码修改单元，用于在使用所述新的服务器随机数更新服务器随机数完成后，更新服务器密码。

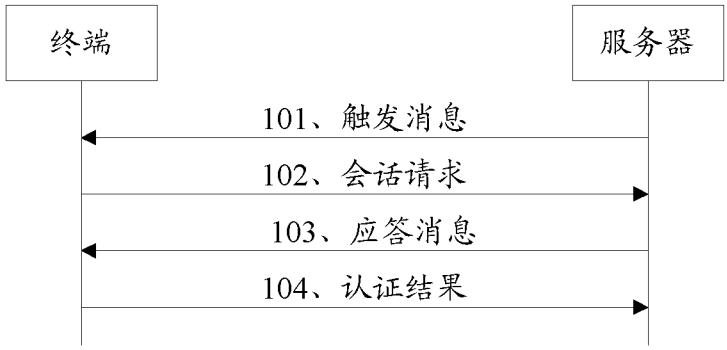
终端
服务器
101、触发消息
102、会话请求
103、应答消息
104、认证结果

图 1

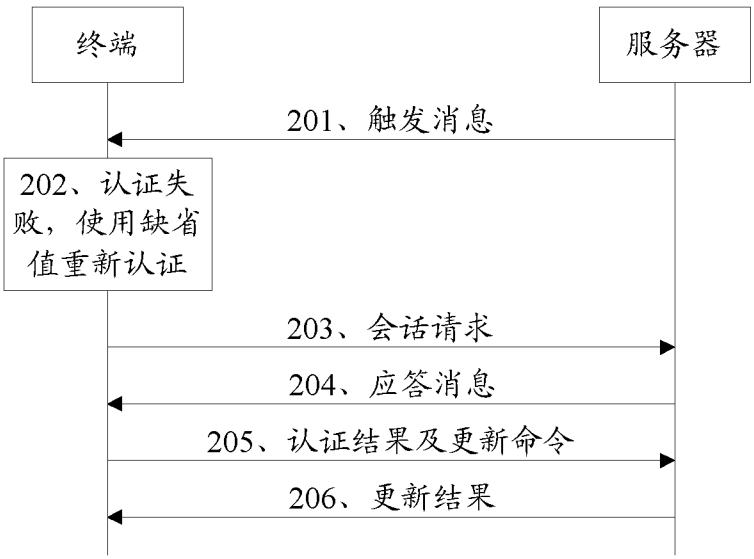
终端
服务器
201、触发消息
202、认证失败，使用缺省值重新认证
203、会话请求
204、应答消息
205、认证结果及更新命令
206、更新结果

图 2

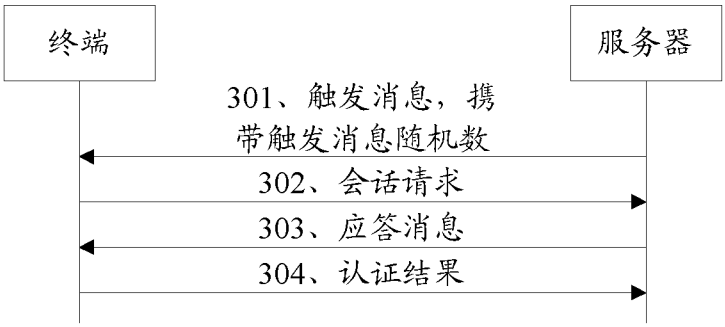
终端
服务器
301、触发消息，携带触发消息随机数
302、会话请求
303、应答消息
304、认证结果

图 3

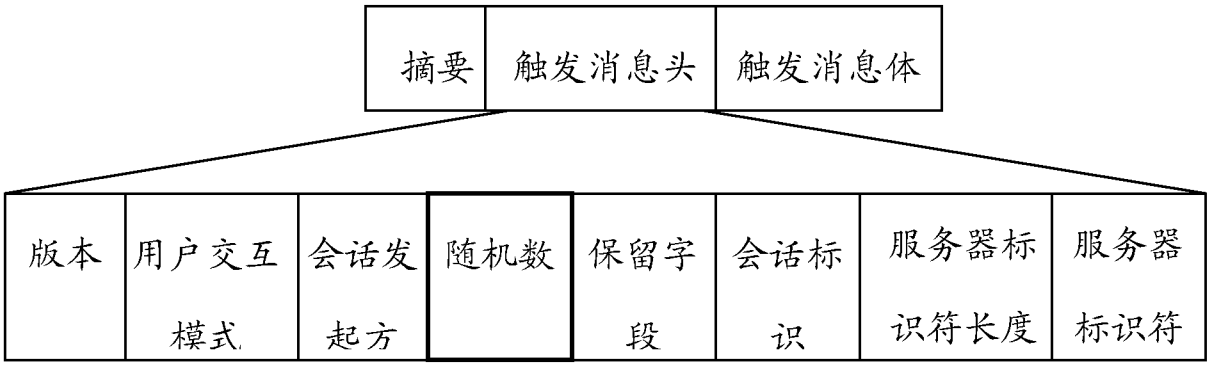
摘要
触发消息头
触发消息体
版本
用户交互模式
会话发起方
随机数
保留字段
会话标识
服务器标识符长度
服务器标识符

