[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04M 1/725 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200880004289.7

[43] 公开日 2009 年 12 月 16 日

[11] 公开号 CN 101606372A

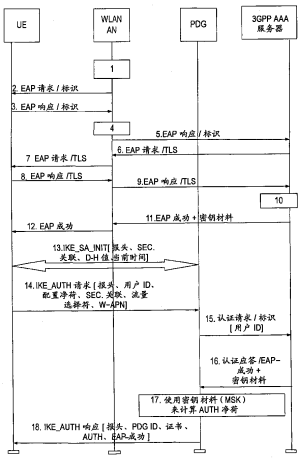
[22] 申请日 2008.2.5
[21] 申请号 200880004289.7
[30] 优先权
[32] 2007. 2. 6 [33] US [31] 60/899,643
[86] 国际申请 PCT/EP2008/051385 2008.2.5
[87] 国际公布 WO2008/095918 英 2008.8.14
[85] 进入国家阶段日期 2009.8.6
[71] 申请人 诺基亚公司
地址 芬兰埃斯波
[72] 发明人 张大江 李长红 P·埃罗南
[74] 专利代理机构 北京市金杜律师事务所
代理人 吴立明
权利要求书 4 页 说明书 11 页 附图 2 页

[54] 发明名称

支持无 UICC 呼叫

[57] 摘要

本发明涉及一种方法，所述方法包括：从订户终端发起会话，其中所述订户终端不包括专用用户标识模块，以及通过使用执行服务器认证并且避免客户端认证的过程，基于所述订户终端的临时标识来认证所述会话。



1. 一种方法，包括:

从订户终端发起会话，其中所述订户终端不包括专用用户标识模块，以及

通过使用执行服务器认证并且避免客户端认证的过程，基于所述订户终端的临时标识来认证所述会话。

2. 根据权利要求 1 所述的方法，其中所述过程是可扩展认证协议传输层安全性（EAP/TLS）协议。

3. 根据权利要求 1 所述的方法，其中在可用于用户数据加密的订户终端中生成共享主会话密钥。

4. 根据权利要求 1 所述的方法，其中在可用于用户数据加密的服务器中生成共享主会话密钥。

5. 根据权利要求 1 所述的方法，其中所述临时标识包括用户标识符和区域，所述区域包括用于由不包括所述用户标识模块的订户终端发起的会话的专用指示。

6. 根据权利要求 5 所述的方法，其中所述专用指示指示出应急。

7. 根据权利要求 5 所述的方法，其中基于终端标识符或者经哈希变换的终端标识符来创建所述用户标识符。

8. 根据权利要求 7 所述的方法，其中所述终端标识符是国际移动设备标识。

9. 根据权利要求 5 所述的方法，其中基于经哈希变换的终端标识符来创建所述用户标识符，其中基于完整的终端标识符来执行认证。

10. 根据权利要求 7 所述的方法，其中在所述订户终端中创建所述用户标识符。

11. 根据权利要求 5 所述的方法，其中基于所述订户终端的介质访问控制地址或者由接入网元分配给所述订户终端的互联网协议地址，来创建所述用户标识符。

12. 根据权利要求 5 所述的方法，其中基于所述订户终端的介质访问控制地址以及网络标识符的组合、或者消息认证代码介质访问控制地址以及所述网络标识符的经哈希变换的组合，来创建所述用户标识符。

13. 根据权利要求 12 所述的方法，其中在网络控制单元中创建所述用户标识符。

14. 根据权利要求 13 所述的方法，其中在初始消息中，所述订户终端使用标识符来接入所述网元，并且所述网元响应于所述初始消息来创建用户标识符。

15. 根据权利要求 1 所述的方法，进一步包括:

检查是否已经存在用于所述订户终端的会话，以及

如果已经存在会话，则拒绝所述会话。

16. 根据权利要求 1 所述的方法，其中所述订户终端以及所述网元经由互通无线局域网来连接。

17. 一种设备，包括:

控制器，配置用于:

发起会话，其中所述设备订户终端不包括专用用户标识模块，以及

创建临时标识，

其中使用执行服务器认证并且避免客户端认证的认证过程。

18. 根据权利要求 17 所述的设备，其中所述过程是可扩展认证协议传输层安全性（EAP/TLS）协议。

19. 根据权利要求 17 所述的设备，其中生成可用于用户数据加密的主会话。

20. 根据权利要求 17 所述的设备，其中所述临时标识包括用户标识符和区域，所述区域包括用于由不包括用户标识模块的设备发起的会话的专用指示。

21. 根据权利要求 20 所述的设备，其中所述专用指示指示出应急。

22. 根据权利要求 19 所述的设备，其中通过基于设备的终端标识符或者经哈希变换的终端标识符来创建所述用户标识符。

23. 根据权利要求 22 所述的设备，其中所述终端标识符是国际移动设备标识。

24. 根据权利要求 20 所述的设备，其中所述控制器配置用于在初始化消息中创建为了访问网元将使用的用户标识符，并且配置用于在稍后消息中使用用户标识，所述稍后消息是由所述网元基于所述订户终端的消息认证代码地址而创建。

