[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 12/56 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580049552.0

[43] 公开日 2008 年 4 月 23 日

[11] 公开号 CN 101167328A

[22] 申请日 2005.4.22
[21] 申请号 200580049552.0
[86] 国际申请 PCT/US2005/013712 2005.4.22
[87] 国际公布 WO2006/115479 英 2006.11.2
[85] 进入国家阶段日期 2007.10.22
[71] 申请人 汤姆森特许公司
地址 法国布洛涅
[72] 发明人 索拉布·马瑟 张俊彪

[74] 专利代理机构 北京市柳沈律师事务所
代理人 史新宏 吕晓章

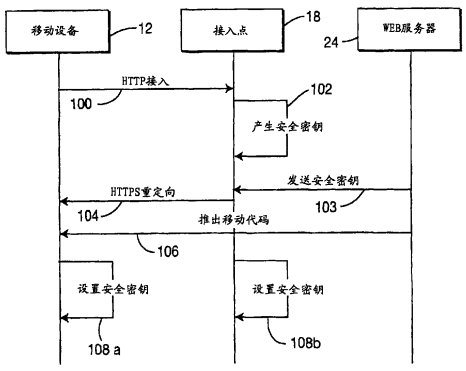
权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称

安全的匿名无线局域网(WLAN)接入机制

[57] 摘要

描述了一种用于对无线局域网提供安全、匿名接入的方法和系统，包括：配置接入点(18)来丢弃除了呈现 HTTP/HTTPS 协议的分组之外的分组，由接入点(18)经由浏览器从移动设备(12)截获 HTTP 接入请求，由接入点(18)将 HTTP 接入请求(100)重定向到 web 服务器(24)，由接入点(18)和 web 服务器(24)的一个产生安全密钥(102)，由接入点(18)将产生的安全密钥(103)安全地交换给所述 web 服务器，或者反之，以及由接入点设置安全密钥(108b)。 还描述了一种移动设备(12)，包括：用于经由 HTTP 接入请求(100)转发供安全接入无线局域网的请求的装置，用于接收移动代码(106)或者供显示安全密钥的信号的装置，和用于设置安全密钥(108a)的装置。



1. 一种用于提供对无线局域网的安全、匿名接入的方法，所述方法包括：

配置接入点来丢弃除了呈现 HTTP/HTTPS 协议的分组之外的分组；

所述接入点经由 web 浏览器从移动设备截获 HTTP 接入请求；

所述接入点将所述 HTTP 接入请求重定向到 web 服务器；

所述接入点和所述 web 服务器之一产生安全密钥；

所述接入点将产生的安全密钥安全地与所述 web 服务器交换，或者所述 web 服务器将产生的安全密钥安全地与所述接入点交换；和

所述接入点设置所述产生的安全密钥。

2. 根据权利要求 1 的方法，进一步包括由所述移动设备接收移动代码。

3. 根据权利要求 1 的方法，进一步包括在会话的持续时间中使用所述产生的安全密钥安全地通信。

4. 根据权利要求 1 的方法，其中使用分组过滤器来标识 HTTP/HTTPS 分组。

5. 根据权利要求 1 的方法，其中所述产生的安全密钥是有线等效保密密钥。

6. 根据权利要求 1 的方法，其中所述 web 服务器驻留在所述接入点上。

7. 根据权利要求 1 的方法，进一步包括由所述移动设备设置所述产生的安全密钥。

8. 一种用于提供对无线局域网的安全、匿名接入的系统，包括：

用于配置接入点来丢弃除了呈现 HTTP/HTTPS 协议的分组之外的分组的装置；

用于由所述接入点经由 web 浏览器从移动设备截取 HTTP 接入请求的装置；

用于由所述接入点将所述 HTTP 接入请求重定向到 web 服务器的装置；

用于由所述接入点产生安全密钥的装置；和

用于由所述接入点设置所述产生的安全密钥的装置。

9. 根据权利要求 8 的系统，进一步包括用于由所述移动设备接收移动代码的装置。

10. 根据权利要求 8 的系统，进一步包括用于在会话的持续时间中使用

所述产生的安全密钥安全地通信的装置。

11. 根据权利要求 8 的系统，其中使用分组过滤器来标识 HTTP/HTTPS 分组。

12. 根据权利要求 8 的系统，其中所述产生的安全密钥是有线等效保密密钥。

13. 根据权利要求 8 的系统，其中所述 web 服务器驻留在所述接入点上。

14. 根据权利要求 8 的系统，进一步包括用于由所述移动设备设置所述产生的安全密钥的装置。

15. 一种移动设备，包括:

用于经由 HTTP 接入请求转发供安全接入无线局域网的请求的装置;

用于接收移动代码的装置; 和

用于设置安全密钥的装置。

16. 一种移动设备，包括:

用于经由 HTTP 接入请求转发供安全接入无线局域网的请求的装置;

用于接收供显示安全密钥给所述移动设备的信号的装置; 和

用于设置所述安全密钥的装置。

17. 一种接入点，包括：

用于经由 HTTP 接入请求接收供安全接入无线局域网的请求的装置;

用于产生安全密钥的装置; 和

用于设置所述产生的安全密钥的装置。

安全的匿名无线局域网(WLAN)接入机制

技术领域

本发明涉及用于允许移动通信设备去安全地接入无线局域网(WLAN)的机制/技术。

背景技术

随着无线网络的激增，许多的行业采用它们以便利其移动工作。由于与有线网络相比，无线网络更加容易被非法使用和窃听，因此公司要求授权的用户向网络提供某种形式的凭证以便获得接入。该凭证可以是以下的一个或多个：

- 用户名/口令组合;
- 类似安全 ID 的硬件令牌（token）;
- 类似指纹的生物测定标识。

该无线网络维护合法、经授权的用户的数据库(DB)，并且根据这个数据库检查用户的凭证。换句话说，用户必须能够证明其身份，以便获得对网络安全接入。但是，存在另一类的用户。这些是接入商业机构的、公司的访客(商业伙伴、客户等等)。这样的用户在 DB 中没有帐户。典型地，这些访客被给予临时的凭证，在他们的接入期间他们可以使用该凭证。这导致若干管理问题:

- 需要在数据库中维护访客帐户。
- 如果使用硬件令牌，在离开时访客有可能忘记将其返还。在这种情况下，该令牌必须被撤销。

发明内容

作为一个可供选择的办法，企业可以提供(在逻辑或者物理上)单独的无线网络，专门地供访客使用。典型地，这个网络与公司网络隔离，并且任何人无需提供凭证给该网络就可以接入它。换句话说，该网络对其用户提供匿名接入。在下文中，这个网络被称作“访客网络”或者“访客 WLAN”。即使

没有进行用户验证，该无线链路也必须被保护以防止窃听。在没有无线链路安全的情况下，所有访客网络流量都是不加密地发送的。

在访客网络/WLAN 中，接入点(AP)是该访客网络的入口点。此外，该访客网络/WLAN 具有与本发明有关的以下的部件：

•web 服务器

•分组过滤器和重定向器

•可选择的移动代码(ActiveX/插件)

web 服务器、分组过滤器和重定向器可以与 AP 位于在同一地点。

在本发明中，不进行用户验证。在正常浏览器交互之后开始该登录过程，而不需要没有任何用户凭证。其次，启动保护无线链路的该登录步骤是由对 HTTPS 页面的接入产生的。通过使用 HTTPS，用户可以确保该网络/WLAN 属于他/她正在接入的站点(用户可以验证颁布给该站点的数字证书)。最后，该安全密钥被设置在客户机器(移动通信设备)和 AP 两者上。因此，该无线链路是安全的。

描述了一种用于对无线局域网提供安全、匿名接入的方法和系统，包括：配置接入点以丢弃除了呈现 HTTP/HTTPS 协议的分组之外的分组，由接入点经由 web 浏览器从移动设备截取一个 HTTP 接入请求，由接入点将 HTTP 接入请求重定向到 web 服务器，由接入点和 web 服务器的一个产生安全密钥，由接入点将产生的安全密钥安全地与所述 web 服务器交换，或者由 web 服务器将产生的安全密钥安全地与所述接入点交换，和由接入点设置安全密钥。还描述了一种移动设备，包括：用于经由 HTTP 接入请求转发供安全接入无线局域网的请求的装置，用于接收移动代码或者供显示安全密钥的信号的装置，和用于设置安全密钥的装置。