图 4

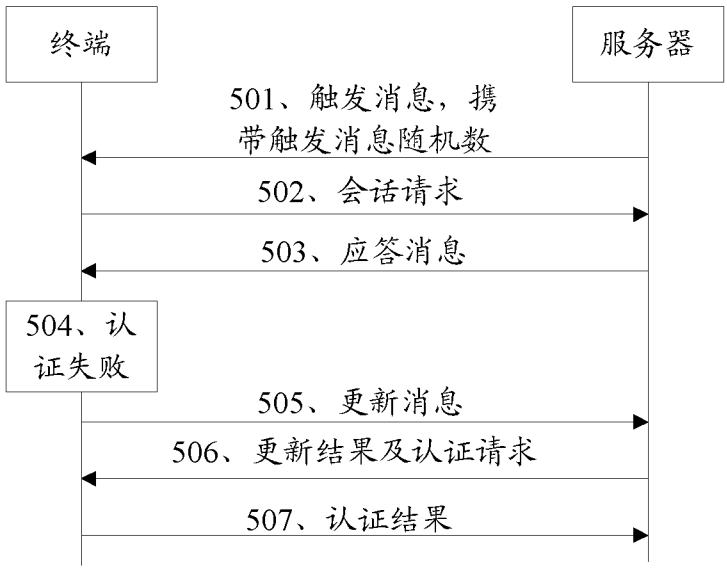
终端
服务器
501、触发消息，携带触发消息随机数
502、会话请求
503、应答消息
504、认证失败
505、更新消息
506、更新结果及认证请求
507、认证结果

图 5

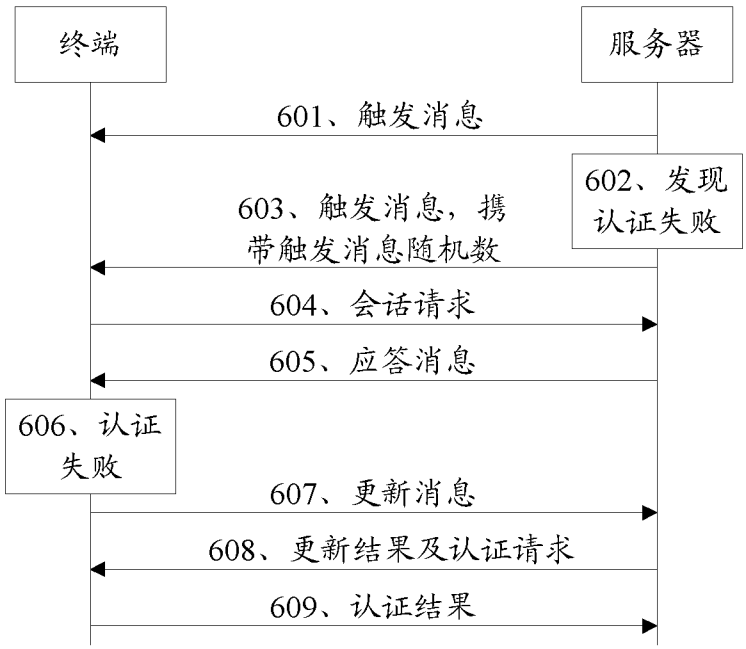
终端
服务器
601、触发消息
602、发现认证失败
603、触发消息，携带触发消息随机数
604、会话请求
605、应答消息
606、认证失败
607、更新消息
608、更新结果及认证请求
609、认证结果

