



(12) 发明专利

(10) 授权公告号 CN 1697386 B

(45) 授权公告日 2010.04.07

(21) 申请号 200410044235.7

(22) 申请日 2004.05.14

(73) 专利权人 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 刘淑玲 刘廷永 尹瀚 冯凯锋

(74) 专利代理机构 北京德琦知识产权代理有限
公司 11018

代理人 王琦 程殿军

(51) Int. Cl.

H04L 12/14 (2006.01)

H04L 9/32 (2006.01)

(56) 对比文件

CN 1416072 A, 2003.05.07, 说明书第 2、3、
18、19 页。

CN 1490984 A, 2004.04.21, 全文。

WO 03092190 A1, 2003.11.06, 说明书第 4
页, 第 9 页, 第 14 页。

CN 1464682 A, 2003.12.31, 全文。

US 2003232615 A1, 2003.12.18, 全文。

审查员 彭锐

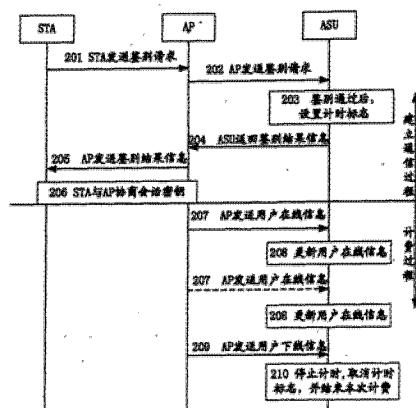
权利要求书 2 页 说明书 5 页 附图 2 页

(54) 发明名称

一种基于无线局域网鉴别与保密基础结构体
系的计费方法

(57) 摘要

本发明提供了一种基于无线局域网鉴别与保密基础结构体系的计费方法, 其关键是, 由颁发并保存有 STA 证书的 ASU 作为计费主体, 统计用户在线时间, 并根据在线时间对 STA 证书进行计费。进一步完善了 WAPI 体系。本发明保证了对 WAPI 体系中终端用户的较为精确的计时。而且, 即使某 STA 证书被恶意拦截复制并向 ASU 发送鉴别请求, ASU 也不会发生多收费的现象。另外, 当 AP 本身出现故障时, 比如死机时, ASU 也可以及时地结束对 STA 的本次计时, 从而停止计费。



1. 一种基于无线局域网鉴别与保密基础结构体系的计费方法，其特征在于，该方法包括以下步骤：

a、鉴别服务单元 ASU 接收到来自无线接入用户终端 STA 的鉴别请求，并对该 STA 鉴别成功后，根据保存的该 STA 的 STA 证书，对该 STA 证书设置计时标志，以记录该 STA 的已在线时间；

b、ASU 定时检测是否有来自访问接入点 AP 的 STA 在线信息，如果有，进一步检测该在线信息所指向的 STA 证书是否已设置计时标志，如果是，则 ASU 更新该 STA 的已在线时间信息，然后重复执行步骤 b，如果该在线信息所指向的 STA 证书没有设置计时标志，则认为该在线信息无效，忽略该在线信息，不做任何处理；如果没有来自 AP 的 STA 在线信息，则停止该 STA 已在线时间的计时操作，统计该 STA 的在线时间并根据该时间实现对 STA 证书计费。

2. 根据权利要求 1 所述的方法，其特征在于，步骤 b 所述当 ASU 在定时时间内没有检测到来自 AP 的 STA 在线信息时，该方法进一步包括：ASU 再次确认该 STA 是否在线，如果在线，则更新该 STA 的已在线时间信息，然后重复执行步骤 b，否则，停止该 STA 已在线时间的计时操作，统计该 STA 的在线时间并根据时间实现计费。

3. 根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：在 STA 下线时，AP 向 ASU 发送 STA 下线信息，ASU 接收到来自 AP 的 STA 下线信息后，停止该 STA 已在线时间的计时操作，统计该 STA 的在线时间并根据时间实现计费。

