[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/28

[12] 发明专利申请公开说明书

[21] 申请号 200410069176.9

[43] 公开日 2005 年 7 月 27 日

[11] 公开号 CN 1645826A

[22] 申请日 2004.7.5
[21] 申请号 200410069176.9
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 张文林

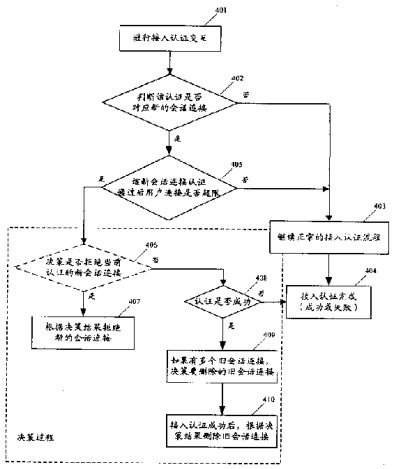
[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 张颖玲 王 琦

权利要求书 3 页 说明书 21 页 附图 7 页

[54] 发明名称 无线局域网用户建立会话连接的方法

[57] 摘要

本发明公开了一种无线局域网用户建立会话连接的方法，该方法包括：a. 对用户进行接入认证的 AAA 服务器判断本次认证是否对应新的会话连接，如果不是，则结束当前处理流程；否则执行步骤 b；b. 所述 AAA 服务器根据网络配置规则和/或用户签约信息，判断增加当前新会话连接后是否超出网络对当前用户的会话连接限制，如果不是，则结束当前处理流程；如果是，则确定需要删除的会话连接。采用该方法能避免同一 WLAN 用户从多个 AAA 服务器接入认证，从而保证用户数据不分散，且实现简单、方便、灵活。



ISSN1008-4274

1、一种无线局域网用户建立会话连接的方法，其特征在于，该方法包括：

a. 对用户进行接入认证的 AAA 服务器判断本次认证是否对应新的会话连接，如果不是，则结束当前处理流程；否则执行步骤 b；

b. 所述 AAA 服务器根据网络配置规则和/或用户签约信息，判断增加当前新会话连接后是否超出网络对当前用户的会话连接限制，如果不是，则结束当前处理流程；如果是，则确定需要删除的会话连接。

2、根据权利要求 1 所述的方法，其特征在于，步骤 a 所述判断具体是：判断当前认证过程中携带给所述 AAA 服务器的用户设备 MAC 地址、或 WLAN 接入网标识信息、或 VPLMN 标识信息是否与已有会话连接不同。

3、根据权利要求 1 或 2 所述的方法，其特征在于，网络只允许同一用户建立一个会话连接时，步骤 b 中所述确定需要删除的会话连接为：确定删除已有的会话连接。

4、根据权利要求 1 或 2 所述的方法，其特征在于，网络只允许同一用户建立一个会话连接时，步骤 b 中所述确定需要删除的会话连接进一步包括：网络判断当前已有的会话连接是否还存在，如果存在，则拒绝本次认证对应的新会话建立请求；否则，删除已有的会话连接，允许新的会话连接接入。

5、根据权利要求 4 所述的方法，其特征在于，该方法进一步包括：拒绝本次认证对应的新会话建立请求的同时，向用户返回新连接超出限制的失败原因。

6、根据权利要求 4 所述的方法，其特征在于，所述判断当前已有会话连接是否存在进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令。

7、根据权利要求 1 或 2 所述的方法，其特征在于，网络只允许同一用户建立一个会话连接时，步骤 b 中所述确定需要删除的会话连接为：网络判断当前已有的会话连接是否还存在，如果不存在，删除已有的会话连接，允许新的会话连接接入；如果存在，则再根据会话连接的标识信息比较会话连接的接入优

先级，判断是否已有会话连接的优先级低，如果是，则删除已有的会话连接；如果不是，则拒绝本次认证对应的新会话建立请求。

8、根据权利要求 7 所述的方法，其特征在于，所述判断当前已有会话连接是否存在进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令。

9、根据权利要求 1 或 2 所述的方法，其特征在于，网络允许同一用户建立一个以上会话连接时，步骤 b 中所述确定需要删除的会话连接为：删除已有会话连接中当前没有响应的或未响应时间最长的一个会话连接。

10、根据权利要求 9 所述的方法，其特征在于，该方法进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令，确认已有会话连接是否有响应。

11、根据权利要求 1 或 2 所述的方法，其特征在于，网络允许同一用户建立一个以上会话连接，且当前发起认证的会话建立请求中携带有删除会话标识，则步骤 b 中所述确定需要删除的会话连接为：根据会话建立请求中携带的删除会话标识删除已有会话连接。

12、根据权利要求 11 所述的方法，其特征在于，所述删除会话标识已指出要删除的会话连接，则根据删除会话标识删除指定的已有会话连接。

13、根据权利要求 11 所述的方法，其特征在于，该方法进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令，确认已有会话连接是否有响应，删除当前没有响应的或未响应时间最长的一个会话连接。

14、根据权利要求 1 或 2 所述的方法，其特征在于，网络允许同一用户建立一个以上会话连接时，步骤 b 中所述确定需要删除的会话连接为：网络根据用户配置命令确定要删除的会话连接。

15、根据权利要求 1 或 2 所述的方法，其特征在于，网络允许同一用户建立一个以上会话连接时，步骤 b 中所述确定需要删除的会话连接为：网络判断

当前已有的所有会话连接是否还存在，如果有会话连接不存在，删除当前已不存在的会话连接，允许新的会话连接接入；如果所有会话连接都存在，则拒绝本次认证对应的新会话建立请求。

16、根据权利要求 15 所述的方法，其特征在于，所述判断当前已有会话连接是否存在进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令。

17、根据权利要求 1 或 2 所述的方法，其特征在于，网络允许同一用户建立一个以上会话连接时，步骤 b 中所述确定需要删除的会话连接为：先对新的会话建立请求进行认证，在新的会话建立请求认证成功后，删除已有会话连接中接入优先级最低的会话连接。

18、根据权利要求 1 或 2 所述的方法，其特征在于，网络允许同一用户建立一个以上会话连接时，步骤 b 中所述确定需要删除的会话连接为：网络判断当前已有的所有会话连接是否还存在，如果有会话连接不存在，删除当前已不存在的会话连接，允许新的会话连接接入；如果所有会话连接都存在，则根据用户会话标识信息中的属性信息确定要删除的会话连接。

19、根据权利要求 18 所述的方法，其特征在于，所述用户会话标识信息中的属性信息为：会话连接的接入优先级。

20、根据权利要求 1 或 2 所述的方法，其特征在于，步骤 b 中所述确定需要删除的会话连接为：根据用户签约定制的超限删除策略确定要删除的会话连接。

21、根据权利要求 1 或 2 所述的方法，其特征在于，步骤 b 中确定删除已有会话连接，则在新的会话建立请求认证成功后，完成已有会话连接的删除；或者，步骤 b 中确定拒绝新的会话建立请求，则在认证完成前或认证过程中对新的会话建立请求进行拒绝。

无线局域网用户建立会话连接的方法

技术领域

本发明涉及无线局域网（WLAN）中连接建立技术，尤指一种在 WLAN 中限制 WLAN 用户建立多个会话连接的方法。

背景技术

由于用户对无线接入速率的要求越来越高，无线局域网（WLAN，Wireless Local Area Network）应运而生，它能在较小范围内提供高速的无线数据接入。无线局域网包括多种不同技术，目前应用较为广泛的一个技术标准是 IEEE 802.11b，它采用 2.4GHz 频段，最高数据传输速率可达 11Mbps，使用该频段的还有 IEEE 802.11g 和蓝牙（Bluetooth）技术，其中，802.11g 最高数据传输速率可达 54Mbps。其它新技术诸如 IEEE 802.11a 和 ETSI BRAN Hiperlan2 都使用 5GHz 频段，最高传输速率也可达到 54Mbps。

尽管有多种不同的无线接入技术，大部分 WLAN 都用来传输因特网协议（IP）分组数据包。对于一个无线 IP 网络，其采用的具体 WLAN 接入技术对于上层的 IP 一般是透明的。其基本的结构都是利用接入点（AP）完成用户终端的无线接入，通过网络控制和连接设备连接组成 IP 传输网络。

随着 WLAN 技术的兴起和发展，WLAN 与各种无线移动通信网，诸如：GSM、码分多址（CDMA）系统、宽带码分多址（WCDMA）系统、时分双工-同步码分多址（TD-SCDMA）系统、CDMA2000 系统的互通正成为当前研究的重点。在第三代合作伙伴计划（3GPP）标准化组织中，用户终端可以通过 WLAN 的接入网络与因特网（Internet）、企业内部互联网（Intranet）相连，还可以经由 WLAN 接入网络与 3GPP 系统的归属网络或 3GPP 系统的访问网络连接，具体地说就是，WLAN 用户终端在本地接入时，经由 WLAN 接入网络与

3GPP 的归属网络相连，如图 2 所示；在漫游时，经由 WLAN 接入网络与 3GPP 的访问网络相连，3GPP 访问网络中的部分实体分别与 3GPP 归属网络中的相应实体互连，比如：3GPP 访问网络中的 3GPP 认证授权计费（AAA）代理和 3GPP 归属网络中的 3GPP 认证授权计费（AAA）服务器；3GPP 访问网络中的无线局域网接入关口（WAG）与 3GPP 归属网络中的分组数据关口（PDG，Packet Data Gateway）等等，如图 1 所示。其中，图 1、图 2 分别为漫游情况下和非漫游情况下 WLAN 系统与 3GPP 系统互通的组网结构示意图。