图 6

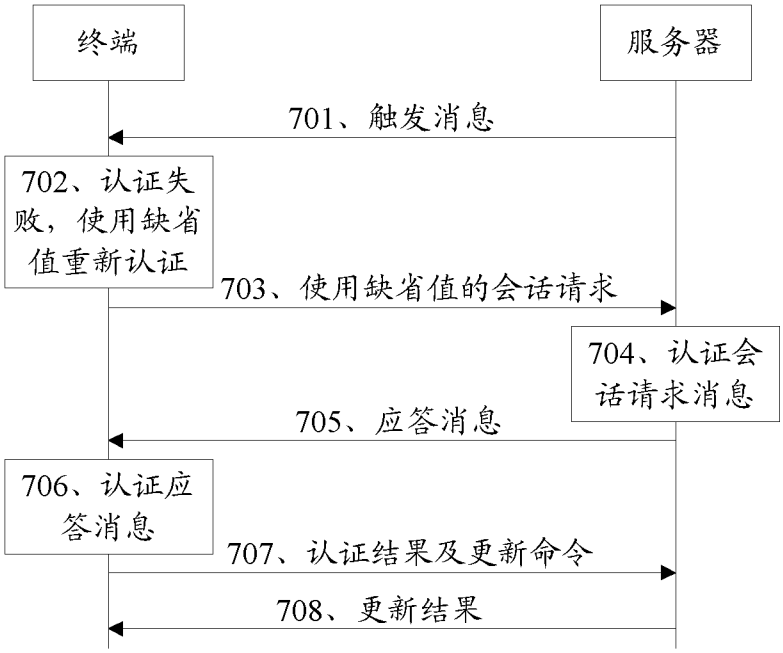
终端
服务器
701、触发消息
702、认证失败，使用缺省值重新认证
703、使用缺省值的会话请求
704、认证会话请求消息
705、应答消息
706、认证应答消息
707、认证结果及更新命令
708、更新结果

图 7

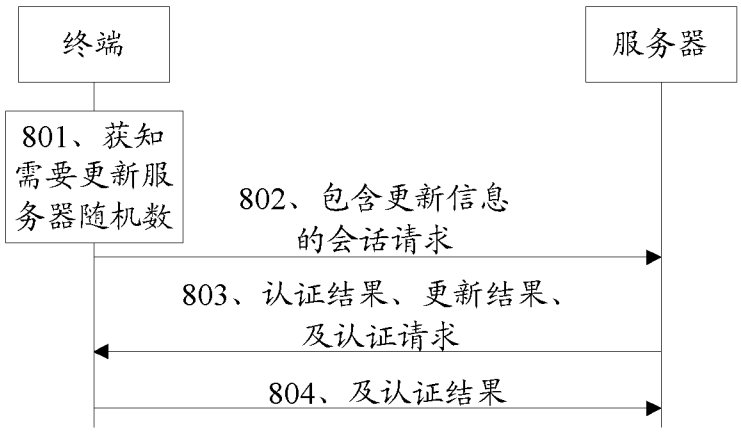
终端
服务器
801、获知需要更新服务器随机数
802、包含更新信息的会话请求
803、认证结果、更新结果、及认证请求
804、及认证结果

图 8

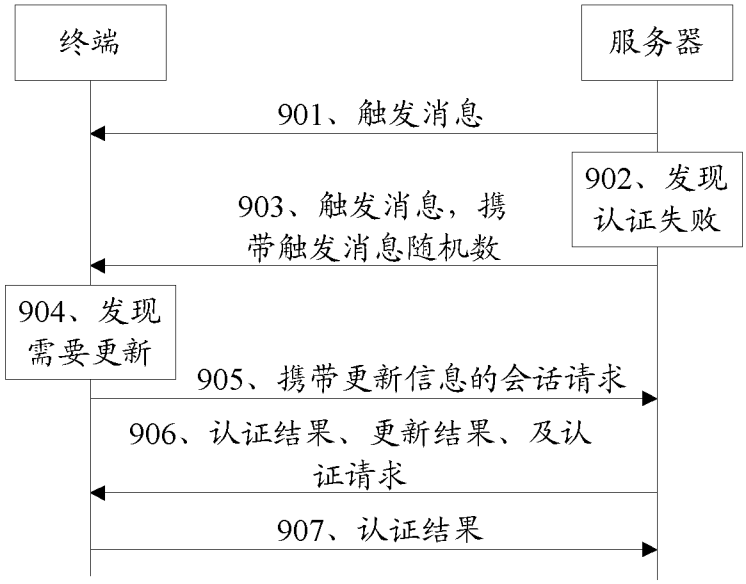
终端
服务器
901、触发消息
902、发现认证失败
903、触发消息，携带触发消息随机数
904、发现需要更新
905、携带更新信息的会话请求
906、认证结果、更新结果、及认证请求
907、认证结果