25. 一种设备，包括：

收发机，配置用于从订户终端接收认证请求消息，其中所述订户终端不包括专用用户标识模块，以及

控制器，配置用于通过使用执行服务器认证并且避免客户端认证的过程，基于临时标识来执行认证。

26. 根据权利要求 21 所述的设备，其中所述过程是可扩展认证协议传输层安全性（EAP/TLS）协议。

27. 根据权利要求 26 所述的设备，其中所述控制器配置用于从来自服务器的认证应答提取主会话密钥。

28. 根据权利要求 26 所述的设备，其中针对用户数据加密生成主会话密钥。

29. 根据权利要求 25 所述的设备，其中所述临时标识包括用户标识符和区域，所述区域包括用于由不包括所述用户标识模块的订户终端发起的会话的专用指示。

30. 根据权利要求 29 所述的设备，其中所述专用指示指示出应急。

31. 根据权利要求 29 所述的设备，其中基于终端标识符或者经哈希变换的终端标识符来创建所述用户标识符。

32. 根据权利要求 31 所述的设备，其中所述终端标识符是国际移动设备标识。

33. 根据权利要求 29 所述的设备，其中在所述订户终端中创建

所述用户标识符。

34. 根据权利要求 29 所述的设备，其中所述控制器配置用于基于所述订户终端的介质访问控制地址或者由接入网元分配给所述订户终端的互联网协议地址，来创建所述用户标识符。

35. 根据权利要求 29 所述的设备，其中所述控制器配置用于基于所述订户终端的介质访问控制地址以及网络标识符的组合、或者所述介质访问控制地址以及所述网络标识符的经哈希变换的组合，来创建所述用户标识符。

36. 根据权利要求 21 所述的设备，其中所述控制器适用于：

检查是否已经存在用于所述订户终端的会话，以及

如果已经存在会话，则拒绝所述会话。

37. 根据权利要求 30 所述的设备，其中所述设备是分组数据网关（PDG）。

38. 一种包括订户终端和服务器的系统，其中所述订户终端包括根据权利要求 17 至 24 中的一项所述的设备，以及所述服务器包括根据权利要求 25 至 37 中的一项所述的设备。

39. 一种用于计算机的包括软件代码部分的计算机程序产品，当所述程序在所述计算机上运行时，用于执行根据权利要求 1 至 15 中的任一项所述的步骤。

40. 根据权利要求 39 所述的计算机程序产品，其中所述计算机程序产品包括其上存储所述软件代码部分的计算机可读介质。

支持无 UICC 呼叫

技术领域

本发明涉及用于支持如下呼叫的方法和设备，所述呼叫诸如来自 I-WLAN 接入网络中不具有订户标识模块（无 UICC）的订户终端的 IMS 应急呼叫。

背景技术

公共 WLAN 的增长为适当装备的终端设备（或者第三代术语中的用户设备（UE））提供了经由此类 WLAN 访问蜂窝归属网络和拜访网络的机会。由此，将提供此类互通功能的 WLAN 称作 I-WLAN。I-WLAN 连接至公共陆地移动网络（PLMN），所述 PLMN 支持 UE 来访问归属网络（HPLMN）以及拜访网络（VPLMN）上的网络服务。

将按照法律绑定无线设备以便支持应急呼叫。即使当在多个接入设备的特定无线信道之上当前没有活跃的会话时（即，用户当前没有附着至任何无线、或者当前设备中没有插入订户标识模块（SIM）或者通用移动通信系统 SIM（USIM）），应急报告应该也是可以的。

通常，通过拨动开关或者呼叫应急号码所发起的应急报告通常是以优先级化的方式处理的，以便容易获得接入来调用应急警报。然而，无线设备在应急期间可能不具有可靠的功能或者可能无法可靠地使用，从而可能无法正确地完成输入口令或者其他认证过程。此外，无线设备可能靠近网络或者接入网络，但是并不与该网络相关联。因此，在听到警报或者联系应急中心之前，并不需要进行授权，以便加速该应急呼叫。