参见图 1、图 2 所示，在 3GPP 系统中，主要包括归属签约用户服务器（HSS）/归属位置寄存器（HLR）、3GPP AAA 服务器、3GPP AAA 代理、WAG、分组数据关口、计费关口（CGw）/计费信息收集系统（CCF）及在线计费系统（OCS）。用户终端、WLAN 接入网络与 3GPP 系统的所有实体共同构成了 3GPP-WLAN 交互网络，此 3GPP-WLAN 交互网络可作为一种无线局域网服务系统。其中，3GPP AAA 服务器负责对用户的鉴权、授权和计费，对 WLAN 接入网络送来的计费信息收集并传送给计费系统；分组数据关口负责将用户数据从 WLAN 接入网络到 3GPP 网络或其他分组网络的数据传输；计费系统主要接收和记录网络传来的用户计费信息，还包括 OCS 根据在线计费用户的费用情况指示网络周期性的传送在线费用信息，并进行统计和控制。

在非漫游情况下，当 WLAN 用户终端希望直接接入 Internet/Intranet 时，用户终端通过 WLAN 接入网与 AAA 服务器（AS）完成接入认证授权后，用户终端可通过 WLAN 接入网接入到 Internet/Intranet。如果 WLAN 用户终端还希望接入 3GPP 分组交换（PS）域业务，则可进一步向 3GPP 归属网络申请互通场景 3（Scenario3）的业务，即：WLAN 用户终端向 3GPP 归属网络的 AS 发起互通场景 3 的业务授权请求，3GPP 归属网络的 AS 对该业务授权请求进行业务鉴权和授权，如果成功，则 AS 给用户终端发送接入允许消息，且 AS 给用户终端分配相应的 PDG，用户终端与所分配的 PDG 之间建立隧道后，即可接入 3GPP PS 域业务。同时，CGw/CCF 和 OCS 根据用户终端的网络使用情况记录计费信

息。在漫游情况下，当 WLAN 用户终端希望直接接入 Internet/Intranet 时，用户终端可通过 3GPP 访问网络向 3GPP 归属网络申请接入到 Internet/Intranet。如果用户终端还希望申请互通场景 3 业务，接入到 3GPP PS 域业务，则用户终端需要通过 3GPP 访问网络向 3GPP 归属网络发起业务授权过程，该过程同样在用户终端和 3GPP 归属网络的 AS 之间进行，当授权成功后，AS 给用户终端分配相应的归属 PDG，用户终端通过 3GPP 访问网络中的 WAG 与分配的 PDG 之间建立隧道后，用户终端即可接入归属网络的 3GPP PS 域业务。

根据 3GPP 协议规定，在现有 3GPP-WLAN 交互网络中，WLAN 用户接入网络的鉴权和授权过程如图 3 所示，包括以下步骤：

步骤 301~302：当前 WLAN 用户终端与 WLAN 接入网根据 3GPP 协议规定的流程建立无线连接；之后，发起当前 WLAN 用户终端与 3GPP AAA 服务器之间的接入认证过程，该接入认证通过可扩展认证协议（EAP）进行，即：在当前 WLAN 用户终端与 3GPP AAA 服务器之间进行 EAP 请求和 EAP 响应消息的交互。

步骤 303~304：3GPP AAA 服务器收到接入认证请求后，判断自身是否存在针对当前 WLAN 用户终端的鉴权信息，如果不存在，则从 HSS 中获取当前 WLAN 用户终端的鉴权信息，比如：鉴权五元组/三元组。并且，如果该 3GPP AAA 服务器中不存在当前 WLAN 用户终端的用户签约信息，比如：授权信息、用户临时标识，同样要从 HSS 中获取。也就是说，3GPP AAA 服务器自身没有用户信息的话，就需要从 HSS 中获取。

步骤 305：3GPP AAA 服务器可以将策略执行信息发送给当前 WLAN 用户终端漫游到的访问公众陆地移动网络（VPLMN）中的 WAG，本步骤是可选的。

步骤 306：如果鉴权和授权成功，则 3GPP AAA 服务器向 WLAN 接入网发送允许接入消息 Access Accept，在该消息中包括 EAP 成功消息 EAP Success，该成功消息中携带有连接授权信息，比如：接入过滤规则、隧道属性等等。

步骤 307：WLAN 接入网收到允许接入消息后，向当前 WLAN 用户终端发

送鉴权成功消息 EAP Success。

步骤 308: 如果当前 WLAN 用户终端在 HSS 中没有当前为其提供接入认证 3GPP AAA 服务器的登记信息，则为当前 WLAN 用户终端提供鉴权的 3GPP AAA 服务器在 HSS 中进行登记，登记消息中根据用户的临时标识来确定用户。

从上述流程可以看出，当前的规范和过程还没有涉及归属网络中有多个 AAA 服务器提供服务时，如果用户已经连接到一个 AAA 服务器，下次发起认证时如何保障继续连接到该 AAA 的解决方案。那么，当一个归属公众陆地移动网络（HPLMN）网络中有多个 AAA 服务器能够为 WLAN 用户提供服务时，某用户第一次接入 AAA 服务器 1 之后，下次进行认证或接入可能被送入 AAA 服务器 2，而该 AAA 服务器 2 会重新与 HSS 进行交互，从 HSS 中请求用户的签约数据。如此，就会对同一个用户建立多个会话连接，不仅导致用户数据分散，不能集中管理；而且会占用大量的系统资源。

虽然目前业界也提出一种限制同一用户建立多会话进程的方案，但该方案的具体实现需要 HSS 进行多重条件的判断，经过的过程较为复杂繁琐，而且也在一定程度上加大了 HSS 的负荷。

发明内容

有鉴于此，本发明的主要目的在于提供一种 WLAN 用户建立会话连接的方法，能够避免同一 WLAN 用户建立多个会话连接，从而保证用户数据不分散，且实现简单、方便、灵活。

为达到上述目的，本发明的技术方案是这样实现的：

一种无线局域网用户建立会话连接的方法，该方法包括：

a. 对用户进行接入认证的 AAA 服务器判断本次认证是否对应新的会话连接，如果不是，则结束当前处理流程；否则执行步骤 b；

b. 所述 AAA 服务器根据网络配置规则和/或用户签约信息，判断增加当前新会话连接后是否超出网络对当前用户的会话连接限制，如果不是，则结束当前处理流程；如果是，则确定需要删除的会话连接。

其中，步骤 a 所述判断具体是：判断当前认证过程中携带给所述 AAA 服务器的用户设备 MAC 地址、或 WLAN 接入网标识信息、或 VPLMN 标识信息是否与已有会话连接不同。

当网络只允许同一用户建立一个会话连接时，步骤 b 中所述确定需要删除的会话连接为：确定删除已有的会话连接。

或者，步骤 b 中所述确定需要删除的会话连接进一步包括：网络判断当前已有的会话连接是否还存在，如果存在，则拒绝本次认证对应的新会话建立请求；否则，删除已有的会话连接，允许新的会话连接接入。此时，该方法进一步包括：拒绝本次认证对应的新会话建立请求的同时，向用户返回新连接超出限制的失败原因。所述判断当前已有会话连接是否存在进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令。

或者，步骤 b 中所述确定需要删除的会话连接为：网络判断当前已有的会话连接是否还存在，如果不存在，删除已有的会话连接，允许新的会话连接接入；如果存在，则再根据会话连接的标识信息比较会话连接的接入优先级，判断是否已有会话连接的优先级低，如果是，则删除已有的会话连接；如果不是，则拒绝本次认证对应的新会话建立请求。其中，所述判断当前已有会话连接是否存在进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令。

或者，步骤 b 中所述确定需要删除的会话连接为：删除已有会话连接中当前没有响应的或未响应时间最长的一个会话连接。此时，该方法进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令，确认已有会话连接是否有响应。

当网络允许同一用户建立一个以上会话连接，且当前发起认证的会话建立请求中携带有删除会话标识，则步骤 b 中所述确定需要删除的会话连接为：根据会话建立请求中携带的删除会话标识删除已有会话连接。其中，所述删除会

话标识已指出要删除的会话连接，则根据删除会话标识删除指定的已有会话连接。此时，该方法进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令，确认已有会话连接是否有响应，删除当前没有响应的或未响应时间最长的一个会话连接。

当网络允许同一用户建立一个以上会话连接时，步骤 b 中所述确定需要删除的会话连接为：网络根据用户配置命令确定要删除的会话连接。

或者，步骤 b 中所述确定需要删除的会话连接为：网络判断当前已有的所有会话连接是否还存在，如果有会话连接不存在，删除当前已不存在的会话连接，允许新的会话连接接入；如果所有会话连接都存在，则拒绝本次认证对应的新会话建立请求。其中，所述判断当前已有会话连接是否存在进一步包括：所述 AAA 服务器向已有会话连接发起重认证过程，或是发送要求用户终端返回响应的测试信令。

或者，步骤 b 中所述确定需要删除的会话连接为：先对新的会话建立请求进行认证，在新的会话建立请求认证成功后，删除已有会话连接中接入优先级最低的会话连接。

或者，步骤 b 中所述确定需要删除的会话连接为：网络判断当前已有的所有会话连接是否还存在，如果有会话连接不存在，删除当前已不存在的会话连接，允许新的会话连接接入；如果所有会话连接都存在，则根据用户会话标识信息中的属性信息确定要删除的会话连接。其中，所述用户会话标识信息中的属性信息为：会话连接的接入优先级。

步骤 b 中所述确定需要删除的会话连接还可以是：根据用户签约定制的超限删除策略确定要删除的会话连接。

上述方案中，步骤 b 中确定删除已有会话连接，则在新的会话建立请求认证成功后，完成已有会话连接的删除；或者，步骤 b 中确定拒绝新的会话建立请求，则在认证完成前或认证过程中对新的会话建立请求进行拒绝。

本发明所提供的 WLAN 用户建立会话连接的方法，如果 AAA 服务器在进

行接入认证时发现：当前认证对应的会话连接是与现有会话连接不同的新的会话连接，则 AAA 服务器在允许的范围内进行正常的接入认证过程，如果是超出允许范围，则 AAA 服务器确定需要拒绝或取消的会话连接，然后根据决策结果完成后续的会话连接拒绝或取消流程。如此，可保证每个用户仅由一个 AAA 服务器为其提供服务，以避免用户数据的分散和系统资源的浪费，保证数据的集中管理。