图 9

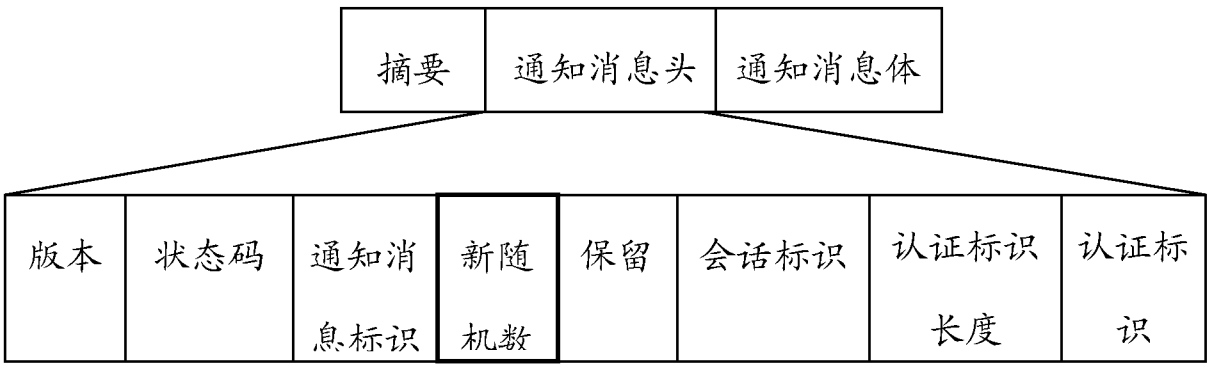
摘要
通知消息头
通知消息体
版本
状态码
通知消息标识
新随机数
保留
会话标识
认证标识长度
认证标识

图 10

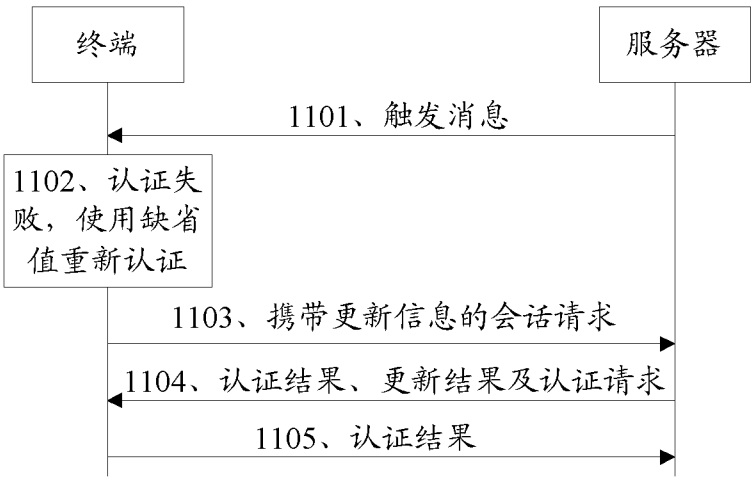
终端
服务器
1101、触发消息
1102、认证失败，使用缺省值重新认证
1103、携带更新信息的会话请求
1104、认证结果、更新结果及认证请求
1105、认证结果

图 11

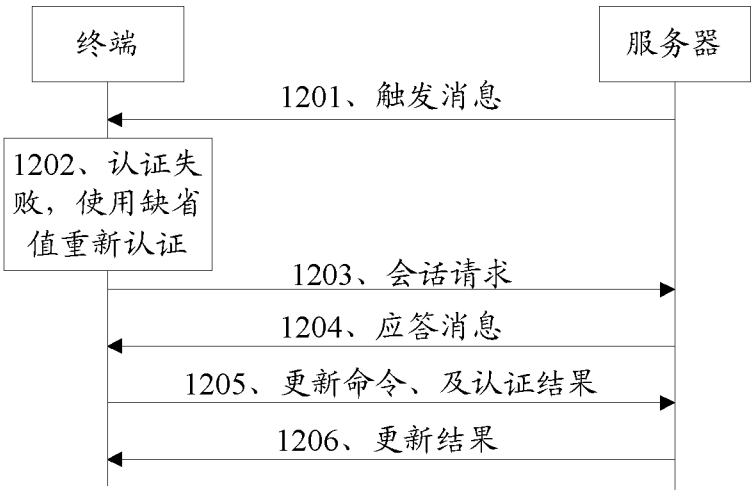
终端
服务器
1201、触发消息
1202、认证失败，使用缺省值重新认证
1203、会话请求
1204、应答消息
1205、更新命令、及认证结果
1206、更新结果