在第三代合作伙伴计划（3GPP）的规范 TS 23.234、33.234、24.234 以及 29.234 中定义了 I-WLAN（交互式无线局域网）接入。针对直接 IP 接入（所谓的情况 2）以及 3GPP IP 接入（所谓的情况 3），

使用可扩展认证协议（EAP）SIM/AKA（认证和密钥协商）过程来认证，其中基于针对订户数据库（例如，归属订户服务器 HSS））处保持的信息进行的订户检查来进行授权。

支持 IMS 应急呼叫的 W-APN 网络标识符应该采取公共的、预留的网络标识符的“sos”形式，如在 TS 23.003 中定义的“sos.w-apn.mnc012.mcc345.pub.3gppnetwork.org”。

此类 W-APN 向 WLAN 接入网络或者 3GPP AAA 服务器指示为了应急呼叫或者另一优先级化呼叫而需要接入。

目前，在 3GPP 中尚无达成一致的解决方案，即对于无 UICC 用户（不具有通用集成电路卡的用户）来说，将采用何种认证方法和用户 ID 来针对 IMS 应急而接入 I–WLAN。

对于 I-WLAN 中的所有用户来说，可以使用公共用户名和公共口令以便进行无 UICC 的 IMS 应急呼叫。

在 3GPP TSG SA WG2 架构的临时文档 S2-051950（2005 年 9 月 5-9 日）中，描述了一种因特网协议上的语音（VoIP）应急呼叫支持，其中通过使用伪 IMSI（国际移动订户标识）来便于 WLAN 接入，而经由 WLAN 来支持 VoIP 应急呼叫。所述伪 IMSI 继而可以用于创建用户专用伪网络接入标识符（NAI），以便在初始接入和认证过程中使用。伪 IMSI 是由移动国家代码（MCC）和移动网络代码（MNC）以及来自国际移动设备标识（IMEI）的数字的唯一组合而构成的。由 WLAN 所倡导的 VPLMN 都能够支持使用所述伪 NAI 来支持认证以便进行应急服务，或者可能以指示对此支持的能力和意愿的优先级顺序来向 UE 呈现。VPLMN 继而将 UE 视为临时归属订户，并且或者略过认证和授权（AAA）或者确保其成功。

然而，同样在此情况下，会话不能继续。

在当前的 TS 23.234 中，支持 IMS 应急呼叫的要求在于，向 WLAN UE 提供 IP 承载能力，以便在 UICC 和无 UICC 两种情况下接入 IMS 应急呼叫。此外，认证可以是（i）被完全略过；或者（ii）使用“哑”或者“空”的认证方法。

由此，当前对于 I-WLAN 上的无 UICC 用户的 IMS 应急呼叫，没有规定可靠的机制。并且没有对将用于无 UICC 用户的用户 ID 的定义，所述用户 ID 的定义对于形成 NAI 是需要的（与 W-APN 一起）。

发明内容

由此，本发明的一个目的是解决上述问题，并且提供用于处理呼叫的可靠机制，所述呼叫诸如来自 I-WLAN 系统中无 UICC 用户的 IMS 应急呼叫。

根据本发明的实施方式，通过一种方法来实现此目的，该方法包括：从订户终端发起会话，其中所述订户终端不包括专用用户标识模块，以及通过使用执行服务器认证并且避免客户端认证的过程，基于所述订户终端的临时标识来认证所述会话。

备选地，根据本发明的实施方式，通过一种设备来实现此目的，该设备包括：配置用于发起会话的控制器，其中所述设备订户终端不包括专用用户标识模块，以及创建临时标识，其中使用执行服务器认证并且避免客户端认证的认证过程。

此外，备选地，根据本发明的实施方式，通过一种设备实现上述目的，该设备包括：收发机，配置用于从订户终端接收认证请求消息，其中所述订户终端不包括专用用户标识模块，以及控制器，配置用于通过使用执行服务器认证并且避免客户端认证的过程，基于所述临时标识来实施认证。

由此，根据权利要求书，由不执行客户端认证而是执行服务器认证的过程（认证方法或者协议）来执行认证。

以此方式，可以以可靠的方式处理来自无 UICC 订户终端的应急呼叫。

附图说明

通过参考所附附图来描述本发明，在附图中：

图 1 示出了根据本发明第一实施方式的消息信令图；以及

图 2A 至图 2D 示出了在本发明的实施方式中所包括的网元的基础配置。

具体实施方式

在下文中，通过参考所附附图来描述本发明的优选实施方式。

根据本实施方式，在 IMS 应急情况下，针对无 UICC 用户来说，建议使用可扩展认证协议-传输层安全性（EAP-TLS）作为 I-WLAN 中的认证方法。即，EAP-TLS 可以略过客户端认证。然而，仍然提供服务器认证。这意味着，如果需要，仍然可以获取密钥来继续以及用户加密。通过此方式，不需要对 WLAN AN 进行改变。