4. 根据权利要求 1、2 或 3 所述的方法，其特征在于，该方法进一步包括：

步骤 b 所述 ASU 停止对该 STA 已在线时间的计时操作后，取消本地保存的该 STA 证书的计时标志，然后再执行后续步骤。

5. 根据权利要求 3 所述的方法，其特征在于，所述 AP 向 ASU 发送的 STA 下线信息的方法是：AP 直接将 STA 下线信息发送给 ASU，或者，AP 对整个 STA 下线信息进行私钥签名，将签名后的下线信息发送给 ASU。

6. 根据权利要求 3 所述的方法，其特征在于，所述 STA 下线信息内至少包括：STA 证书中的用户名和序列号；或者，该 STA 下线信息内包括完整的 STA 证书和 AP 证书，以及 AP 对整个消息的私钥签名信息；或者，该下线信息内包括 STA 证书中的用户名称和序列号，AP 证书中的用户名称和序列号，以及 AP 对整个消息的私钥签名信息。

7. 根据权利要求 1 所述的方法，其特征在于，所述 STA 在线信息至少包括：STA 证书中的用户名和序列号。

8. 根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：

如果一个 STA 证书仅允许一个 STA 使用，则 ASU 对该 STA 鉴别成功后，且 ASU 更新了该 STA 的已在线时间后，在该 STA 证书用户下线之前，ASU 拒绝对同一 STA 证书的鉴别请求进行鉴别处理，并给 AP 发送鉴别失败；

如果一个 STA 证书允许一个以上 STA 同时使用，则 ASU 统计该 STA 的在线时间并根据该时间实现对 STA 证书计费包括：

ASU 对多个使用该 STA 证书的通信端口的使用该 STA 证书时间进行累加，实现对该 STA 证书的计费。

9. 根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：同级别的 ASU 之

间交换 STA 在线信息，或低级别的 ASU 将自身保存的 STA 在线信息发送给更高级别的 ASU。

一种基于无线局域网鉴别与保密基础结构体系的计费方法

技术领域

[0001] 本发明涉及无线局域网鉴别与保密基础结构 (WAPI) 体系技术领域, 特别是指一种基于 WAPI 体系的计费方法。

背景技术

[0002] 我国宽带无线 IP 标准工作组制定了无线局域网 (WLAN) 国家标准 GB/T15629.11, 推出了基于 WAPI 体系的安全方案, 该方案提供了一种基于公钥证书的无线局域网移动终端安全接入方法。

[0003] 在 WAPI 体系中, 有无线接入用户终端 (STA, Station), 访问接入点 (AP, Access Point) 和鉴别服务单元 (ASU, Authentication Service Unit) 三种实体, 分别作为鉴别请求者实体 (ASUE, Authentication Supplicant Entity), 鉴别器实体 (AE, Authentication Entity) 和鉴别服务实体 (ASE, Authentication Service Entity) 的载体。其中, ASUE 是通过鉴别服务单元进行鉴别的实体, 驻留在 STA 中; AE 为鉴别请求者在接入服务之前提供鉴别操作的实体, 驻留在 AP; ASE 为鉴别器和鉴别请求者提供相互鉴别的实体, 驻留在 ASU。

[0004] ASU 对其管理范围内的 AP 和 STA 进行管理并为每一个合法的 AP 和 STA 颁发一个公钥证书, 以作为网络设备在该 WLAN 内的数字身份凭证。该公钥证书中包括证书序列号以及用户名等信息, 其中, 颁发者 ASU 和序列号唯一标识了每个证书。同时, ASU 内也保存了 STA 证书和 AP 证书。STA 与 AP 之间通过 ASU 实现身份的相互鉴别。