图 12

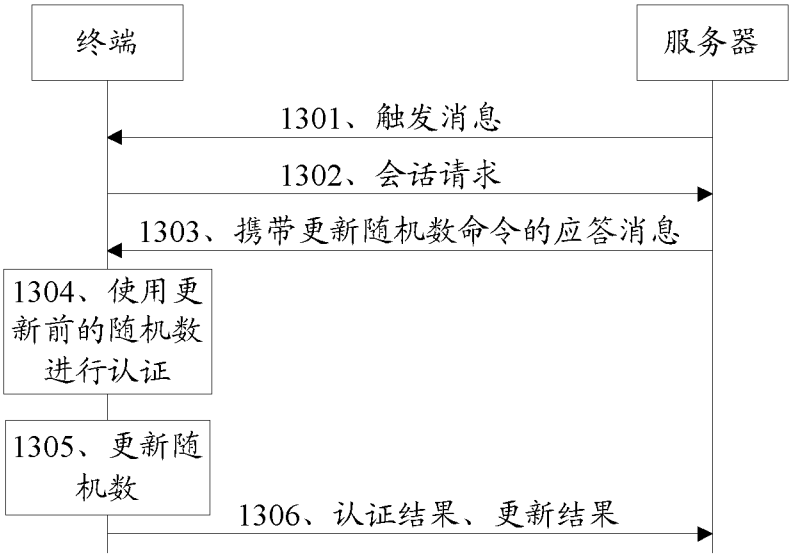
终端
服务器
1301、触发消息
1302、会话请求
1303、携带更新随机数命令的应答消息
1304、使用更新前的随机数进行认证
1305、更新随机数
1306、认证结果、更新结果

图 13

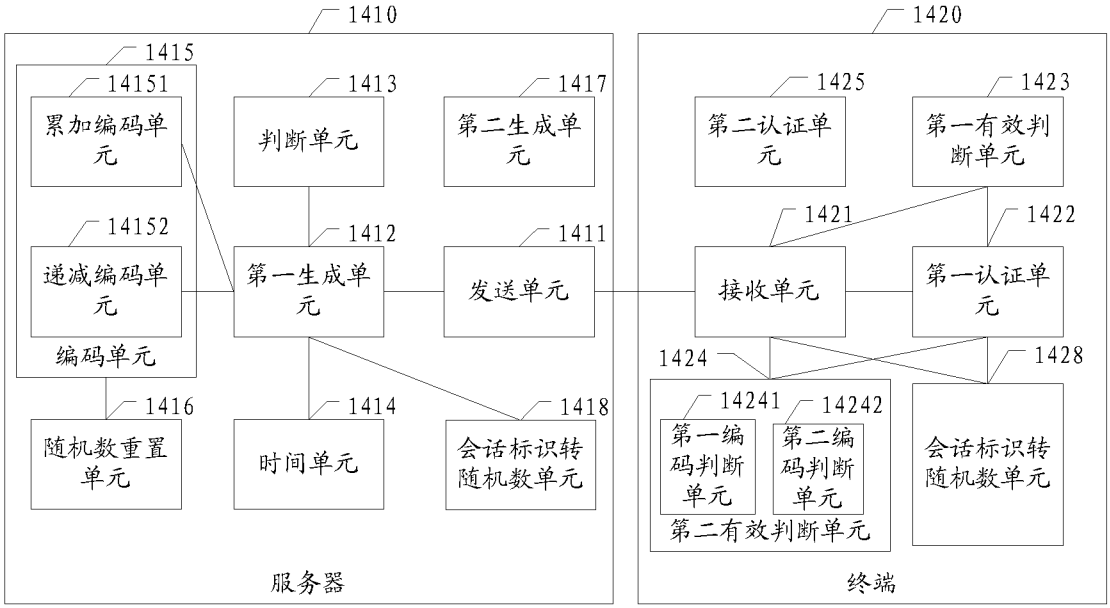
1410
1415
14151
累加编码单元
14152
递减编码单元
编码单元
1413
判断单元
1412
第一生成单元
1417
第二生成单元
1411
发送单元
1416
随机数重置单元
1414
时间单元
1418
会话标识转随机数单元
服务器
1420
1425
第二认证单元
1423
第一有效判断单元
1421
1422
接收单元
第一认证单元
1424
1428
14241
第一编码判断单元
14242
第二编码判断单元
第二有效判断单元
会话标识转随机数单元
终端