在附图 1 中示出了针对无 UICC 用户的应急呼叫的详细信令序列。应该注意，在此序列中仅示出了主要网元，即用户实体（UE）、WLAN 接入网络（AN），其可以是单一网元或者分布式网元，分组数据网关（PDG）以及授权和计费（AAA）服务器。

在步骤 1 中，在 WLAN 用户实体（UE）和 WLAN 接入网（AN）之间使用无线 LAN 技术专用过程来建立连接。

在步骤 2 中，WLAN AN 向 WLAN UE 发送 EAP 请求/标识。应该注意，通过封装在无线 LAN 技术专用协议中的无线 LAN 接口来传输 EAP 分组。

在步骤 3 中，WLAN UE 发送 EAP 响应/标识消息。WLAN UE 发送用户标识，其符合在 3GPP TS 23.003 中规定的网络接入标识符（NAI）格式。以应急专用区域来填充用户标识中的 NAI 的区域部分（realm part）。即，如上所述，例如区域可以包括“sos”。无 UICC 的 WLAN UE 的标识可以是 IMEI、MAC 地址或者由 WLAN AN（作为接入网元的示例）分配的本地 IP 地址，并伴随有 WLAN AN 信息，在下文中将更为详细地描述。

在步骤 4 中，基于 NAI 的区域部分，向合适的 3GPP 认证、授权和计费（AAA）服务器路由消息。路由路径可以包括一个或者多个 AAA 代理（在附图中未示出）。

还应该注意，可以应用直径（diameter）推举来查找 AAA 服务器。

在步骤 5 中，3GPP AAA 服务器接收包含终端标识的 EAP 响应/标识分组。利用如在 3GPP TS 23.003 中所定义、以应急专用区域填充的用户标识中的 NAI 的区域部分，3GPP AAA 服务器基于所接收的标识来确定用户正在请求应急呼叫。3GPP AAA 服务器将设置 Emergency_Access（应急接入）标记。

WLAN 无线网络的标识符以及 WLAN UE 的 MAC 地址也将由 3GPP AAA 服务器在同一消息中接收。

在步骤 6 中，3GPP AAA 服务器使用 EAP-TLS 来发起认证，其中省略了客户端认证。即，并不这样地（即，如在具有 UICC 的订户的情况下那样）检查订户标识。

在步骤 7 中，WLAN AN 向 WLAN UE 转发 EAP 请求/TLS。

在步骤 8 中，WLAN UE 以 EAP 响应/TLS 做出响应。

在步骤 9 中，WLAN AN 向 3GPP AAA 服务器转发 EAP 响应/TLS。

在步骤 10 中，从 TLS 主秘密导出主会话密钥（MSK），参见 RFC 4346。

在步骤 11 中，3GPP AAA 服务器向 WLAN AN 发送 EAP 成功消息。WLAN AN 可以存储密钥材料（MSK），其用在与认证的 WLAN UE 的通信中。

在步骤 12 中，向 WLAN UE 转发 EAP 成功消息。

在步骤 13 中，WLAN UE 和 PDG 交换第一对消息，其已知为 IKE_SA_INIT（例如参见 TS 33.324），其中 PDG 和 WLAN UE 协商加密算法，交换当前时间（nonce）并且执行 Diffie_hellman 交换。

在步骤 14 中，在 IKE_AUTH 阶段的该第一消息中，无 UICC 的 WLAN UE 发送用户标识（在 Idi 净荷中）以及应急 W-APN 信息（在 Idr 净荷中），并且开始子安全性关联的协商。WLAN UE 通过其 NAI 中的区域部分向 PDG 指示，连接请求针对于应急呼叫，并且其希望

使用 IKEv2 之上的 EAP。

用户标识应该与 IETF RFC 4282（2005 年 12 月：“The Network Access Identifier（网络接入标识符）”）中规定的网络接入标识符（NAI）格式相一致。根据 IETF RFC 4306（2005 年 12 月：“Internet Key Exchange(IKEv2) Protocol（因特网密钥交换（IKEv2）协议）”），当在 IKEv2 上使用时，在 EAP 交换中生成的共享秘密（MSK）应用于生成 AUTH 参数。

如果 WLAN UE 的远程 IP 地址需要动态配置时，则 WLAN UE 应在 IKE_AUTH 请求消息内发送配置净荷（CFG_REQUEST），以便获取远程 IP 地址。

