



(12) 发明专利申请

(10) 申请公布号 CN 102014384 A

(43) 申请公布日 2011.04.13

(21) 申请号 200910189965.9

(22) 申请日 2009.09.04

(71) 申请人 黄金富

地址 100032 北京市西城区金融街 27 号投  
资广场 B 座 19 层

(72) 发明人 黄金富

(51) Int. Cl.

H04W 12/04 (2009.01)

H04W 12/06 (2009.01)

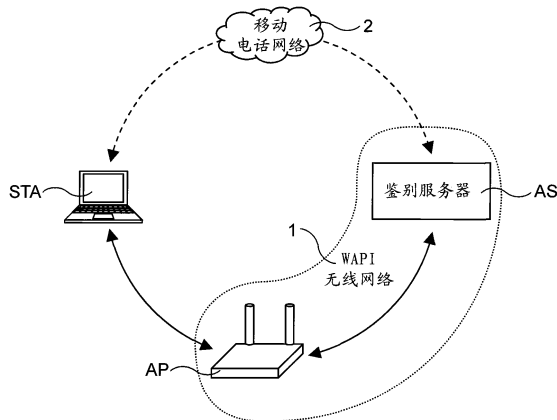
权利要求书 1 页 说明书 3 页 附图 1 页

(54) 发明名称

通过移动电话网络验证 WAPI 无线网络终端身份的方法

(57) 摘要

一种通过移动电话网络验证 WAPI 无线网络终端身份的方法,在无线终端 (STA) 上设置用于验证身份的数字证书和 WAPI 无线网络装置及移动电话上网装置, WAPI 无线网络 (1) 与无线终端 (STA) 互相鉴别验证对方身份时,除了通过 WAPI 无线网络 (1) 传送身份信息外,还通过移动电话网络传送身份信息,并在核对两者所传送的信息均无误后,才确认鉴别验证身份成功。通过本发明的方法鉴别验证无线终端 (STA) 和 WAPI 无线网络 (1) 双方身份,即使黑客盗取了无线终端 (STA) 内的数字证书,也无法使用该数字证书假冒用户接入 WAPI 无线网络 (1),使无线终端 (STA) 和 WAPI 无线网络 (1) 鉴别验证对方的身份更安全可靠。



1. 一种通过移动电话网络验证 WAPI 无线网络终端身份的方法，在无线终端 (STA) 上设置用于验证身份的数字证书和 WAPI 无线网络装置及移动电话上网装置，其特征在于，所述的方法于无线终端 (STA) 与 WAPI 无线网络 (1) 的进行身份鉴别时，采用包括如下步骤：

无线终端 (STA) 将包含数字证书的接入鉴别请求信息传送给无线接入点 (AP)，然后无线接入点 (AP) 将包含该接入鉴别请求信息的证书鉴别请求信息传送到鉴别服务器 (AS) 请求鉴别，以及，无线终端 (STA) 同时将该接入鉴别请求信息通过移动电话网络 (2) 传送到鉴别服务器 (AS) 请求鉴别；

鉴别服务器 (AS) 分别鉴别验证从无线接入点 (AP) 传来的证书鉴别请求信息和从移动电话网络 (2) 传来的接入鉴别请求信息，两者均鉴别验证无误后鉴别服务器 (AS) 将包含鉴别结果的证书鉴别响应信息传送给无线接入点 (AP) 和将该证书鉴别响应信息通过移动电话网络 (2) 传送给无线终端 (STA)，无线接入点 (AP) 核对该鉴别结果无误后将该证书鉴别响应信息传送到无线终端 (STA) 和允许该无线终端 (STA) 接入；

无线终端 (STA) 分别核对从无线接入点 (AP) 传来的证书鉴别响应信息中的鉴别结果和从移动电话网络 (2) 传来的证书鉴别响应信息中的鉴别结果，核对两者均无误后才接入该无线接入点 (AP)。