图 14

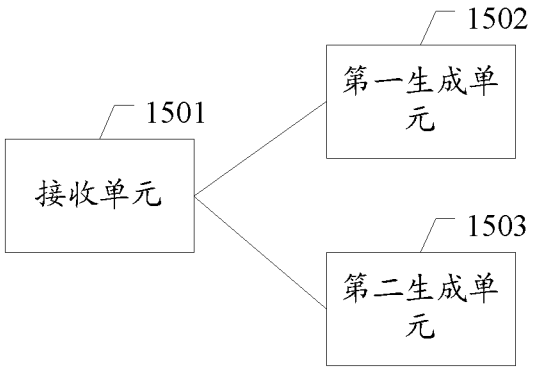
1502
第一生成单元
1501
接收单元
1503
第二生成单元

图 15

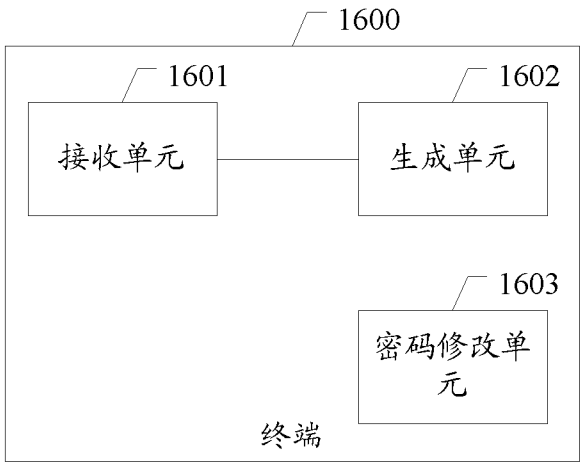
1600
1601
接收单元
1602
生成单元
1603
密码修改单元
终端

图 16

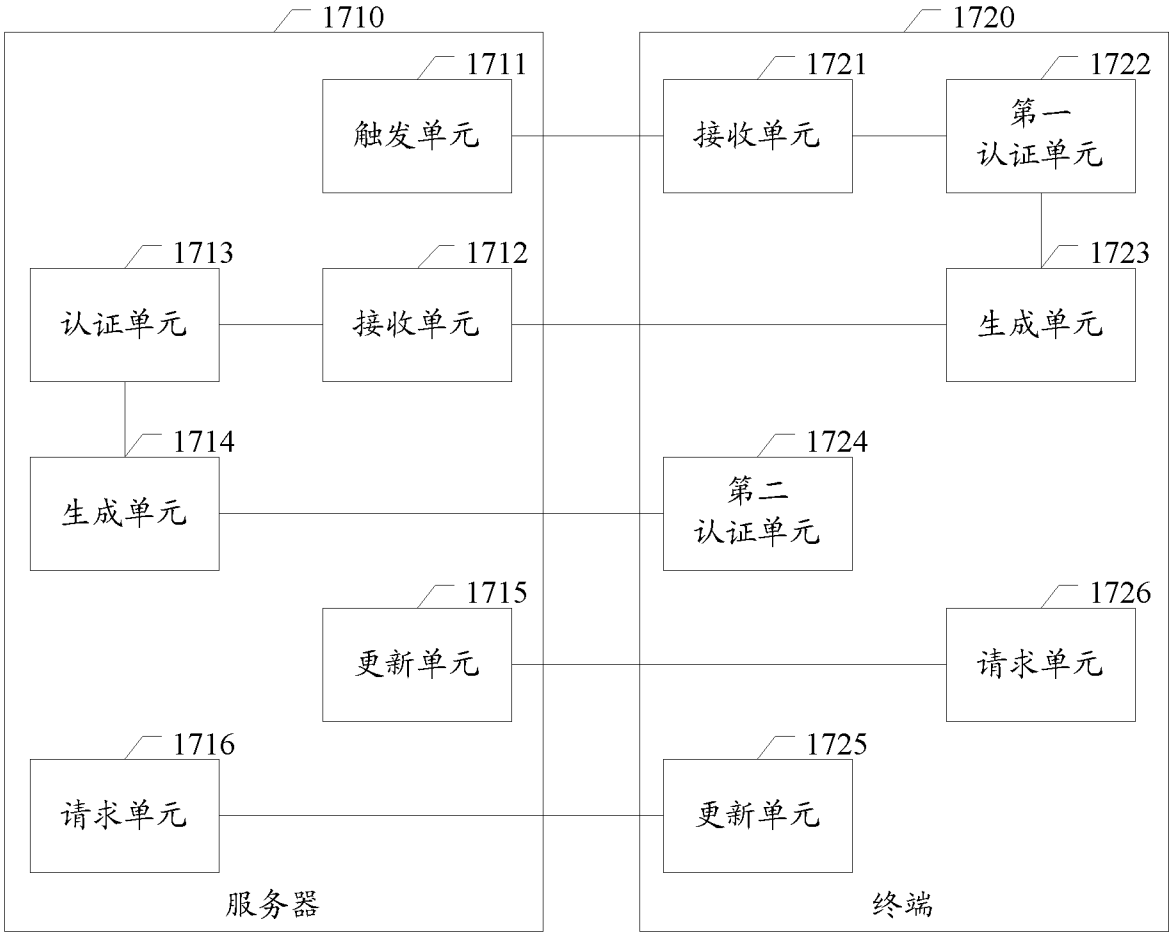
1710
1711
触发单元
1713
认证单元
1712
接收单元
1714
生成单元
1715
更新单元
1716
请求单元
服务器
1720
1721
接收单元
1722
第一
认证单元
1723
生成单元
1724
第二
认证单元
1726
请求单元
1725
更新单元
终端