在步骤 15 中，PDG 向 3GPP AAA 服务器发送具有空 EAP 属性值对（AVP）的请求消息，其包含用户标识。PDG 将包括一个参数，该参数指示正在为建立隧道而执行认证。这将有助于 3GPP AAA 服务器来区分用于 WLAN 接入的认证以及用于隧道建立的认证。

在步骤 16 中，3GPP AAA 服务器将检查是否为用户设置了 Emergency_Access 标记。如果设置了 Emergency_Access 标记，且 W-APN 并不是如 3GPP TS 23.003 中定义的用于应急情况，则结果代码将被设置为 DIAMETER_AUTHORIZATION_REJECTED（直径授权拒绝）。

当所有检查均成功时，3GPP AAA 服务器向 PDG 发送包括 EAP 成功以及密钥材料的认证应答。此密钥材料将包括在认证过程期间生成的主会话密钥（MSK）。当使用直径实现 Wm 接口（PDG-3GPP AAA 服务器）时，MSK 将封装在 EAP 主会话密钥参数中，如参考 RFC 4072（2005 年 8 月：“Diameter Extensible Authentication Protocol(EAP) Application（直径可扩展认证协议（EAP）应用）”）所定义。

在步骤 17 中，MSK 将由 PDG 使用来检查 AUTH 参数，以便认证 IKE_SA_INIT 阶段消息，如在参考 IETF RFC 4306 中所规定（2005 年 12 月：“Internet Key Exchange(IKEv2) Protocol（因特网密钥交换

（IKEv2）协议）”）。

在步骤 18 中，PDG 以其标识和证书做出响应。其还完成子安全性关联的协商。还将 EAP 成功消息转发至 WLAN UE。

在下文中，描述了可以如何形成用户标识（例如，在步骤 3 和 13 中使用）。

也即，如果针对无 UICC IMS 应急呼叫而向所有用户提供公共用户名/口令，则问题在于如何定义此类名/口令，并且如果某人故意进行虚假应急呼叫时，则根本无法基于公共名/口令追踪到它。

根据本实施方式，建议三种类型的标识用于无 UICC 的 UE：国际移动设备标识（IMEI）、介质访问控制（MAC）地址和 IP 地址。

具体地，在 3GPP 限制连接使得其应来自于移动终端（即，来自于可以向其中插入 SIM 卡的终端）的情况下，则应使用 IMEI 或者经哈希变换的 IMEI。可以以哈希形式使用 IMEI，这是由于 IMEI 的长度为 15 字节，这可能将不适合于所有的情况。IMEI 或者经哈希变换的 IMEI 继而可以用作在图 1 中步骤 3 和步骤 14 处的用户标识。

在此步骤使用经哈希变换的 IMEI 的优势在于，可以防止冒充。UE 可以在步骤 3 处使用经哈希变换的 IMEI，并且在步骤 14 处使用原始完整的 IMEI。从而即使攻击者可以窃听经哈希变换的 IMEI 并且使用其来开始另一应急呼叫，他可以获得合适的 IMEI 以便在步骤 14 处使用。如果 PDG 在步骤 14 处从攻击者接收了错误的 IMEI，则在 PDG 处将不生成正确的经哈希变换的 IMEI。也即，在步骤 3 中，当 EAP 响应/标识中包括经哈希变换的 IMEI 时，攻击者可以通过监听无线链路来获得此经哈希变换的 IMEI，并且在步骤 14 中可以使用其来攻击 PDG。因此，如果在步骤 14 中，在 AUTH 请求中使用未经哈希变换的完整 IMEI，则即使攻击者能够获得经哈希变换的 IMEI（在步骤 3）中，他/她也不能使用其来攻击 PDG，这是由于攻击者并不知晓完整的 IMEI。

备选的是，如果 3GPP 允许其他 WLAN UE（诸如 PDA 或者笔记本电脑）来进行 IMS 应急呼叫，则在步骤 3 和步骤 14 中，可以以

如下方式使用 MAC 地址:

1）MAC 地址。每个 WLAN UE 将具有唯一的 MAC 地址。

每个 WLAN UE 将具有唯一的 MAC 地址。ID 的长度是最短的。

2）MAC 地址 + WLAN AN ID（SSID）。

这可以提供应急呼叫的位置，以便知晓应急的位置，或者追踪到虚假呼叫。如果攻击者在相同 WLAN AN 中使用另一 MAC 地址，则其将被检测到。备选的是，可以使用经哈希变换的地址（MAC 地址 + WLAN AN ID（SSID））。