[0005] 图 1 所示为基于 WAPI 体系的接入控制原理图。STA 通过 WLAN 从未受控端口向 AP 发出连接请求, AP 进一步封装该请求后发送给 ASU, 由 ASU 协助 AP 和 STA 进行相互身份认证, 即证书鉴别, 若认证成功, AP 开放受控端口允许 STA 接入, 且 STA 和 AP 之间进行密钥协商, 利用协商的会话密钥对数据进行加密和解密, 并进行数据通信; 若认证不成功, AP 拒绝 STA 接入或 STA 放弃接入 AP。

[0006] WAPI 体系提出了独特的鉴别方法和加密方法, 弥补了现有国际标准在安全性方面的缺陷, 提高了用户使用的安全可靠性。但同时, WAPI 在计费方面没有给出明确的方法, 而且也没有表明其可以支持的方法, 而在 WLAN 的实际应用中, 合理进行计费很有必要, 为了更好地实施 WAPI, 如何计费应该得到体现。

发明内容

[0007] 有鉴于此, 本发明的目的在于提供一种基于 WAPI 体系的计费方法, 进一步完善 WAPI 体系。

[0008] 为达到上述目的, 本发明的技术方案是这样实现的:

[0009] 一种基于无线局域网鉴别与保密基础结构体系的计费方法, 该方法包括以下步骤:

[0010] a、鉴别服务单元 ASU 接收到来自无线接入用户终端 STA 的鉴别请求, 并对该 STA 鉴别成功后, 根据保存的该 STA 的 STA 证书, 对该 STA 证书设置计时标志, 以记录

该 STA 的已在线时间；

[0011] b、ASU 定时检测是否有来自访问接入点 AP 的 STA 在线信息，如果有，进一步检测该在线信息所指向的 STA 证书是否已设置计时标志，如果是，则 ASU 更新该 STA 的已在线时间信息，然后重复执行步骤 b，如果该在线信息所指向的 STA 证书没有设置计时标志，则认为该在线信息无效，忽略该在线信息，不做任何处理；如果没有来自 AP 的 STA 在线信息，则停止该 STA 已在线时间的计时操作，统计该 STA 的在线时间并根据该时间实现对 STA 证书计费。

[0012] 较佳地，步骤 b 所述当 ASU 在定时时间内没有检测到来自 AP 的 STA 在线信息时，该方法进一步包括：ASU 再次确认该 STA 是否在线，如果在线，则更新该 STA 的已在线时间信息，然后重复执行步骤 b，否则，停止该 STA 已在线时间的计时操作，统计该 STA 的在线时间并根据时间实现计费。

[0013] 较佳地，该方法进一步包括：在 STA 下线时，AP 向 ASU 发送 STA 下线信息，ASU 接收到来自 AP 的 STA 下线信息后，停止该 STA 已在线时间的计时操作，统计该 STA 的在线时间并根据时间实现计费。

[0014] 较佳地，该方法进一步包括：

[0015] 步骤 b 所述 ASU 停止对该 STA 已在线时间的计时操作后，取消本地保存的该 STA 证书的计时标志，然后再执行后续步骤。

[0016] 较佳地，所述 AP 向 ASU 发送的 STA 下线信息的方法是：AP 直接将 STA 下线信息发送给 ASU，或者，AP 对整个 STA 下线信息进行私钥签名，将签名后的下线信息发送给 ASU。

[0017] 较佳地，所述 STA 下线信息内至少包括：STA 证书中的用户名和序列号；或者，该 STA 下线信息内包括完整的 STA 证书和 AP 证书，以及 AP 对整个消息的私钥签名信息；或者，下线信息内包括 STA 证书中的用户名称和序列号，AP 证书中的用户名称和序列号，以及 AP 对整个消息的私钥签名信息。

[0018] 较佳地，所述 STA 在线信息至少包括：STA 证书中的用户名和序列号。

[0019] 较佳地，该方法进一步包括：如果一个 STA 证书仅允许一个 STA 使用，则 ASU 对该 STA 鉴别成功后，且 ASU 更新了该 STA 的已在线时间后，在该 STA 证书用户下线之前，ASU 拒绝对同一 STA 证书的鉴别请求进行鉴别处理，并给 AP 发送鉴别失败；如果一个 STA 证书允许一个以上 STA 同时使用，则 ASU 统计该 STA 的在线时间并根据该时间实现对 STA 证书计费包括：