图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2008/070686

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

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: H04L, H04Q, G06F

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)

WPI, EPODOC, PAJ, CNPAT, CNKI: server, trigger, random w number, nonce, authenticat+, verify+, valid+, digest, DS, DM, session, default, safe, attack+, security, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1476709A (GEN INSTR CORP) 18 Feb. 2004 (18.02.2004) whole document	1-36
A	WANG Xiaojun, LU Jiande, Attack on 4-way Handshake of 802.11i, Computer and Modernization, May 2006 (05.2006), year 2006 No.5, pages 72-75, ISSN 1006-2475	1-36
A	SHI Tingjun, MA Jianfeng, Design and analysis of a wireless authentication protocol against DoS attacks based on Hash function, System Engineering and Electronics, Jan. 2006 (01.2006), Vol.28 No.1, pages 122-126, ISSN 1001-506X	1-36
A	US2004111615A1 (CHUNG B H et al) 10 Jun. 2004 (10.06.2004) whole document	1-36
A	US2003115464 A1 (CHUNG B H et al) 19 Jun. 2003 (19.06.2003) whole document	1-36
A	US6058480A (CRANBERRY PROPERTIES LLC) 02 May 2000 (02.05.2000) Whole document	1-36
A	JP2005005778A (ZH SEISAN GIJUTSU KENKYU SHOREIKAI) 06 Jan. 2005 (06.01.205) whole document	1-36

☐ 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
06 Aug. 2008 (06.08.2008)	**21 Aug. 2008 (21.08.2008)**
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 ZHANG Xin Telephone No. (86-10)62411280

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2008/070686

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

This international application includes the following 4 inventions:
1. Claims 1, 24, 25, 30 relate to the method and apparatus for processing authentication using a trigger message random number;
2. Claims 12, 13, 15, 35 relate to the method for processing authentication using a default random number;
3. Claim 20 relates to the method for processing authentication using a common random number;
4. Claims 9, 34 relate to the method and terminal for requesting to update the server random number.

However, the above 4 inventions don't have the same or corresponding special features, and don't belong to a total invention conception, so they are lack of unity of invention, and don't comply with PCT Rule13.1, 13.2 and 13.3.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2008/070686

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1476709A	18.02.2004	WO0225899A1	28.03.2002
		AU9295501A	02.04.2002
		EP1320975A1	25.06.2003
		JP2004509567T	25.03.2004
		KR20040014400A	14.02.2004
		EP1320975 B1	07.12.2005
		DE60115672E	12.01.2006
		DE60115672T2	20.07.2006
		CN1285202C	15.11.2006
		CA2421628 A	28.03.2002
		US6892308B	10.05.2005
		US2005120248A	02.06.2005
		AT312464T	15.12.2005
US2004111615A1	10.06.2004	CA2444423A1	10.06.2004
		KR20040050625A	16.06.2004
US2003115464A1	19.06.2003	CA2388906A1	19.06.2003
		KR20030050620A	25.06.2003
		KR100445574B	25.08.2004
		CA2388906C	13.03.2007
US6058480A	02.05.2000	US5740361A	14.04.1998
		US6487667B	26.11.2002
JP2005005778A	06.01.2005	NONE	