本发明的方法 AAA 服务器只需对当前认证请求中携带的用户信息或网络信息判断是否与自身存储的相应信息相同，即可确定是否为同一用户建立多个不同的会话连接，实现简单、方便，既不会增加 HSS 的负荷，也不会使接入认证流程复杂化。并且，本发明可采用不同的方案达到避免同一 WLAN 用户终端建立多个 WLAN 会话连接的目的，实现更灵活。

附图说明

图 1 为 WLAN 系统与 3GPP 系统互通的网络结构示意图；

图 2 为 WLAN 运营网络的一种组网结构示意图；

图 3 为现有技术中 WLAN 用户终端进行鉴权和授权的流程图；

图 4 为本发明第一实施例的处理流程图；

图 5 为本发明第二实施例的处理流程图；

图 6 为本发明第五实施例的处理流程图；

图 7 为本发明第六实施例的处理流程图。

具体实施方式

本发明的核心思想是：在 WLAN 用户终端接入认证交互过程中，AAA 服务器判断该认证是否对应一个新会话连接，如果是新会话则需要进一步判断增加新的会话是否超出网络对用户会话连接的限制，如果超出，则需要决策删除某个旧的会话连接或是拒绝新会话的建立请求。如果确定拒绝新会话建立请求，则该拒绝操作可以在认证前或认证过程中进行；如果确定删除旧会话连接，则

删除过程要在新会话连接认证通过后进行。如此，可保证仅有一个 AAA 服务器为每个 WLAN 用户终端提供接入认证服务。

这里，所述 AAA 服务器判断当前认证过程是否对应一个新会话连接，是 AAA 服务器根据 WLAN 用户认证过程中，携带给 AAA 服务器的用户设备 MAC 地址、或 WLAN 接入网标识信息、或 VPLMN 标识信息来判断当前会话连接是否与已有会话连接不同。在认证中，这些信息中的任何一个信息不同，都表明对应的会话连接不同。这些信息可以是由用户终端主动通过认证信令携带上来，也可以是 AAA 服务器通过与用户终端一次或多次的交互获得的。所述决策要删除会话连接还是拒绝新会话建立请求，可以根据需要启动一个决策交互流程，其中，确定要删除的会话连接是从旧会话连接中选择的。

所述判断增加新的会话是否超出网络对用户的会话连接限制，主要是根据网络配置和/或决策规则来确定的。决策规则根据网络配置或用户签约信息可分为三种情况：

第一种情况，网络不允许用户建立多连接、或根据该用户的签约不允许其多连接，也就是说，只允许用户存在一个连接。此种情况下，决策规则有三种：① 要删除的会话连接就是旧的会话连接；② 网络先与旧会话连接交互，验证其是否还存在，如果存在，则拒绝新的连接，并提示用户失败原因为新连接超出限制；③ 网络先与旧会话连接交互，验证其是否还存在，如果存在，再根据会话连接的标识信息，比较当前请求的新会话连接的接入优先级与旧会话连接的接入优先级，拒绝接入优先级低的会话连接，比如：如果当前请求的新会话连接接入优先级低，则拒绝该新会话建立请求。

第二种情况，网络允许用户建立多连接，此种情况下，决策规则有以下几种：① 要删除的会话连接是旧会话连接中的一个，优先拆除没有响应或未响应时间最长的会话连接。在决策过程中，可以对旧连接进行活性确认，以确认当前会话是否存在，所谓活性是指某个会话是否处于激活状态，所谓确认就是：对超过一定时限没有进行动态交互的会话发起确认，比如发起重认证过程，可

以是快速重认证，或简单的信令交互来表明对方还存在。② 用户发起新的会话认证时，直接携带要删除的会话的标识， 此时网络根据该标识删除旧会话。这里，可以直接标识出要删除的某个会话连接；也可以是只标识要删除旧会话，AAA 服务器再根据活性确认或优先级比较进行选择。③ 网络与用户发起信令交互，要求用户决定一个要删除的会话连接，该交互中可以要求对选择权限设置密码或其他认证措施，保障用户有删除其他会话连接的权限。④ 网络先与旧连接交互，验证其是否还存在，如果旧的会话连接中有已经不存在的，则删除已经不存在的会话连接，接入新的会话连接；如果旧的会话连接都存在，则拒绝新会话建立请求，并提示用户失败原因为新连接超出限制。⑤ 先对新会话连接进行认证，新会话连接认证成功后，对现有旧会话连接中优先级最低的进行删除。⑥ 网络先与旧连接交互，验证其是否还存在，如果旧的会话连接中有已经不存在的，则删除已经不存在的连接，接入新的会话连接；如果旧的会话连接都存在，则进一步根据用户会话标识信息中的属性决策要删除的会话，比如：新会话连接的 VPLMN2 和旧会话连接的 VPLMN1 相比优先权低，则拒绝新会话建立请求，反之，在新会话连接认证成功后，删除旧会话连接中优先权最低的会话连接。

第三种情况，用户签约选择定制超限删除策略，比如：如果旧会话连接都是激活的，则拒绝新会话连接；或是根据活性、会话连接时间等参数选择删除旧会话连接；或根据设置的参数判断会话连接优先级进行选择。

以上所述方案主要适用于：网络能够确保对一个 WLAN 用户而言，只有一个 AAA 服务器为其提供接入认证授权服务，则 AAA 服务器来完成对多个会话连接认证的判断处理。

实施例一：

本实施例为一个增强功能的 AAA 服务器中的判断逻辑，也就是说，在 AAA 服务器中增加对于同一用户是否存在多个会话连接的判断，以确保仅有一个 AAA 服务器为当前用户提供服务。本实施例中，先判断是否删除新的会话连接，

再决定是否对新会话连接进行认证。

如图 4 所示，本实施例中 AAA 服务器的判断流程包括以下步骤：

步骤 401~404：在 WLAN 用户终端的接入认证交互过程中，对当前发起认证请求用户进行接入认证的 AAA 服务器判断当前请求的认证是否对应一个新会话连接，如果不是，则继续正常的认证流程，结束当前判断流程，并且，在接入认证完成后向发起认证请求的用户终端返回成功或失败的结果；如果是新会话连接，则执行步骤 405；

步骤 405：AAA 服务器根据网络配置规则或/和用户签约信息，判断如果新会话连接认证通过后，该发起认证的用户的会话连接是否超出网络对用户的会话连接限制，如果没有超出，则结束当前处理流程，继续正常的认证过程，即执行步骤 403~404；如果超出，则启动一个决策交互过程，即执行步骤 406~410；

步骤 406~410：决策是否拒绝当前认证的新会话连接，如果是，则根据决策结果拒绝新会话建立请求，结束当前处理；否则，判断认证是否成功，如果认证不成功，则向用户返回接入认证失败的结果，结束当前处理流程；如果认证成功，则确定要删除的旧会话连接：如果有多个旧会话连接，则决策一下要删除的会话连接，然后在新会话连接认证成功后，根据决策结果删除选定的旧会话连接。步骤 406 和步骤 409 中所提到的决策，具体过程和规则是这样的：

首先对旧连接发起重认证过程，可以是快速重认证，也可以是一个简单的测试信令要求用户终端响应，如果该认证成功或测试信令得到响应，则表明旧会话连接是激活的，否则，表明旧会话连接已经消失，需要通过删除流程清除其残余信息。

如果决策结果是有至少一个旧会话连接已清除，则新会话连接的认证继续顺利完成；如果决策结果是现有的旧连接都处于激活状态，则根据按会话识别参数设置的优先级参考数据来判断新会话连接和所有旧会话连接的优先级，选出优先级最低的会话连接，如果选出的是新认证的会话连接，则拒绝该认证，即拒绝新的会话建立请求；如果选出的是一个旧会话连接，则在新会话连接认

证成功后，发起对该选出的旧会话连接的删除流程。这里，所述的会话识别参数为：VPLMN 标识、WLAN 接入网标识信息、用户 MAC 地址等。

实施例二：

本实施例为另一个增强功能的 AAA 服务器中的判断逻辑，也就是说，在 AAA 服务器中增加对于同一用户是否存在多个会话连接的判断，以确保仅有一个 AAA 服务器为当前用户提供服务。本实施例中，决策删除某个旧会话连接，所以直接对新会话连接进行认证。

如图 5 所示，本实施例中 AAA 服务器的判断流程包括以下步骤：

步骤 501~504：与实施例一的描述完全相同。

步骤 505~508：判断如果新会话连接认证通过后，用户连接是否超出网络对用户的会话连接限制，如果没有超出，则不作特殊处理，继续正常认证流程，即执行步骤 503~504；如果超出，则在新会话连接认证成功后，如果只有一个现有会话连接，则删除该现有会话连接，接入新的会话连接，否则启动一个决策交互过程，对旧会话连接进行优先级判断：根据按会话识别参数设置的优先级参考数据判断新会话连接与所有旧会话连接的优先级，选出优先级最低的会话连接，发起对该选出的旧会话连接的删除。这里，所述的会话识别参数为：VPLMN 标识、WLAN 接入网标识信息、用户 MAC 地址等。

实施例三：

本实施例是基于图 3 所示的处理流程，将图 3 给出的交互流程与本发明核心思想的处理步骤相结合，主要涉及步骤 302、303 和 304 的变化，其它步骤基本不变。本实施例中，步骤 302 的主要修改是：

在认证交互过程中，增加 AAA 服务器对当前认证是否对应新会话连接的判断，如果是新会话连接，则需要再判断增加新的会话连接后是否超出网络对用户的会话连接限制，如果超出，则需要决策一个要删除的会话连接或拒绝新的会话建立请求。如果需要拒绝新的会话建立请求，则该拒绝可以在认证前或认证过程中进行；如果需要删除旧的会话连接，则该删除应该在对新会话连接