2. 如权利要求 1 所述的通过移动电话网络验证 WAPI 无线网络终端身份的方法，其特征在于，所述的无线终端 (STA) 是笔记本型计算机。

3. 如权利要求 1 所述的通过移动电话网络验证 WAPI 无线网络终端身份的方法，其特征在于，所述的无线终端 (STA) 是手机。

4. 如权利要求 1 所述的通过移动电话网络验证 WAPI 无线网络终端身份的方法，其特征在于，所述的移动电话网络 (2) 是 TD-SCDMA 移动电话网络。

## 通过移动电话网络验证 WAPI 无线网络终端身份的方法

### 【技术领域】

[0001] 本发明涉及网络安全技术，特别是涉及一种通过移动电话网络验证 WAPI 无线网络终端身份的方法。

### 【背景技术】

[0002] 随着我国的 TD-SCDMA 移动电话即 3G 移动电话服务推出，3G 移动电话网络的覆盖范围包括了各大小城市和乡镇，同时 3G 移动电话网络的营运商在全国各地也设置了大量的 WAPI 无线网络热点，为用户提供方便快捷的无线上网服务，所以越来越多计算机配置有 3G 移动电话上网装置和 WAPI 无线网络装置，在一些设置了 WAPI 无线网络热点位置，计算机可以采用廉价通讯收费的 WAPI 无线网络上网，而在一些没有 WAPI 无线网络热点的地方，计算机可以采用覆盖范围广阔的 TD-SCDMA 上网。目前，通过 WAPI 无线网络上网的终端，是通过终端内的数字证书作为上网身份的凭证，虽然 WAPI 无线网络至今还未被发现安全漏洞，但是储存在终端内作为身份凭证的数字证书却有可能被黑客通过病毒或木马程式等种种手段盗取，然后黑客以盗取回来的数字证书假冒用户，令用户蒙受损失。本发明通过采用双重验证身份方式，在 WAPI 无线网络与用户的无线终端互相鉴别验证对方身份时，除了通过 WAPI 无线网络传送验证身份信息外，还通过 3G 移动电话网络传送验证身份信息，并核对两者所传送的验证身份信息均无误后，才确认鉴别验证身份成功。

### 【发明内容】

[0003] 本发明的目的，在于提供一种通过移动电话网络验证 WAPI 无线网络终端身份的方法，以实现在 WAPI 无线网络中鉴别验证身份的应用。

[0004] 本发明的目的是这样实现的，采用这样一种通过移动电话网络验证 WAPI 无线网络终端身份的方法，在无线终端 (STA) 上设置用于验证身份的数字证书和 WAPI 无线网络装置及移动电话上网装置，其特征在于，所述的方法于无线终端 (STA) 与 WAPI 无线网络 (1) 的进行身份鉴别时，采用包括如下步骤：

[0005] 无线终端 (STA) 将包含数字证书的接入鉴别请求信息传送给无线接入点 (AP)，然后无线接入点 (AP) 将包含该接入鉴别请求信息的证书鉴别请求信息传送到鉴别服务器 (AS) 请求鉴别，以及，无线终端 (STA) 同时将该接入鉴别请求信息通过移动电话网络 (2) 传送到鉴别服务器 (AS) 请求鉴别；

[0006] 鉴别服务器 (AS) 分别鉴别验证从无线接入点 (AP) 传来的证书鉴别请求信息和从移动电话网络 (2) 传来的接入鉴别请求信息，两者均鉴别验证无误后鉴别服务器 (AS) 将包含鉴别结果的证书鉴别响应信息传送给无线接入点 (AP) 和将该证书鉴别响应信息通过移动电话网络 (2) 传送给无线终端 (STA)，无线接入点 (AP) 核对该鉴别结果无误后将该证书鉴别响应信息传送到无线终端 (STA) 和允许该无线终端 (STA) 接入；

[0007] 无线终端 (STA) 分别核对从无线接入点 (AP) 传来的证书鉴别响应信息中的鉴别

结果和从移动电话网络 (2) 传来的证书鉴别响应信息中的鉴别结果, 核对两者均无误后才接入该无线接入点 (AP)。

[0008] 在本说明书中, 设置在无线终端 (STA) 中的移动电话上网装置内插有一 SIM 卡, 该 SIM 卡就是移动电话上网装置连接到移动电话网络 (2) 的身份凭证, 无线终端 (STA) 除了以数字证书作为其连接到 WAPI 无线网络 (1) 的身份凭证外, 还需要以该 SIM 卡作为其连接到移动电话网络 (2) 的身份凭证, 才能通过移动电话网络 (2) 传送验证身份信息, 无线终端 (STA) 和 WAPI 无线网络 (1) 才能成功互相鉴别验证对方的身份。

[0009] 这样就实现了本发明的目的。

[0010] 通过本发明的方法验证无线终端 (STA) 和 WAPI 无线网络 (1) 双方的身份, 即使用户的无线终端 (STA) 内的数字证书被黑客盗取了, 没有用户的移动电话上网装置, 黑客无法使用盗取回来的数字证书假冒用户接入 WAPI 无线网络 (1), 使无线终端 (STA) 和 WAPI 无线网络 (1) 验证对方的身份更安全可靠。

### 【附图说明】

[0011] 图 1 是本发明的通过移动电话网络验证 WAPI 无线网络终端身份的方法的示意说明图;