3）本地 IP 地址（由 WLAN AN 分配）+ WLAN AN ID（SSID）。

这可以提供应急呼叫的位置，以便可以追踪虚假呼叫。如果攻击者在相同 WLAN AN 中使用另一 IP 地址，则其将被检测到。备选的是，可以使用本地 IP 地址 + WLAN AN ID 地址的经哈希变换的组合。

当 UE 连接至 WLAN AN 而具有情况 2 连接时，在步骤 3 处可以使用用户标识符，例如“userID@sos.w-apn.mnc012.mcc345.pub.3gppnetwork.org”。也即，在初始消息（步骤 3）中，订户终端使用用户标识符。响应于此，AAA 服务器可以从 WLAN AN 获取 UE 的 MAC/IP 地址以及 WLAN AN 信息。由此，响应于此，在步骤 5 中，AAA 服务器可以从 MAC/IP（以及 WLAN AN 信息）形成用户 ID，而所述 MAC/IP（以及 WLAN AN 信息）是从 WLAN AN 接收到的。

当 UE 与 PDG 建立了情况 3 的连接时，由于在其 NAI 中的区域部分可以向 PDG 指示所述连接请求用于应急呼叫，并且其希望使用 IKEv2 上的 EAP，并且在 WLAN UE 和 AAA 服务器之间已经存在共享密钥（MSK），WLAN UE 可以生成 AUTH 参数并且将其发送至 PDG。PDG 可以从 AAA 服务器获取 MSK 以检查 AUTH。以此方式，在常规的情况 3 下，不需要更多的步骤。

由此，根据本实施方式，诸如可以略过客户端认证的 EAP-TLS 认证方法的认证方法用于在应急呼叫情况下由无 UICC 用户在

I-WLAN 中使用。

以此方式，仍然提供服务器认证。服务器认证支持在 WLAN UE 和 AAA 服务器之间生成共享 MSK 以便使用 IKE2 上的 EAP。

由此，认证仅用于服务器，而不用于客户端。因此，网络将不会拒绝应急呼叫（EM 呼叫）。认证具有两个目的。一个目的是保持 WLAN AN 不变。否则，WLAN AN 应检查 UE 的 NAI 以确定是否是 EM 呼叫。另一目的是，生成在情况 3 过程中使用的 MSK。

此外，如果 AAA 服务器不具有用于此终端的认证矢量，则可以建立到 PDG 的加密隧道（=无 UICC 情况）。也即，如上所述，可以在 UE 和 AAA 服务器中，如 RFC 4346 中所规定的从 TLS 主秘密生成 MSK。PDG 从 3GPP AAA 服务器获得 MSK。从而可以在 UE 和 PDG 之间建立加密的隧道。

在 WLAN AN 处不需要改变。AAA 服务器需要从 MAC/IP（以及 WLAN AN ID）形成用户 ID。

由此，在无 UICC 情况下，可以建立可靠的和经认证的连接。

在下文中，描述本发明的第二实施方式，其中考虑了攻击者可以开始双重应急呼叫的情况。

具体地，根据 TS 33.234，在情况 2 和情况 3 中允许同时会话（即，经由 IP 接入和 3GPP 接入），并且同时会话的数量基于运营商的策略。尤其是在 WLAN UE 分离的情况下，针对具有同时会话的请求是有效的。例如，用户可以使用其移动终端来访问运营商的网站，并且同时使用其笔记本电脑来接入到他公司的 VPN。

然而，当用户通过无 UICC 终端来进行 IMS 应急呼叫时（例如，如第一实施方式中所述），他不太可能进行同时的 IMS 应急呼叫。如果出现，则第二个呼叫可能是欺骗呼叫以及可能是针对应急服务的破坏行为。因此通过无 UICC 终端进行的同时 IMS 应急呼叫将被禁止。

根据本实施方式，在 PDG（即，用于应急呼叫的 W-APN，而不是 AAA 服务器）处执行相应的控制，这是由于 WLAN UE 可以不接

收 EAP 成功消息（在图 1 的步骤 12 处），并且不开始情况 3 的过程。

当 PDG 从 WLAN UE 接收请求时（步骤 14），其应该检查对于该用户是否已经存在会话。如果是的话，则将拒绝新的请求而不是接受该请求。基本原理在于，对于攻击者来说，难以事先知晓受害者的 ID，但是在 UE 建立情况 2 连接期间，可以对其进行拦截。