认证通过后进行。步骤 302 实际就是一个决策过程，具体的决策交互过程与实施例一中步骤 406~410 的描述完全相同。

对步骤 303 和 304 的主要修改是：通过 AAA 服务器与 HSS 之间的交互，保障仅有一个 AAA 服务器为同一用户提供服务，也就是说，防止同一个用户同时与多个 AAA 服务器建立联系，避免同一用户从多个 AAA 服务器接入认证。

具体来说，在步骤 303 中，增加 HSS 对当前要获取用户信息的 AAA 服务器的判断：HSS 收到 AAA 服务器发来的签约信息请求后，检查自身是否有该 WLAN 用户的 AAA 登记，如果不存在，则继续原有正常流程；如果存在，再根据 AAA 标识判断登记的 AAA 服务器与当前发请求的 AAA 服务器是否为同一个 AAA 服务器，如果是同一个 AAA 服务器，也继续原有正常流程；如果不是同一个 AAA 服务器但 HSS 确定选用当前发请求的 AAA 服务器，也继续原有正常流程，只是在步骤 308 中或步骤 308 之后需要增加删除已登记 AAA 服务器与当前 WLAN 用户相关的信息和连接的步骤。

如果不是同一个 AAA 服务器且 HSS 确定选用已登记的 AAA 服务器，HSS 给当前发请求的 AAA 服务器返回已登记 AAA 服务器的地址，当前发请求的 AAA 服务器将接入认证请求转发给已登记的 AAA 服务器，步骤 303 和后续步骤通过已登记的 AAA 服务器继续完成。

实施例四：

本实施例也是基于图 3 所示的处理流程，将图 3 给出的交互流程与本发明核心思想的处理步骤相结合，主要涉及步骤 302 的变化，步骤 302 的变化与实施例三相同，其它步骤基本不变。

与实施例三的不同之处在于：不需要对步骤 303 和 304 进行修改，但增加了网络的预先配置和对认证路由的规划，根据不同的用户标识特征将用户路由到特定的 AAA 服务器上，以保障同一用户不可能同时与多个 AAA 服务器建立联系；或者是，在特殊的应用场景下，全网只有一个 AAA 服务器为用户提供服务，该 AAA 服务器本身可能是通过多个 AAA 服务器实体进行组合的，多个

AAA 服务器实体互为备份，以保障容灾和负荷分担，但对外只作为一个 AAA 服务器出现。这里，所提到的用户标识可以是用户的 NAI、临时用户名或永久用户名。

实施例五：

本实施例是本发明方法在 EAP-AKA 的 WLAN 接入认证过程中的应用，所述 EAP-AKA 认证的基本过程在规范中有详细规定。本实施例主要描述该过程在 WLAN-3GPP 交互运营网络中运行时，如何保障只有一个 AAA 服务器同时为一个用户服务。如图 6 所示，本实施例的方法包括以下步骤：

步骤 601：WLAN 用户终端与 WLAN 接入网根据 WLAN 技术规范建立无线连接。

步骤 602：WLAN 接入网向 WLAN 用户终端发送用户名请求信令 EAP Request/Identity，该 EAP 内容封装于 WLAN 具体的技术协议中。

步骤 603：WLAN 用户终端返回用户名响应消息 EAP Response/Identity，该消息中包括该 WLAN 用户终端自己的标识，该标识采用 IETF 规范 RFC 2486 定义的网络接入标识（NAI），该 NAI 可以是前次认证时分配的临时标识、或是永久标识 IMSI。其中，由 IMSI 构造 NAI 格式的方法在 EAP/AKA 规范中有详细定义，在此不再赘述。

步骤 604：根据 NAI 的域名，WLAN 用户终端发起的认证消息被路由到适当的 3GPP AAA 服务器。这里，路由中可能有一个或多个 AAA 代理（图中省略），可以用 Diameter referral 方法寻找和确定 AAA 服务器路由；也可以通过配置数据确定 AAA 服务器路由。

步骤 605：3GPP AAA 服务器收到包含有用户标识的 EAP Response/Identity 消息后，该消息中还含有 WLAN 接入网标识、VPLMN 标识以及 WLAN 用户终端的 MAC 地址。

步骤 606：3GPP AAA 服务器根据收到的标识把该用户作为 EAP-AKA 认证的候选，然后，3GPP AAA 服务器检查自身是否有该用户没有使用的认证元组

（Authentication Vectors），如果没有，则向 HSS/HLR 请求获取该认证元组，此时需要一个临时标识和 IMSI 的对照关系表。其中，3GPP AAA 服务器是否将当前用户作为候选也可以是：服务器先获取没有使用过的认证元组，基于获得的认证元组，比如获得 UMTS 的认证元组，再决定是否将该用户作为 EAP-AKA 认证的候选。

HSS/HLR 收到请求后，如果经检查发现已有另外一个 3GPP AAA 服务器已登记作为该用户的服务 AAA，并且，HSS/HLR 确认该已登记的 AAA 服务器工作正常，则该 HSS/HLR 会将该已登记的 AAA 服务器的地址通知当前请求获取认证元组的 3GPP AAA 服务器，那么，请求获取认证元组的 3GPP AAA 服务器就作为 PROXY 代理或 REDIRECTION 代理将认证消息转移给已登记的 3GPP AAA 服务器。此步骤之后，已登记的 3GPP AAA 服务器就作为为当前用户提供服务的 3GPP AAA 服务器。

步骤 607：3GPP AAA 服务器发出 EAP Request/AKA Identity 消息再次请求用户标识，发出该请求是因为中间节点可能改变或替换了在 EAP Response/Identity 消息中收到的用户标识，但如果确定 EAP Response/Identity 消息中的用户标识不可能被改变，相应处理步骤也可以被归属运营商省略。

步骤 608~609：WLAN 接入网将 EAP Request/AKA Identity 消息转发给 WLAN 用户终端；WLAN 用户终端响应一个与 EAP Response/Identity 中完全相同的用户标识。

步骤 610：WLAN 接入网转发 EAP Response/AKA Identity 消息到 3GPP AAA 服务器，3GPP AAA 服务器将使用本消息收到的用户标识来进行认证。如果 EAP Response/Identity 中的用户标识和 EAP Response/AKA Identity 中的用户标识不一致，则以前从 HSS/HLR 取得的用户签约信息和认证元组都是无效的，应该重新申请。也就是说，在步骤 611 之前要重复执行步骤 606 中请求认证元组的过程。

为了优化过程，当 3GPP AAA 服务器有足够的信息来识别一个用户作为

EAP-AKA 用户，则标识重新请求的过程应该在用户签约信息和认证信息被获得之前进行。虽然 Wx 接口的协议设计可能不允许以上四个步骤在所需的用户签约信息下载到 3GPP AAA 服务器上之前进行。

步骤 611：3GPP AAA 服务器检查是否已拥有 WLAN 接入所需的用户签约信息，如果没有这些信息，则应该从 HSS 取得；然后 3GPP AAA 服务器检查用户是否被授权使用 WLAN 接入服务。

虽然在本实施例中，本步骤在步骤 606 之后，但在实际应用中，本步骤可以在步骤 614 之前的任意位置执行。

步骤 612：由 IK 和 C 推导得到新的密钥信息，具体内容在规范中有详细规定，该密钥信息是 EAP-AKA 所需要的，当然，可能有更多的密钥信息会被产生出来提供给 WLAN 接入的安全性或完整性保护使用。

一个新的假名也可能被选择，并采用 EAP-AKA 产生的密钥信息保护。

步骤 613：3GPP AAA 服务器在 EAP Request/AKA-Challenge 消息中发送给 WLAN 接入网如下信息：RAND、AUTN、一个消息认证码（MAC，Message Authentication Code）和两个用户标识（如果有），其中，两个标识是指被保护的假名和/或重认证标识（Re-authentication ID）。是否发送重认证标识取决于 3GPP 运营商的运营规则是否允许重认证机制，也就是说，任何时候 AAA 服务器根据运营商的规则决定是否包含重认证标识，从而决定允许或不允许重认证过程进行。

步骤 614：WLAN 接入网将 EAP Request/AKA-Challenge 消息发送给 WLAN 用户终端。

步骤 615：WLAN 用户终端运行 USIM 上的 UMTS 算法，USIM 验证 AUTN 是否正确从而认证网络，如果 AUTN 是不正确的，该 WLAN 用户终端就拒绝该认证过程。如果序列数是不同步的，则该 WLAN 用户终端会发起一个同步过程，规范中有详细说明，在此不在详述。如果 AUTN 正确，则 USIM 计算出 RES、IK 和 CK。

WLAN 用户终端根据 USIM 新计算的 IK 和 CK 计算得到其他新的密钥信息，利用这些密钥信息检查得到的 MAC

如果收到了被保护的假名，WLAN 用户终端存储该假名待以后认证使用。

步骤 616: WLAN 用户终端用新的密钥信息计算一个覆盖 EAP 消息的新的 MAC 值，WLAN 用户终端将包含计算得到的 RES 和新计算的 MAC 值的 EAP Response/AKA-Challenge 消息发送给 WLAN 接入网。

步骤 617: WLAN 接入网将 EAP Response/AKA-Challenge 信息转发给 3GPP AAA 服务器。

步骤 618: 3GPP AAA 服务器检查得到的 MAC，并比较 XRES 和得到的 RES。

步骤 619: 如果全部检查通过，则 3GPP AAA 服务器发送认证成功消息 EAP Success 给 WLAN 接入网，如果一些为 WLAN 接入层安全和完整性保护准备的新的密钥产生，则 3GPP AAA 服务器把这些密钥信息包含在承载该 EAP 信息的 AAA 层协议消息中，即不包含在 EAP 层的信令中。WLAN 接入网保存这些密钥用来和认证通过的 WLAN 用户终端进行通信使用。

步骤 620: WLAN 接入网用 EAP Success 消息通知 WLAN 用户终端认证成功。此时，EAP AKA 交互成功的完成，并且 WLAN 用户终端和 WLAN 接入网都拥有了交互中产生的共享密钥信息。