[0012] 图 2 是将本发明的方法应用于移动电话的实施例的示意说明图。

[0013] 附图是示意性的, 用以说明本发明的构成和主要特征。

### 【具体实施方式】

[0014] 下面结合附图, 对本发明的方法作进一步详细说明。

[0015] 参阅图 1, 图 1 是本发明的通过移动电话网络验证 WAPI 无线网络终端身份的方法的示意说明图, 图 1 示出的包括有 WAPI 无线网络 (1)、移动电话网络 (2)、无线终端 (STA)、无线接入点 (AP)、鉴别服务器 (AS), 其中, 带箭头的实线示出了 WAPI 无线网络 (1) 与无线终端 (STA) 鉴别验证双方身份信息的流动方向, 这鉴别验证双方身份信息就是 WAPI 无线网络标准中的鉴别身份的信息, 而带箭头的虚线示出了通过移动电话网络 (2) 传送鉴别验证双方身份信息的流动方向, 这虚线部份是本发明的主要特征之一, 通过两条不同的路径传送鉴别验证身份的信息, 可以更安全可靠地鉴别验证双方的身份。

[0016] 继续参阅图 1, 图 1 示出的无线终端 (STA) 上设置有用于验证身份的数字证书和 WAPI 无线网络装置及移动电话上网装置, 移动电话上网装置内插有 SIM 卡, 移动电话上网装置以该 SIM 卡的身份接入移动电话网络 (2)。在本发明的方法中, 无线终端 (STA) 与 WAPI 无线网络 (1) 的进行身份鉴别时, 采用包括如下步骤:

[0017] 无线终端 (STA) 将包含数字证书的接入鉴别请求信息传送给无线接入点 (AP), 然后无线接入点 (AP) 将包含该接入鉴别请求信息的证书鉴别请求信息传送到鉴别服务器 (AS) 请求鉴别, 以及, 无线终端 (STA) 同时将该接入鉴别请求信息通过移动电话网络 (2) 传送到鉴别服务器 (AS) 请求鉴别;

[0018] 鉴别服务器 (AS) 分别鉴别验证从无线接入点 (AP) 传来的证书鉴别请求信息和从移动电话网络 (2) 传来的接入鉴别请求信息, 两者均鉴别验证无误后鉴别服务器 (AS) 将包含鉴别结果的证书鉴别响应信息传送给无线接入点 (AP) 和将该证书鉴别响应信息通

过移动电话网络 (2) 传送给无线终端 (STA)，无线接入点 (AP) 核对该鉴别结果无误后将该证书鉴别响应信息传送到无线终端 (STA) 和允许该无线终端 (STA) 接入；

[0019] 无线终端 (STA) 分别核对从无线接入点 (AP) 传来的证书鉴别响应信息中的鉴别结果和从移动电话网络 (2) 传来的证书鉴别响应信息中的鉴别结果，核对两者均无误后才接入该无线接入点 (AP)。

[0020] 参阅图 2，图 2 是将本发明的方法应用于移动电话的实施例的示意说明图，与图 1 相比，主要不同之处在于图 1 示出的无线终端 (STA) 是笔记本型计算机，而图 2 示出的无线终端 (STA) 是手机。在本发明中，无线终端 (STA) 可以是笔记本型计算机、或 PDA、或手机、或台式计算机等设备。此外，在本说明书中所述的移动电话网络 (2) 是 TD-SCDMA 移动电话网络，也可以是采用其他标准的移动电话网络，例如 GSM、CDMA、3G、4G 等移动电话网络，都可很好地实现本发明的目的，都是属于本发明的保护范围。

[0021] 以上已经说明了本发明的方法的主要特征，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。

[0022] 本发明的通过移动电话网络验证 WAPI 无线网络终端身份的方法，可以使无线终端 (STA) 和 WAPI 无线网络 (1) 鉴别验证对方的身份更安全可靠，它的实施，可有效提高 WAPI 无线网络 (1) 的安全性。