[0020] ASU 对多个使用该 STA 证书的通信端口的使用该 STA 证书时间进行累加，实现对该 STA 证书的计费。

[0021] 较佳地，该方法进一步包括：同级别的 ASU 之间交换 STA 在线信息，或低级别的 ASU 将自身保存的 STA 在线信息发送给更高级别的 ASU。

[0022] 本发明由颁发并保存有 STA 证书的 ASU 作为计费主体，统计用户在线时间，并根据在线时间对 STA 证书进行计费。进一步完善了 WAPI 体系。

[0023] 本发明保证了对 WAPI 体系中终端用户的较为精确的计时。即使某 STA 证书被恶意拦截复制并向 ASU 发送鉴别请求，ASU 也不会发生多收费的现象。因为即便这样的证书通过鉴别，由于没有用户私钥，其无法和 AP 进行有效的会话密钥协商，因而 AP 不

会向 ASU 发送 STA 在线信息。另外，当 AP 本身出现故障时，比如死机时，由于 AP 无法向 ASU 发送在线信息，因而 ASU 在定时时间内也就无法收到 STA 在线信息，这样，ASU 可以及时地结束对 STA 的本次计时，从而停止计费。

[0024] 在授权许可下，同级别的 ASU 之间可以交换 STA 在线信息，或者，低级别的 ASU 将自身保存的 STA 在线信息发送给更高级别的 ASU，使高级别的 ASU 进行有效的计费管理，方便用户查询。这一点，对于联网的运营项目，比如一些联网的酒店是很有必要的。

附图说明

[0025] 图 1 所示为基于 WAPI 体系的接入控制原理图；

[0026] 图 2 所示为应用本发明的 ASU 实现计费的流程示意图。

具体实施方式

[0027] 为使本发明的技术方案更加清楚，下面结合附图对本发明再做进一步地详细说明。

[0028] 本发明的思路是：由颁发并保存有 STA 证书的 ASU 作为计费主体，统计用户在线时间，并根据在线时间对 STA 证书进行计费。

[0029] 图 2 所示为应用本发明的 ASU 实现计费的流程示意图。

[0030] 步骤 201，STA 向 AP 发送鉴别请求消息；

[0031] 步骤 202，AP 将该鉴别请求消息发送给 ASU；

[0032] 步骤 203，ASU 协助 AP 和 STA 进行身份互认证，即证书鉴别，认证成功后，针对本地保存的该 STA 证书设置计时标志，根据该 STA 证书开始记录该 STA 的已在线时间信息，开始记录时通常为 0 分钟；

[0033] 步骤 204，ASU 将鉴别成功的结果信息发送给 AP；

[0034] 步骤 205，AP 将鉴别成功的结果信息发送给 STA；

[0035] 步骤 206，STA 与 AP 之间协商会话密钥，并利用协商的会话密钥对数据进行加解密，进行数据通信；

[0036] 步骤 207，当 AP 开始与 STA 之间进行有效通信，即 AP 与 STA 的会话密钥协商完毕，STA 通过受控端口与 AP 开始数据通信之后，AP 定时向 ASU 发送该 STA 证书的在线信息，也就是该 STA 的在线信息；

[0037] 上述在线信息中至少需要包括 STA 证书的用户名和序列号，且该信息的发送频率和 ASU 的计时单位要相匹配，如每分钟发送一次，以支持 ASU 能够较为精确地计算该用户的在线时间；