步骤 621: 3GPP AAA 服务器比较认证交互中用户的 MAC 地址、VPLMN 标识和 WLAN 接入网标识信息与当前运行中的会话对应用户相应的信息，如果这些信息和运行中的会话都一致，则该认证过程是与目前运行中的 WLAN 会话关联的，对该会话不需要做任何处理。

如果该用户的 MAC 地址、或 VPLMN 标识、或 WLAN 接入网标识信息不同于当前的 WLAN 会话，则 3GPP AAA 服务器判断该认证过程是为了建立一个新的 WLAN 会话，3GPP AAA 服务器就会根据用户的多个 WLAN 会话是否被允许或 WLAN 会话的最多数目是否超过限制，来决定是否发起中止现有

WLAN 会话的过程。

本步骤实际就是一个判断、决策过程，具体的决策交互流程与实施例一中步骤 406~410 的描述完全相同，所采用的决策规则也可以根据网络是否允许用户建立多连接，选择相应的处理方式，完成拒绝新会话连接请求或删除某个旧会话连接的操作。

上述过程中，该认证过程可能会在任意阶段失败，比如：由于 MAC 验证失败、或 WLAN 用户终端在网络发出请求消息后没有响应失败等等。在这种情况下，EAP AKA 过程就会中止，并且要将失败的通知信息发送到 HSS/HLR。

实施例六：

本实施例是本发明方法在 EAP-SIM 的 WLAN 接入认证过程中的应用，所述 EAP-SIM 认证的基本过程规范中有详细规定。本实施例主要描述该过程在 WLAN-3GPP 交互运营网络中运行时，如何保障只有一个 AAA 服务器同时为一个用户服务。如图 7 所示，本实施例的方法包括以下步骤：

步骤 701：WLAN 用户终端与 WLAN 接入网根据 WLAN 技术规范建立无线连接。

步骤 702：WLAN 接入网向 WLAN 用户终端发送用户名请求信令 EAP Request/Identity，该 EAP 内容封装于 WLAN 具体的技术协议中。

步骤 703：WLAN 用户终端返回用户名响应消息 EAP Response/Identity，该消息中包括该 WLAN 用户终端自己的标识，该标识采用 IETF 规范 RFC 2486 定义的网络接入标识（NAI），该 NAI 可以是前次认证时分配的临时标识、或是永久标识 IMSI。其中，由 IMSI 构造 NAI 格式的方法在 EAP/SIM 规范中有详细定义，在此不再赘述。

步骤 704：根据 NAI 的域名，WLAN 用户终端发起的认证消息被路由到适当的 3GPP AAA 服务器。这里，路由中可能有一个或多个 AAA 代理（图中省略），可以用 Diameter referral 方法寻找和确定 AAA 服务器路由；也可以通过配置数据确定 AAA 服务器路由。

步骤 705: 3GPP AAA 服务器收到包含有用户标识的 EAP Response/Identity 消息后，该消息中还含有 WLAN 接入网络标识、VPLMN 标识以及 WLAN 用户终端的 MAC 地址。

步骤 706: 3GPP AAA 服务器根据收到的标识把该用户作为 EAP-SIM 认证的候选，然后 3GPP AAA 服务器发送 EAP Request/SIM-Start 给 WLAN 接入网，3GPP AAA 服务器重新请求用户标识，发出该请求是因为中间节点可能改变或替换了在 EAP Response/Identity 消息中收到的用户的。但是，如果确定 EAP Response/Identity 消息中的用户标识不可能被改变，则相应处理步骤可以被归属运营商忽略。其中，3GPP AAA 服务器是否将当前用户作为候选也可以是：服务器先获取没有使用过的认证元组，基于获得的认证元组，比如获得 GSM 的认证元组，再决定是否将该用户作为 EAP-SIM 认证的候选。

步骤 707~708: WLAN 接入网将 EAP Request/SIM-Start 信息发送给 WLAN 用户终端；WLAN 用户终端选择一个新的随机数 NONCE_MT，该随机数用于网络认证。WLA N 用户终端响应一个与 EAP Response/Identity 中完全相同的用户标识。

WLAN 用户终端发送给 WLAN 接入网的 EAP Response/SIM-Start 信息中包含有 NONCE_MT 和用户标识。

步骤 709: WLAN 接入网发送 EAP Response/SIM-Start 信息给 3GPP AAA 服务器，3GPP AAA 服务器将使用本消息收到的用户标识来进行认证，如果 EAP Response/Identity 中的用户标识和 EAP Response/SIM Start 中的用户标识不一致，则以前从 HSS/HLR 取得的用户签约信息和认证元组都是无效的，应该重新申请。

步骤 710: 3GPP AAA 服务器检查自身是否有该用户的 N 个没有使用的认证元组，如果有，则 N 个 GSM 认证元组被用来产生一个与 EAP-AKA 长度一致的密钥信息；如果没有 N 个认证元组，则需要从 HSS/HLR 获取一组认证元组，此时需要一个临时标识和 IMSI 的对照关系表。

HSS/HLR 收到请求后，如果经检查发现已有另外一个 3GPP AAA 服务器已登记作为该用户的服务 AAA，并且，HSS/HLR 确认该已登记的 AAA 服务器工作正常，则该 HSS/HLR 会将该已登记的 AAA 服务器的地址通知当前请求获取认证元组的 3GPP AAA 服务器，那么，请求获取认证元组的 3GPP AAA 服务器就作为 PROXY 代理或 REDIRECTION 代理将认证消息转移给已登记的 3GPP AAA 服务器。此步骤之后，已登记的 3GPP AAA 服务器就作为为当前用户提供服务的 3GPP AAA 服务器。

虽然在本实施例中，本步骤在步骤 709 之后，但在实际操作中，本步骤可以在步骤 712 之前的任意位置执行，比如：在步骤 705 之后。

步骤 711：3GPP AAA 服务器检查是否已拥有 WLAN 接入所需的用户签约信息，如果没有这些信息，则应该从 HSS 取得；然后 3GPP AAA 服务器检查用户是否被授权使用 WLAN 接入服务.

虽然在本实施例中，本步骤在步骤 710 之后，但在实际操作中，本步骤可以在步骤 718 之前的任意位置执行。

步骤 712：由 NONCE_MT 和 N 个 Kc 推导得到新的密钥信息，具体内容在规范中有详细规定，该密钥信息是 EAP-SIM 所需要的，当然，可以有更多的密钥信息被产生出来提供给 WLAN 接入的安全性或完整性保护使用。

一个新的假名和/或重认证标识可能被选择，并采用 EAP-SIM 产生的密钥信息保护，比如：加密并作完整性保护。

一个消息认证码(MAC)可以通过采用 EAP-SIM 得到的密钥覆盖整个 EAP 消息计算得到，用来进行网络认证值。

3GPP AAA 服务器在 EAP Request/SIM-Challenge 消息中发送给 WLAN 接入网如下信息：RAND、AUTN、一个消息认证码（MAC）和两个用户标识（如果有），其中，两个标识是指被保护的假名和/或重认证标识（Re-authentication ID）。是否发送重认证标识取决于 3GPP 运营商的运营规则是否允许重认证机制，也就是说，任何时候 AAA 服务器根据运营商的规则决定是否包含重认证

标识，从而决定允许或不允许重认证过程进行。

步骤 713：WLAN 发送 EAP Request/SIM-Challenge 消息给 WLAN 用户终端。

步骤 714：WLAN 用户终端在 SIM 中运行 N 次 GSM A3/A8 算法，为每个收到的 RAND 运行一次，该计算产生 N 个 SRES 和 Kc 值。

WLAN 用户终端根据 N Kc keys 和 NONCE_MT 计算出其他密钥信息。

WLAN 用户终端用最新得到的密钥信息计算一个用于网络认证的 MAC，并检验其是否和收到的 MAC 相同，如果这个 MAC 不正确，则网络认证失败，WLAN 用户终端取消该认证过程，仅当 MAC 正确 WLAN 用户终端才会继续认证交互过程。

WLAN 用户终端用新的密钥信息覆盖每个和 N 个 SRES 响应关联的 EAP 消息，计算一个新的 MAC。

如果收到了被保护的假名，WLAN 用户终端存储该假名待以后认证使用。

步骤 715：WLAN 用户终端将包含新计算得到的 MAC 的 EAP Response/SIM-Challenge 消息发送给 WLAN 接入网。

步骤 716：WLAN 接入网发送 EAP Response/SIM-Challenge 消息给 3GPP AAA 服务器。

步骤 717：3GPP AAA 服务器检查得到的 MAC 是否和自己存储的一致。

步骤 718：如果全部检查通过，则 3GPP AAA 服务器发送认证成功 EAP Success 消息给 WLAN 接入网，如果一些为 WLAN 接入层安全和完整性保护准备的新的密钥产生，则 3GPP AAA 服务器把这些密钥信息包含在承载该 EAP 信息的 AAA 层协议消息中，即不包含在 EAP 层的信令中。WLAN 接入网保存这些密钥用来和认证通过的 WLAN 用户终端进行通信使用。

步骤 719：WLAN 接入网用 EAP Success 消息通知 WLAN 用户终端认证成功。此时 EAP SIM 交互成功的完成，并且，WLAN 用户终端和 WLAN 接入网都拥有了交互中产生的共享密钥信息。

步骤720: 3GPP AAA服务器比较认证交互中用户的MAC地址、VPLMN 标识和 WLAN 接入网络的标识信息与当前运行中的会话对应用户相应的信息，如果这些信息和运行中的会话都一致，则该认证过程是和目前运行中的 WLAN 会话关联的，对该会话不需要做任何处理。

如果该用户的MAC地址或VPLMN 标识或WLAN接入网能力信息不同于当前的 WLAN 会话，则 3GPP AAA 服务器判断该认证过程是为了建立一个新的 WLAN 会话。3GPP AAA 服务器就会根据用户的多个 WLAN 会话是否被允许或 WLAN 会话的最多数目是否超过限制，来决定是否发起中止现有 WLAN 会话的过程。