通过 UE ID，PDG 可以知晓其是无 UICC 的 IMS 应急呼叫。

由此，根据本分实施方式，可靠地检测和防止了双重应急呼叫。

在下文中，通过参考附图 2A 至 2D 描述上述实施方式中包括的网元。应该注意，在 2A 至 2D 中，仅示出了基本元素以便简化附图。

图 2A 示出了订户终端 A 的基础配置。订户终端 A 包括控制器 A1 和收发机 A2。控制器 A1 可以包括 CPU 以及不同类型的存储器单元，诸如 RAM、ROM 等等。计算机程序可以存储在存储器之中，并且可以包括用于实现根据本发明的方法的软件代码部分。所述计算机程序可以存储在记录介质（诸如，CD ROM）之上，并且可以直接加载至控制器的工作存储器中。备选的是，可以经由网络来将计算机程序加载至控制器的存储器之中。

图 2B 示出了 AAA 服务器 B 的基础配置，其包括控制器 B1 和收发机 B2。控制器 B1 以如控制器 A1 类似的方式配置。也即，控制器 B2 也包括 CPU 和不同类型的存储器介质，诸如 RAM、ROM、硬盘、CD 或者 DVD ROM 阅读器等。可以以上述类似方式向 AAA 服务器提供计算机程序。收发机 B2 可以包括一个或者多个接口，通过所述接口可以提供经由网络到其他网元的连接。

附图 2C 示出了 PDG C 的基础配置，其类似于 AAA 服务器 B 的配置，因此不再重复对其的描述。

图 2D 示出了 WLAN AN 的基础配置，其同样类似于 AAA 服务器 B 的配置，因此不再重复对其的描述。

本发明不局限于上述实施方式，并且各种变形均是可以的。

特别地，认证方法（或者认证过程）不限于 EAP-TLS。特别地，

可以使用其中可省略客户端认证的任何其他的适用方法。

此外，订户终端标识符不限于 IMEI。也即，可以使用唯一地标识终端的任何其他标识符。

此外，所包括的认证序列和网元不限于图 1 所示以及上文所述的细节。备选的是，如果需要，可以以不同顺序或通过包括更少或者更多的网元来执行不同的步骤。

此外，上述 IMS 应急呼叫仅仅是无 UICC 呼叫的示例。特别地，可能还存在其中允许无 UICC 呼叫的其他状况。例如，网络可以允许无 UICC 呼叫以便联系提供者的运营商。