[0038] 步骤 208，在 AP 定时向 ASU 发送 STA 在线信息的同时，ASU 也定时检测是否有 AP 发送来的 STA 在线信息，如果检测到，则 ASU 进一步检测该在线信息所指向的 STA 证书是否已设置计时标志，如果是，则更新该 STA 证书的已在线时间信息，如果 ASU 发现检测所指向的 STA 证书没有设置计时标志，则认为该信息无效，并忽略该信息，不做任何处理；这样可以防止由于 AP 运行错误，或者发生了被攻击等情况而对用户进行错误收费；

[0039] 如果 ASU 没有检测到来自 AP 的 STA 在线信息，为了防止 AP 和 ASU 之间偶然发生的通信障碍干扰，ASU 再次确认该 STA 是否在线，例如，通过重复检测来确认该 STA 是否确实不在线，如果确实不在线，则直接执行步骤 210；如果该 STA 还在线，则更新该 STA 的已在线时间信息，并且继续定时检测是否有 AP 发送来的 STA 在线信息；该定时检测的时间同样需要与计时时间相匹配；

[0040] 步骤 209，为了更好地配合 ASU 的计费，在用户下线的时，AP 可以向 ASU 发送 STA 下线的信息，该下线信息可以由 AP 直接发送给 ASU，也可以由 AP 对整个下线信息进行私钥签名，将签名后的下线信息发送给 ASU，ASU 接收到该信息后直接执行步骤 210；

[0041] 上述下线信息内至少包含 STA 证书中的用户名称和序列号，如果需要对下线信息进行私钥签名，则下线信息内包括完整的 STA 证书和 AP 证书，以及 AP 对整个消息的私钥签名；或者，下线信息内包括 STA 证书中的用户名称和序列号，AP 证书中的用户名称和序列号，以及 AP 对整个消息的私钥签名；

[0042] 步骤 210，停止该 STA 已在线时间的计时操作，清除该 STA 证书的计时标志，用户下线时间以首次没有检测到 STA 在线信息的时间为准，统计该 STA 的在线时间并根据该时间实现对 STA 证书计费。

[0043] 由于 WLAN 采用无连接的通信方式，可能发生用户没有收到，或者不能及时收到鉴别结果信息的情况，因此，WAPI 允许一个用户证书多次发送鉴别请求。如果一个证书仅允许一个 STA 使用，则在 ASU 鉴别该证书成功之后，且设置了该 STA 证书的计时标志并开始计时，在 ASU 没有收到来自 AP 的 STA 在线信息之前，仍然可以为相同 STA 证书的鉴别请求进行鉴别处理，此时设置的计时标志不变；但是当 ASU 已经获取了 STA 的在线信息，即更新了 STA 的已在线时间后，在该证书用户下线之前，ASU 拒绝对同一 STA 证书的鉴别请求进行鉴别处理，并给 AP 发送鉴别失败；如果允许一个以上 STA 使用同一个证书，则当同一个证书被多个端口同时使用时，ASU 可以通过累加多个端口的使用时间进行计费。

[0044] 当一个以上 STA 使用同一个证书时，ASU 通过累加多个端口的使用时间进行计费的实现方法，说明如下：

[0045] 当系统允许一个以上 STA 使用同一个证书时，AP 定时向 ASU 发送该 STA 的在线信息中，不仅包括 STA 证书的用户名和序列号，还包括标识 AP 与 STA 通信的参数信息，该参数信息包括 AP 证书的用户名和序列号，通信受控端口的逻辑端口标识等；

[0046] ASU 定时检测到来自 AP 的在线信息后，进一步判断该在线信息中标识 AP 与 STA 通信的参数信息是否与本地已保存的标识 AP 与 STA 通信的参数信息相匹配，如果是，则更新该相匹配 STA 的已在线时间，如果不匹配，则保存该接收到的标识 AP 与 STA 通信的参数信息，以此区别相同证书的不同使用终端，并对该终端开始计时。

[0047] 当 AP 向 ASU 发送下线信息时，该下线信息中除了包括 STA 证书的用户名和序列号，还包括标识 AP 与 STA 通信的参数信息；当 ASU 收到来自 AP 的下线信息后，在所有 AP 与该 STA 通信的参数信息中匹配，查询与之相对的端口，结束对该 STA 证书使用的相应通信端口的计费。