本步骤实际就是一个判断、决策过程，具体的决策交互流程与实施例一中步骤 406~410 的描述完全相同，所采用的决策规则也可以根据网络是否允许用户建立多连接，选择相应的处理方式，完成拒绝新会话连接请求或删除某个旧会话连接的操作。

上述过程中，该认证过程可能会在任意阶段失败，比如：由于 MAC 验证失败、或 WLAN 用户终端在网络发出请求消息后没有响应失败等等。在这种情况下，EAP SIM 过程就会中止，并且要将失败的通知信息发送到 HSS/HLR。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

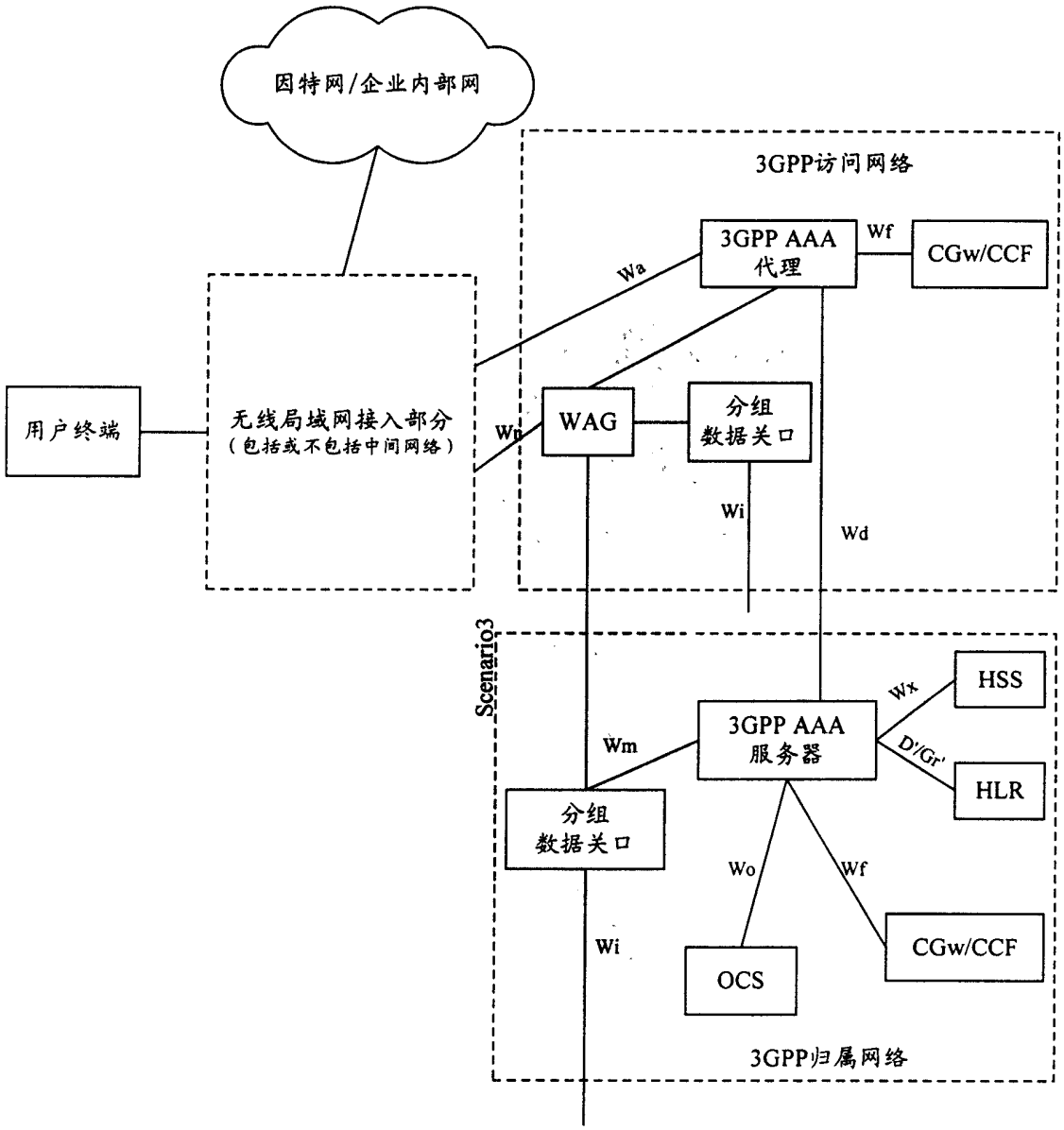

因特网/企业内部网
3GPP访问网络
3GPP AAA
代理
Wf
CGw/CCF
Wa
用户终端
无线局域网接入部分
（包括或不包括中间网络）
Wn
WAG
分组
数据关口
Wi
Wd
Scenario3
Wx
HSS
3GPP AAA
服务器
Wm
D'/Gr'
HLR
分组
数据关口
Wo
Wf
Wi
CGw/CCF
OCS
3GPP归属网络

图 1

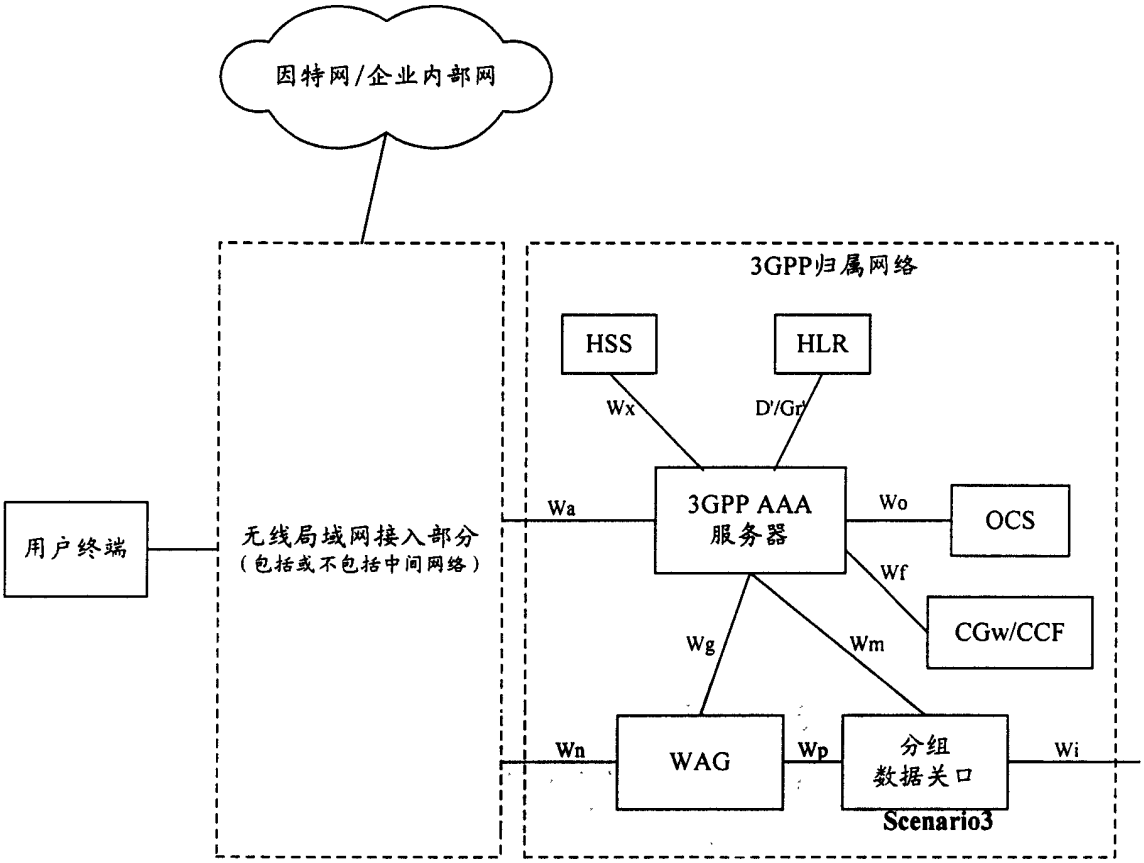

因特网/企业内部网
3GPP归属网络
HSS
HLR
Wx
D'/Gr'
用户终端
无线局域网接入部分
（包括或不包括中间网络）
Wa
3GPP AAA
服务器
Wo
OCS
Wf
CGw/CCF
Wg
Wm
Wn
WAG
Wp
分组
数据关口
Wi
Scenario3