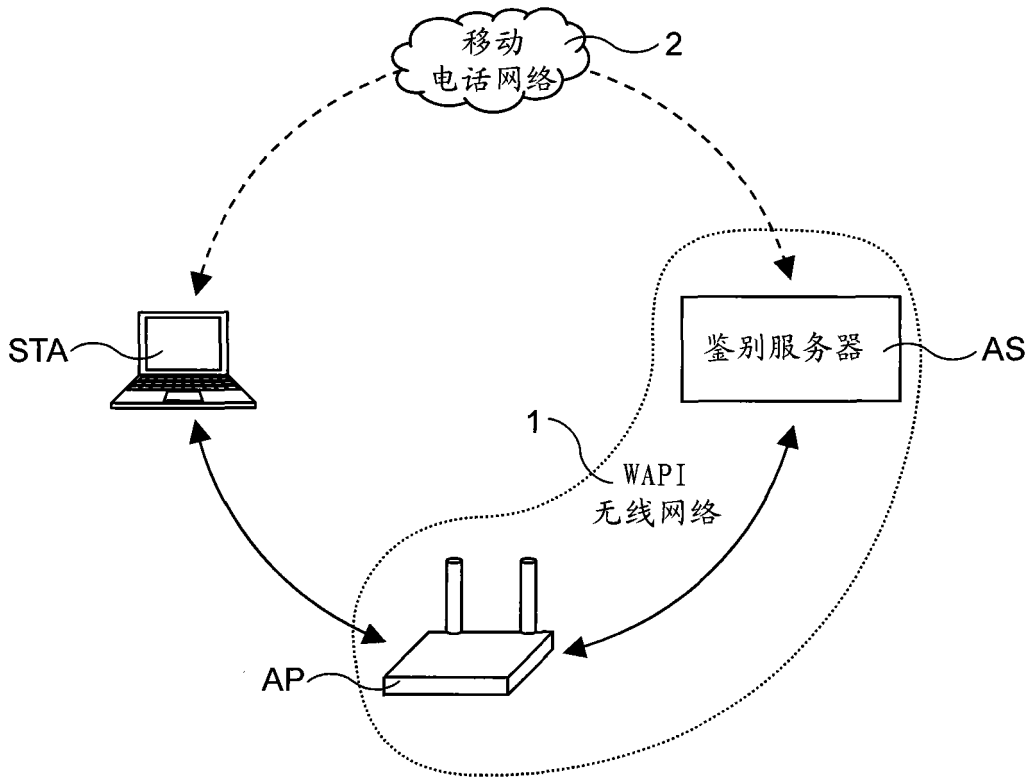


图 1

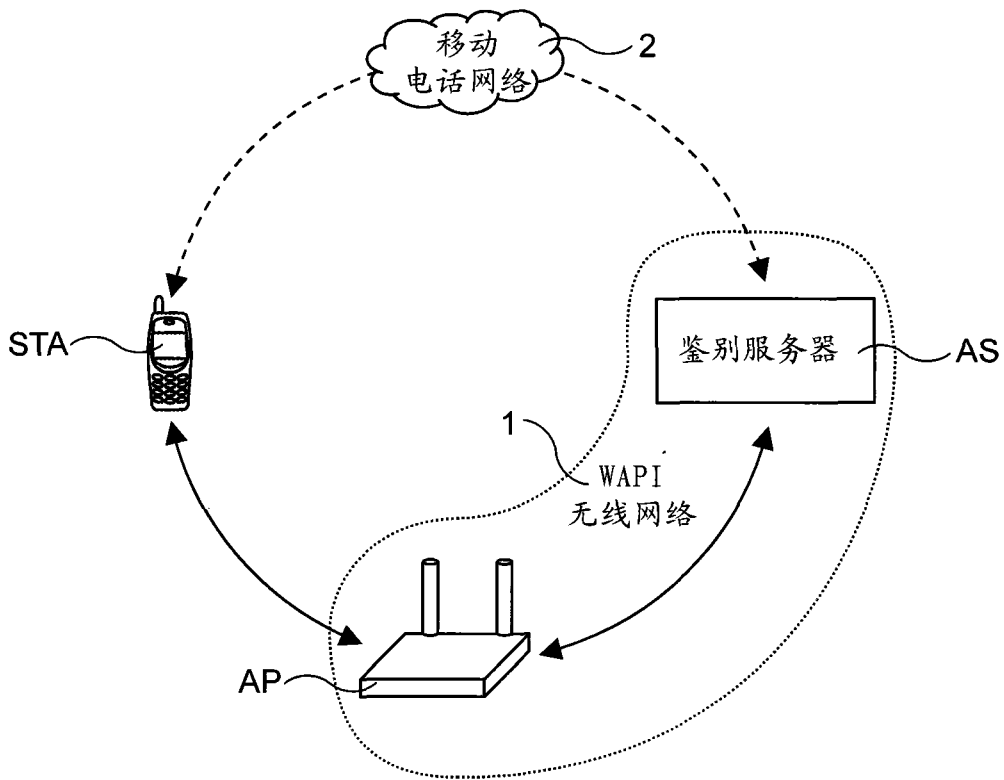


图 2