[0048] 最后，由 ASU 将所有使用同一 STA 证书的 STA 的在线时间相加，得到针对该

STA 证书的累计时间，并根据该时间对 STA 证书实现计费。

[0049] 在授权许可下，同级别的 ASU 之间可以交换 STA 在线信息，或者，低级别的 ASU 将自身保存的 STA 在线信息发送给更高级别的 ASU，使高级别的 ASU 进行有效的计费管理，方便用户查询。这一点，对于联网的运营项目，比如一些联网的酒店是很有必要的。

[0050] 本发明保证了对 WAPI 体系中终端用户的较为精确的计时。即使某 STA 证书被恶意拦截复制并向 ASU 发送鉴别请求，ASU 也不会发生多收费的现象。因为即便这样的证书通过鉴别，由于没有用户私钥，其无法和 AP 进行有效的会话密钥协商，因而 AP 不会向 ASU 发送 STA 在线信息。

[0051] 另外，当 AP 本身出现故障时，比如死机时，由于 AP 无法向 ASU 发送在线信息，因而 ASU 在定时时间内也就无法收到 STA 在线信息，这样，ASU 可以及时地结束对 STA 的本次计时，从而停止计费。

[0052] 再有，由于 STA 和 AP 的密钥协商时间相对于计时单位而言很短，一般密钥协商过程最多为几秒，而如果 AP 和 STA 密钥协商失败，则 ASU 对 STA 的在线计时为 0 分钟，因此，不会发生多计时的情况，因而也就不会多计费。

[0053] WAPI 的安全体系可以方便地应用在酒店，网吧，图书馆等公共场所。ASU 对于使用了资源的 STA，根据其在线时间长度进行合理地收费。例如，当一顾客入住酒店后，酒店利用自己的 WAPI 安全设备对用户提供免费无线上网服务，即产生公钥证书并颁发给用户，同时，采用本发明的方法对用户进行在线计时，在用户离开酒店时，结算相关费用。