图 2

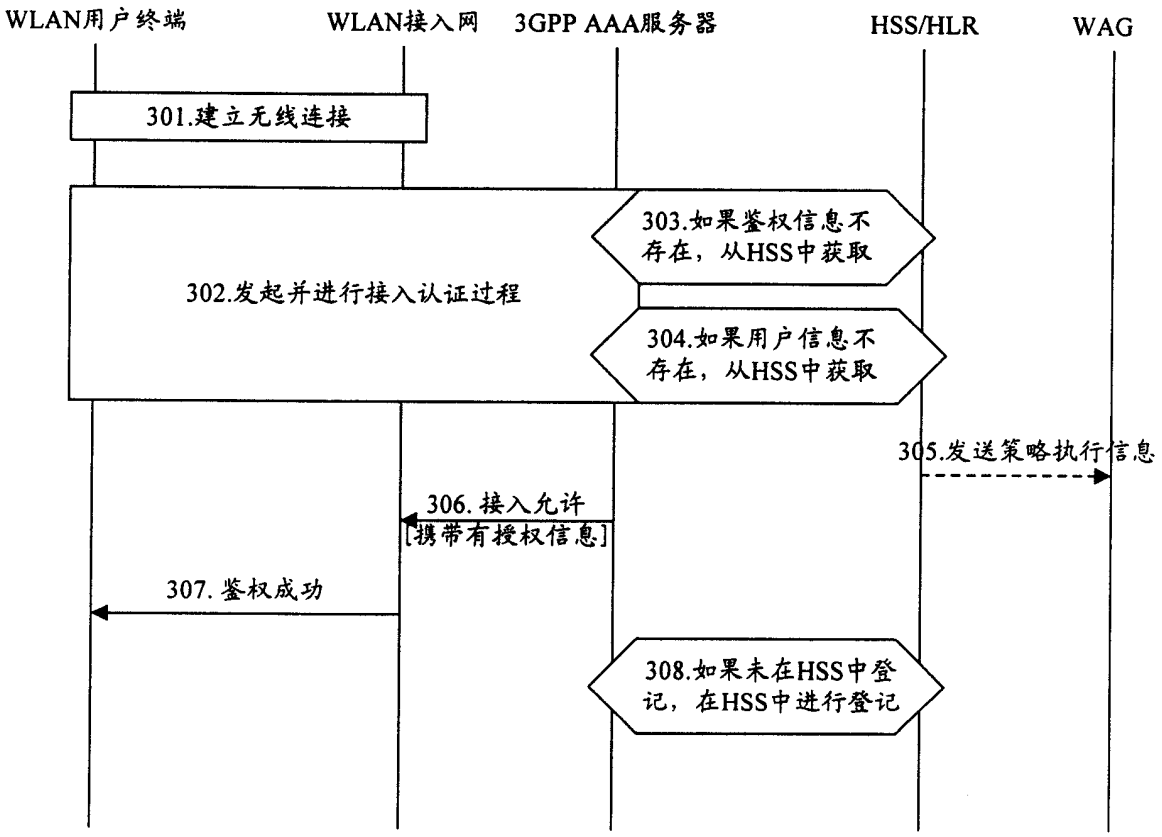

WLAN用户终端
WLAN接入网
3GPP AAA服务器
HSS/HLR
WAG
301.建立无线连接
303.如果鉴权信息不存在，从HSS中获取
302.发起并进行接入认证过程
304.如果用户信息不存在，从HSS中获取
305.发送策略执行信息
306. 接入允许
[携带有授权信息]
307. 鉴权成功
308.如果未在HSS中登记，在HSS中进行登记

图 3

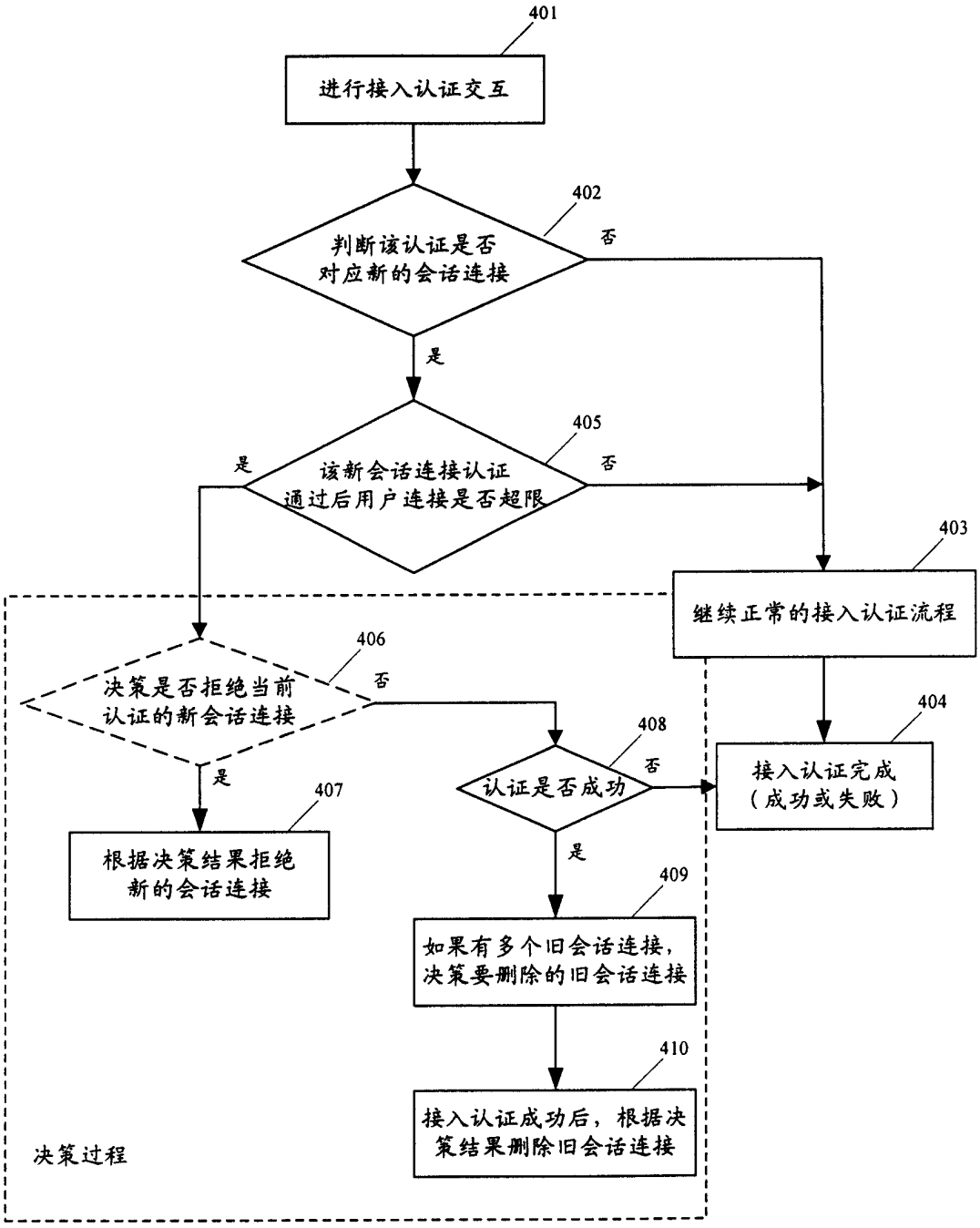

401
进行接入认证交互
402
判断该认证是否对应新的会话连接
否
是
405
该新会话连接认证通过后用户连接是否超限
是
否
403
继续正常的接入认证流程
406
决策是否拒绝当前认证的新会话连接
否
是
407
根据决策结果拒绝新的会话连接
408
认证是否成功
否
是
404
接入认证完成（成功或失败）
409
如果有多个旧会话连接，决策要删除的旧会话连接
410
接入认证成功后，根据决策结果删除旧会话连接
决策过程

图 4

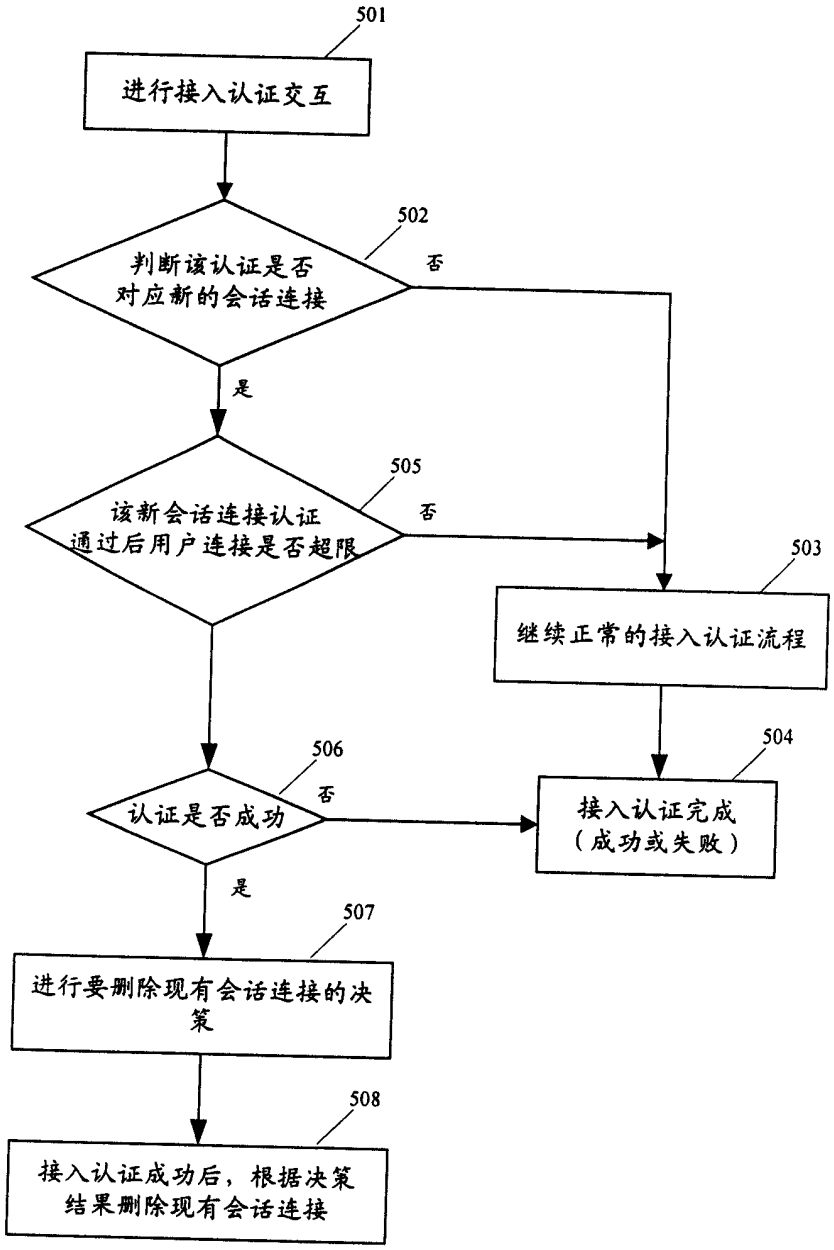

501
进行接入认证交互
502
判断该认证是否
对应新的会话连接
否
是
505
该新会话连接认证
通过后用户连接是否超限
否
503
继续正常的接入认证流程
504
接入认证完成
（成功或失败）
506
认证是否成功
否
是
507
进行要删除现有会话连接的决策
508
接入认证成功后，根据决策
结果删除现有会话连接