国际检索报告

国际申请号
PCT/CN2008/070686

A. 主题的分类

H04L 9/32 (2006.01) i

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: H04L, H04Q, G06F

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））

WPI, EPODOC, PAJ: server, trigger, random w number, nonce, authenticat+, verify+, valid+, digest, DS, DM, session, default, safe, attack+, security, key CNPAT,CNKI: 服务器 触发消息 随机数 现时 认证 验证 鉴权 摘要 数据同步 协议管理 会话 缺省 安全 攻击 密钥

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	CN1476709A (通用器材公司) 18. 2 月 2004 (18.02.2004) 全文	1-36
A	王小军、陆建德，基于 802.11i 的四次握手协议的攻击，计算机与现代化，5 月 2006 (05.2006)，2006 年第 5 期，72-75 页，ISSN 1006-2475	1-36
A	史庭俊、马建峰，基于 Hash 函数的抗攻击无线认证方案，系统工程与电子技术，1 月 2006 (01.2006)，第 28 卷第 1 期，122-126 页，ISSN 1001-506X	1-36
A	US2004111615A1 (CHUNG B H et al) 10. 6 月 2004 (10.06.2004) 全文	1-36
A	US2003115464 A1 (CHUNG B H et al) 19. 6 月 2003 (19.06.2003) 全文	1-36
A	US6058480A (CRANBERRY PROPERTIES LLC) 02. 5 月 2000 (02.05.2000) 全文	1-36
A	JP2005005778A (ZH SEISAN GIJUTSU KENKYU SHOREIKAI) 06. 1 月 2005 (06.01.2005) 全文	1-36

☐ 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
06. 8 月 2008 (06.08.2008)	**21.8 月 2008 (21.08.2008)**
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 张鑫 电话号码：(86-10) **62411280**

国际检索报告

国际申请号
PCT/CN2008/070686

第II栏　关于某些权利要求不能作为检索主题的意见(接第 1 页第 2 项)

按条约 17(2)(a)对某些权利要求未作国际检索报告的理由如下：

1. ☐ 权利要求：

因为它们涉及到不要求本国际检索单位进行检索的主题，即：

2. ☐ 权利要求：

因为它们涉及到国际申请中不符合规定的要求的部分，以致不能进行任何有意义的国际检索，

具体地说：

3. ☐ 权利要求：

因为它们是从属权利要求，并且没有按照细则 6.4(a)第 2 句和第 3 句的要求撰写。

第III栏　关于缺乏发明单一性时的意见(接第 1 页第 3 项)

本国际检索单位在该国际申请中发现多项发明，即：
本国际申请包括下列 4 项发明：
1、独立权利要求 1、24、25、30 涉及使用触发消息随机数进行认证的方法和装置；
2、独立权利要求 12、13、15、35 涉及使用缺省随机数进行认证的方法；
3、独立权利要求 20 涉及使用共用随机数进行认证的方法；
4、独立权利要求 9、34 涉及请求更新服务器随机数的方法和终端。

以上 4 项发明不具有相同或相应的特定技术特征，不属于一个总的发明构思，因而不具备单一性，不符合专利合作条约实施细则 13.1、13.2 和 13.3 的规定。

1. ☒ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告针对全部可作检索的权利要求。

2. ☐ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本国际检索单位未通知缴纳任何附加费。

3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求。
具体地说，是权利要求：

4. ☐ 申请人未按时缴纳被要求的附加检索费。因此，本国际检索报告仅涉及权利要求中首次提及的发明；
包含该发明的权利要求是：

关于异议的说明：☐ 申请人缴纳了附加检索费，同时提交了异议书，缴纳了异议费。

☐ 申请人缴纳了附加检索费，同时提交了异议书，但未缴纳异议费。

☒ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2008/070686

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1476709A	18.02.2004	WO0225899A1	28.03.2002
		AU9295501A	02.04.2002
		EP1320975A1	25.06.2003
		JP2004509567T	25.03.2004
		KR20040014400A	14.02.2004
		EP1320975 B1	07.12.2005
		DE60115672E	12.01.2006
		DE60115672T2	20.07.2006
		CN1285202C	15.11.2006
		CA2421628 A	28.03.2002
		US6892308B	10.05.2005
		US2005120248A	02.06.2005
		AT312464T	15.12.2005
US2004111615A1	10.06.2004	CA2444423A1	10.06.2004
		KR20040050625A	16.06.2004
US2003115464A1	19.06.2003	CA2388906A1	19.06.2003
		KR20030050620A	25.06.2003
		KR100445574B	25.08.2004
		CA2388906C	13.03.2007
US6058480A	02.05.2000	US5740361A	14.04.1998
		US6487667B	26.11.2002
JP2005005778A	06.01.2005	无	