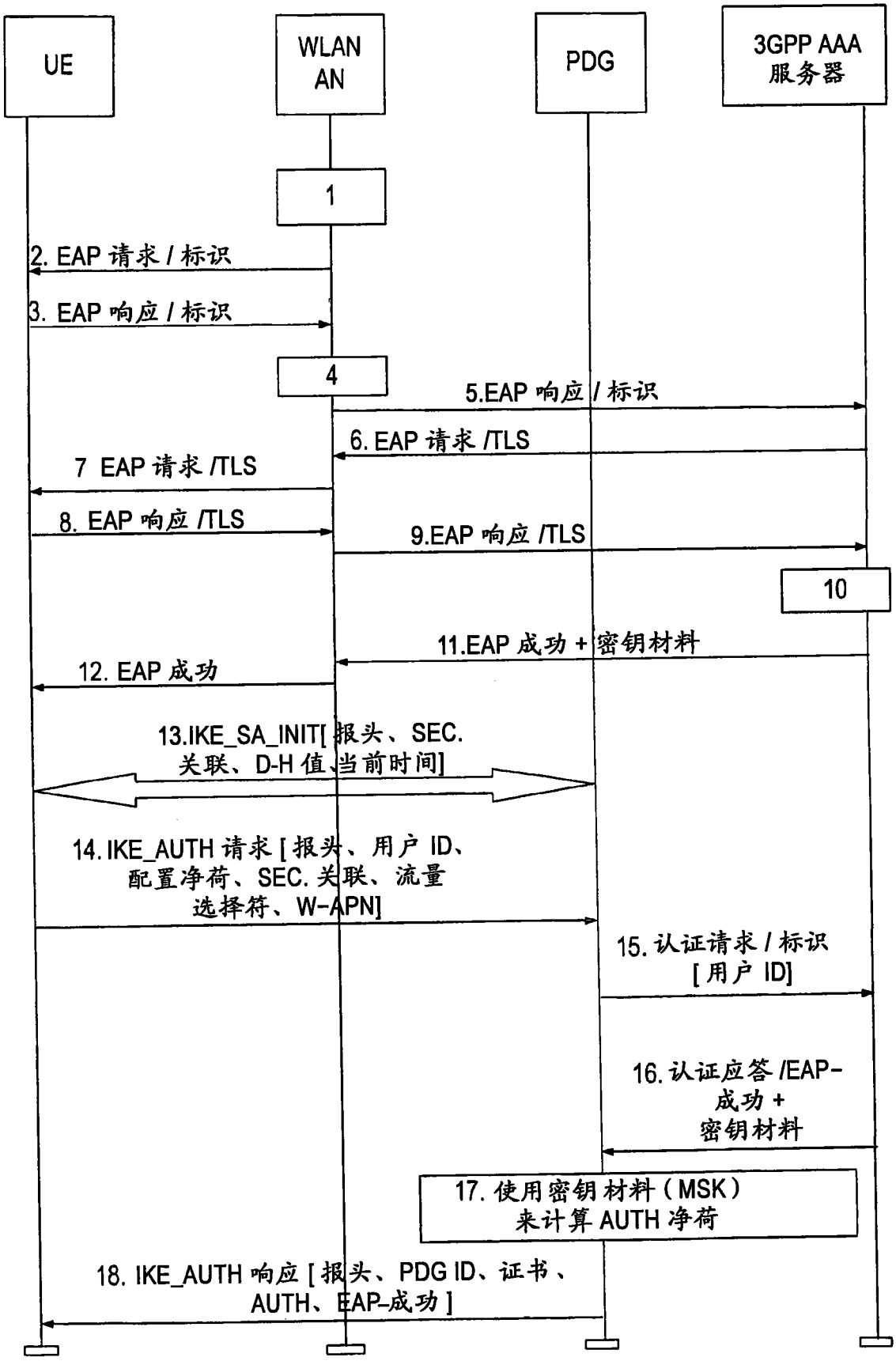

UE
WLAN AN
PDG
3GPP AAA 服务器
1
2. EAP 请求 / 标识
3. EAP 响应 / 标识
4
5.EAP 响应 / 标识
6. EAP 请求 /TLS
7 EAP 请求 /TLS
8. EAP 响应 /TLS
9.EAP 响应 /TLS
10
11.EAP 成功 + 密钥材料
12. EAP 成功
13.IKE_SA_INIT[报头、SEC. 关联、D-H 值、当前时间]
14. IKE_AUTH 请求 [报头、用户 ID、配置净荷、SEC. 关联、流量选择符、W-APN]
15. 认证请求 / 标识 [用户 ID]
16. 认证应答 /EAP-成功 + 密钥材料
17. 使用密钥材料 (MSK) 来计算 AUTH 净荷
18. IKE_AUTH 响应 [报头、PDG ID、证书、AUTH、EAP-成功]

图 1

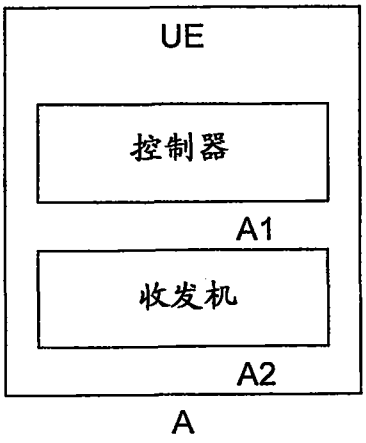


图 2A

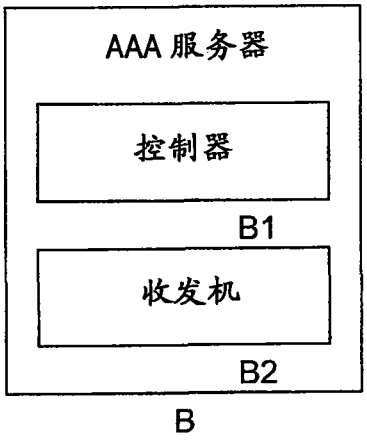


图 2B

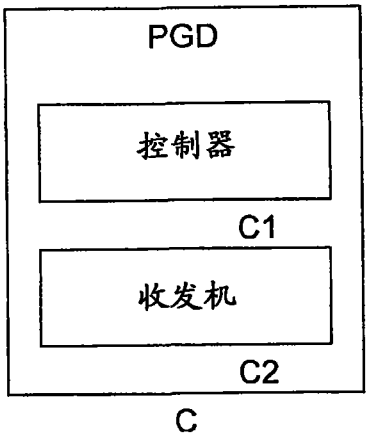


图 2C

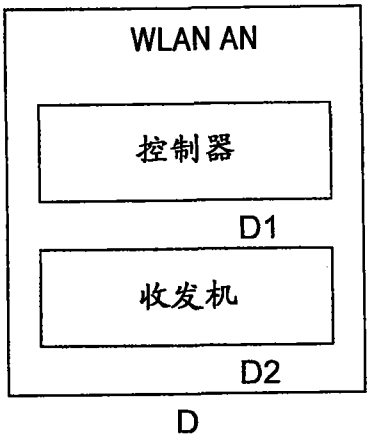


图 2D