图 5

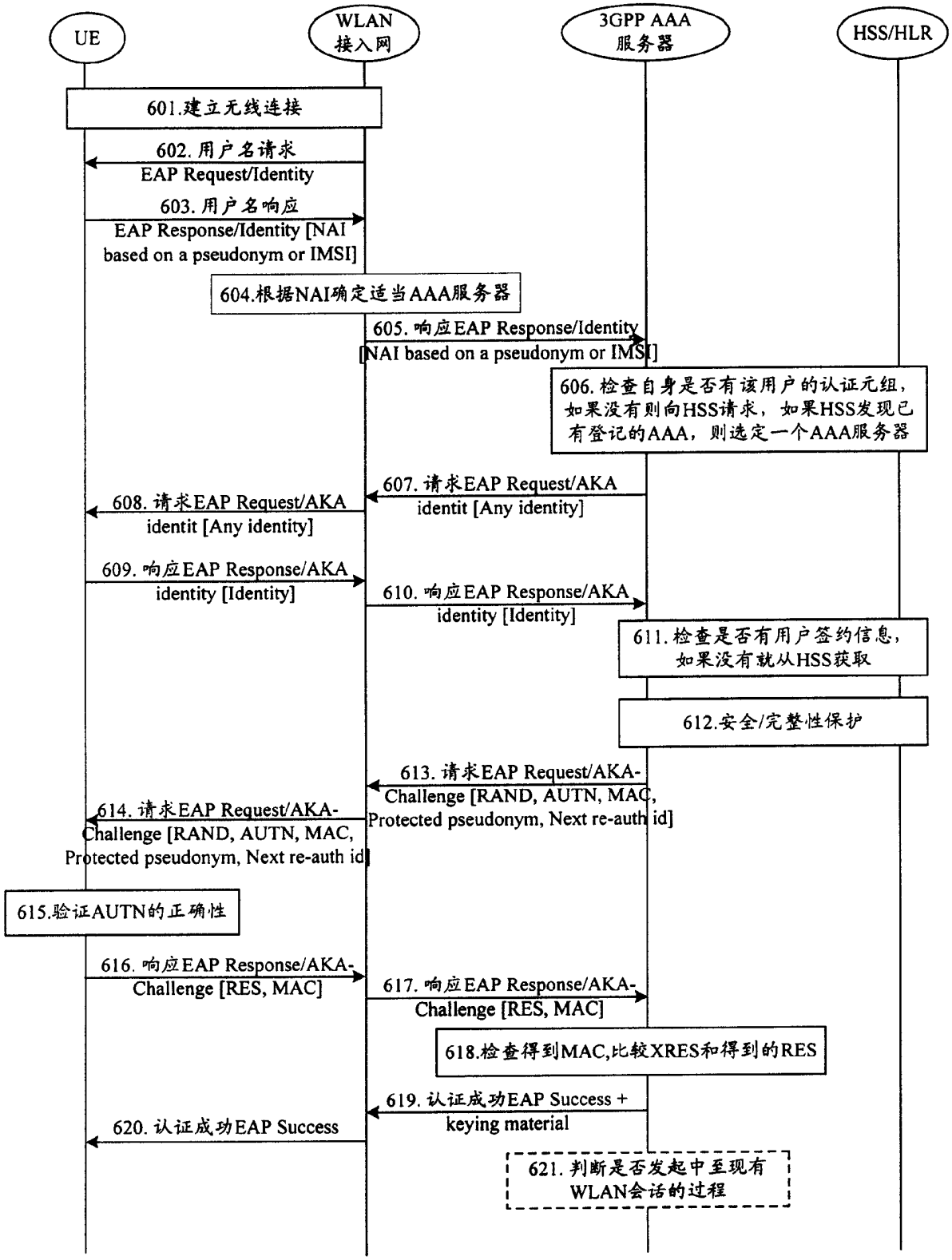

UE
WLAN 接入网
3GPP AAA 服务器
HSS/HLR
601.建立无线连接
602. 用户名请求
EAP Request/Identity
603. 用户名响应
EAP Response/Identity [NAI based on a pseudonym or IMSI]
604.根据NAI确定适当AAA服务器
605. 响应EAP Response/Identity [NAI based on a pseudonym or IMSI]
606. 检查自身是否有该用户的认证元组，如果没有则向HSS请求，如果HSS发现已有登记的AAA，则选定一个AAA服务器
607. 请求EAP Request/AKA identit [Any identity]
608. 请求EAP Request/AKA identit [Any identity]
609. 响应EAP Response/AKA identity [Identity]
610. 响应EAP Response/AKA identity [Identity]
611. 检查是否有用户签约信息，如果没有就从HSS获取
612.安全/完整性保护
613. 请求EAP Request/AKA-Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
614. 请求EAP Request/AKA-Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
615.验证AUTN的正确性
616. 响应EAP Response/AKA-Challenge [RES, MAC]
617. 响应EAP Response/AKA-Challenge [RES, MAC]
618.检查得到MAC,比较XRES和得到的RES
619. 认证成功EAP Success + keying material
620. 认证成功EAP Success
621. 判断是否发起中至现有WLAN会话的过程

图 6

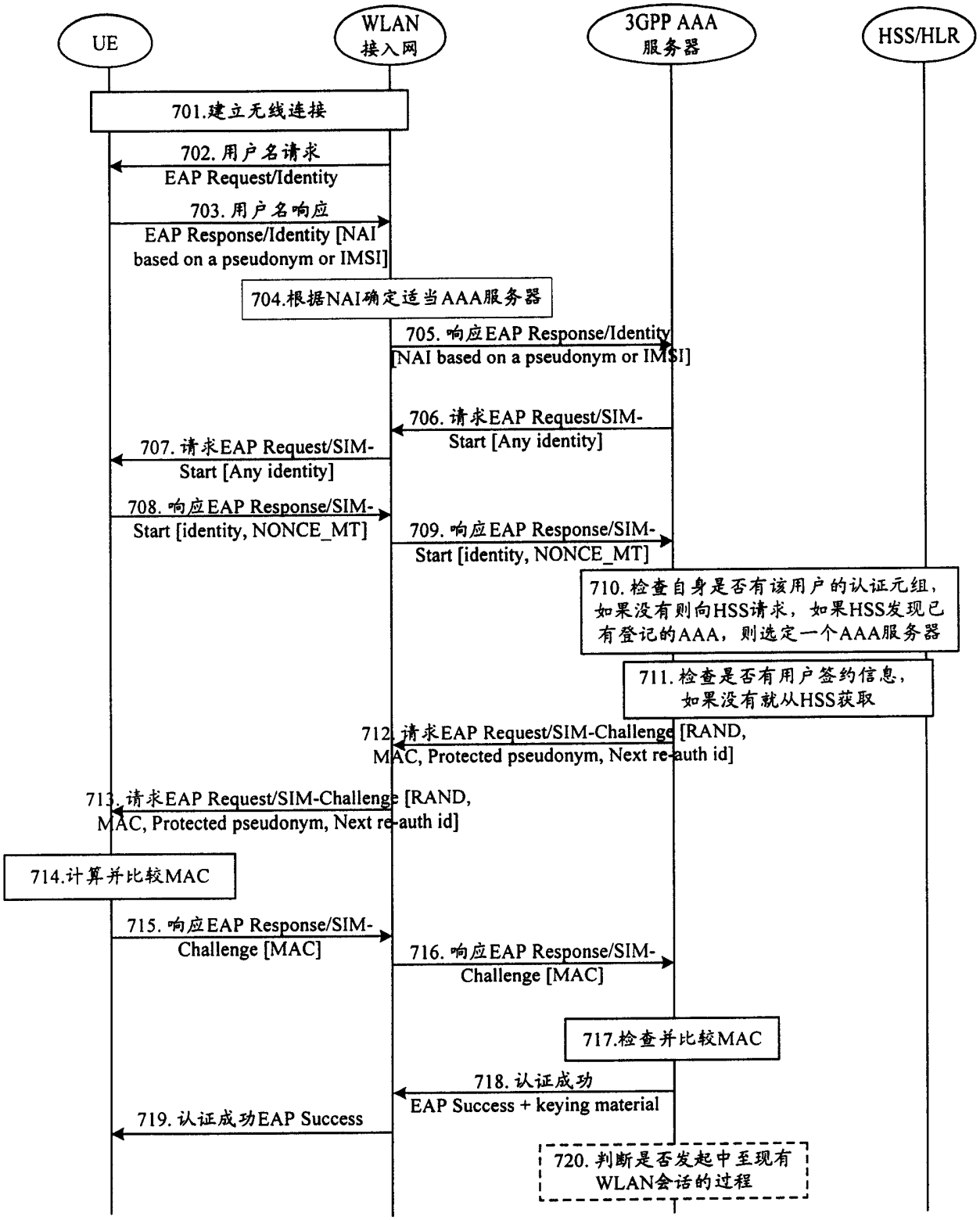

UE
WLAN
接入网
3GPP AAA
服务器
HSS/HLR
701.建立无线连接
702. 用户名请求
EAP Request/Identity
703. 用户名响应
EAP Response/Identity [NAI based on a pseudonym or IMSI]
704.根据NAI确定适当AAA服务器
705. 响应EAP Response/Identity [NAI based on a pseudonym or IMSI]
706. 请求EAP Request/SIM-Start [Any identity]
707. 请求EAP Request/SIM-Start [Any identity]
708. 响应EAP Response/SIM-Start [identity, NONCE_MT]
709. 响应EAP Response/SIM-Start [identity, NONCE_MT]
710. 检查自身是否有该用户的认证元组，如果没有则向HSS请求，如果HSS发现已有登记的AAA，则选定一个AAA服务器
711. 检查是否有用户签约信息，如果没有就从HSS获取
712. 请求EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id]
713. 请求EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id]
714.计算并比较MAC
715. 响应EAP Response/SIM-Challenge [MAC]
716. 响应EAP Response/SIM-Challenge [MAC]
717.检查并比较MAC
718. 认证成功
EAP Success + keying material
719. 认证成功EAP Success
720. 判断是否发起中至现有WLAN会话的过程

图 7