[0054] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

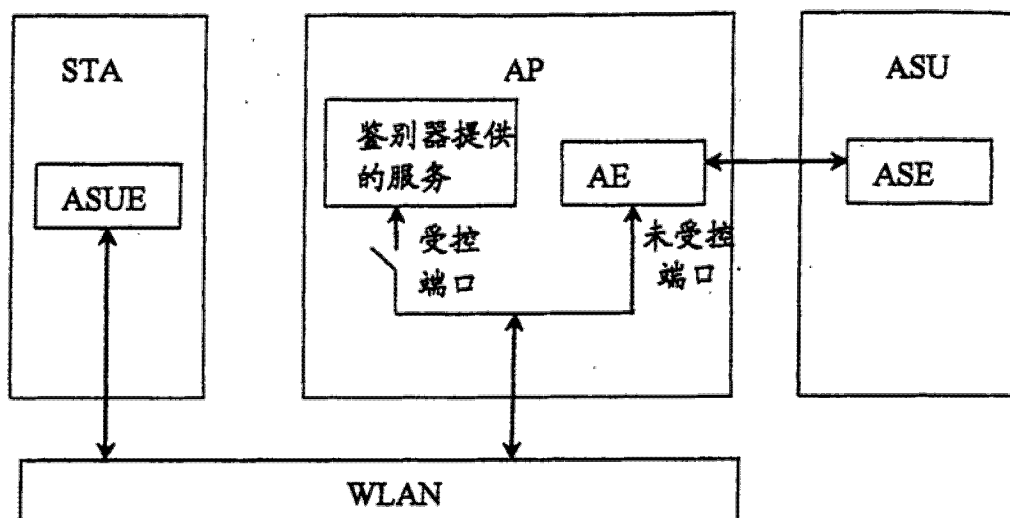


图 1

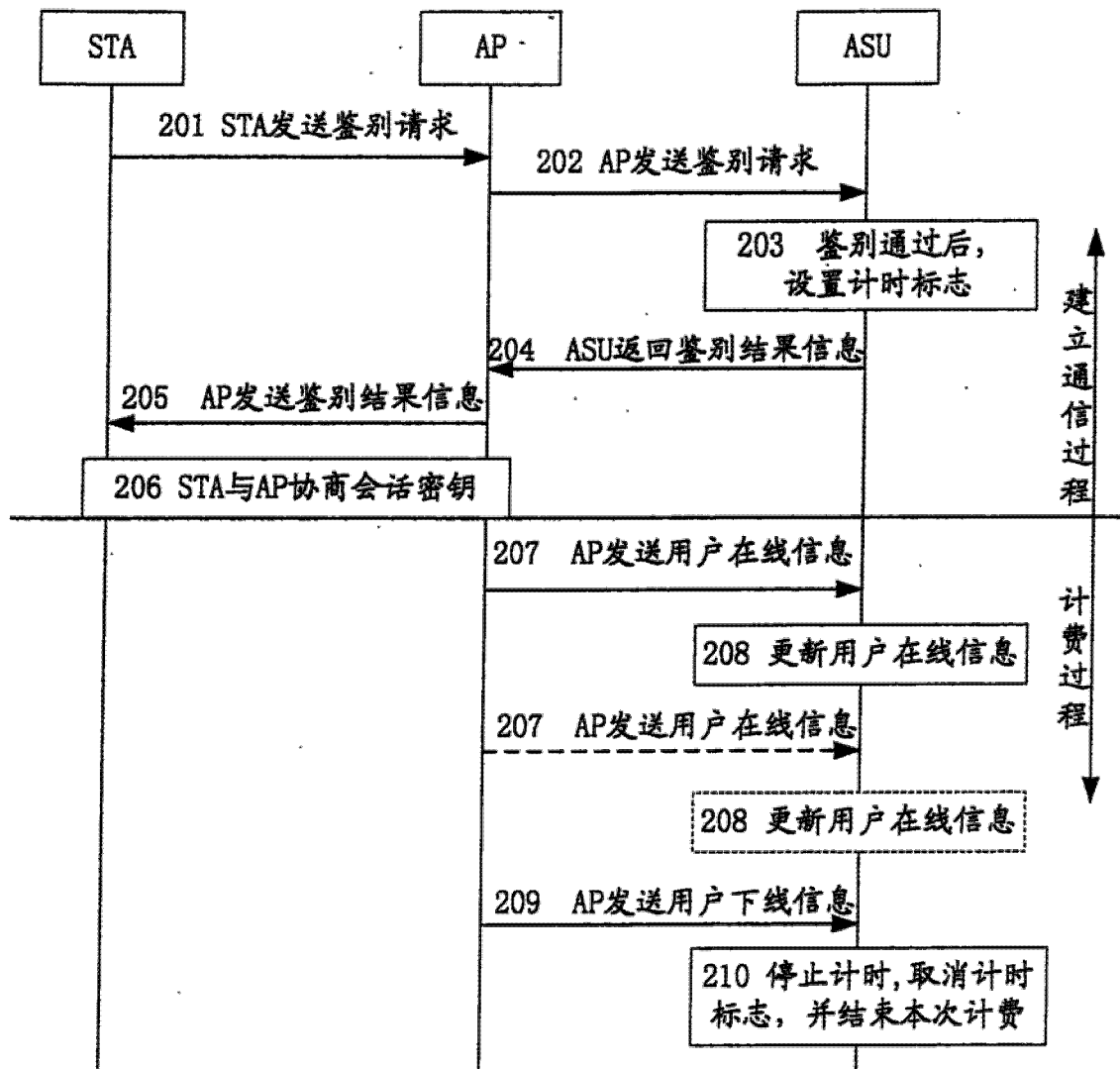


图 2