附图说明

从以下与附图结合阅读的优选实施例的详细说明中，本发明的这些和其他的方面、特征和优点将变得显而易见。

图 1 是用于实施建立对网络（例如，无线局域网）的安全匿名接入方法的系统的方框图。

图 2A 是描绘为了允许对访客网络安全无线局域网接入、在网络/WLAN 和移动通信设备之间按时间顺序发生的通信的一个实施例的“梯形”示意图。

图 2B 是描述为了允许对访客网络安全无线局域网接入、在网络/WLAN 和移动通信设备之间按时间顺序发生的通信的替代实施例的“梯形”示意图。

图 3 是在提供安全匿名无线局域网接入时涉及的部件的方框图。

具体实施方式

图 1 是用于允许至少一个移动通信设备，并且最好是，多个移动通信设备(例如，移动通信设备 12_1、12_2 和 12_3)安全地接入通信网络 10 的无线局域网 20 的方框图。在一个优选实施例中，该移动通信设备 12_1 包括膝上计算机，而移动通信设备 12_2 包括个人数据助理，并且移动通信设备 12_3 包括无线手机。

在举例说明的实施例中，AP 18 包括无线收发信机(未示出)，用于与每个移动通信设备内的无线电收发信机(未示出)交换射频信号。为此，AP 18 采用一个或多个公知的无线数据交换协议，诸如，“HiperLan 2”或者 IEEE 802.11 协议。实际上，无线局域网 20 可以包括多个 AP，这里每个 AP 可以采用不同的无线协议以使适应不同的移动通信设备。

参考图 2A 可以最好地理解本发明的技术，其描述在移动通信设备（例如，移动通信设备 121）、AP 18 和 web 服务器 24 之间按时间顺序发生的一系列通信。当用户移动进入无线 LAN 热点，并且打开 web 浏览器的时候，在 web 服务器、分组过滤器和重定向器与 AP 位于同一地点的一个实施例中发生以下的事件:

1. 该 AP 截获由在移动通信设备上运行的 web 浏览器软件产生的 HTTP 接入请求。该 AP 产生对于该用户唯一的安全密钥(例如，WEP 密钥)。该 AP 被配置来丢弃除了 HTTP/HTTPS 分组之外的分组。

2. 该 AP 经由 HTTPS 将用户到安全地重定向 web 服务器。所产生的安全密钥被作为一个参数传送给 web 服务器。由于使用了 HTTPS，因此所有的参数被安全地送到 web 服务器。作为进一步的措施，可以使用在 AP 和 web 服务器之间预先共享的密钥来加密安全密钥参数。

3. 在某些浏览器交互(例如，WLAN HTTP web 服务器返回欢迎页面，该用户点击这个页面上的“登录”按钮)之后，该用户浏览器到达安全的 HTTPS 网页，其包含移动代码(ActiveX 控件/插件)和所产生的安全密钥，例如，有线等效保密(WEP)密钥。

4. 相同的安全密钥被设置在 AP 和客户的机器上(通过移动代码)。这使

无线链路安全。

为了启动安全接入，在图 2A 的步骤 100 期间该移动通信设备 12_1 传送接入请求给 AP 18。在实践中，通过由移动通信设备 12_1 执行的 web 浏览器软件程序发出的 HTTP 接入要求，该移动通信设备 12_1 启动接入请求。响应该接入请求，AP 18 在图 2A 的步骤 102 产生安全密钥，并且将其与 web 浏览器(未示出)安全地交换。AP 18 然后在步骤 103 上发送安全密钥给 web 服务器 24。该 AP 然后在步骤 104 期间将移动通信设备中的 web 浏览器软件重定向到 AP 上的本地欢迎页。在步骤 104 之后，并且在某些浏览器交互(未示出)之后，该用户浏览器到达安全的 HTTPS 内部网页，其包含移动代码(ActiveX 控件/插件)和所产生的安全密钥。该 web 服务器 24 然后在步骤 106 上将移动代码推出（push）给请求接入的移动设备。一旦收到该移动代码，移动通信设备和 AP 两者在步骤 108a 和 108b 上设置安全密钥，其用于供会话的剩余部分通信。每个新的会话需要重新执行该方法。

ActiveX 控件实质上是一种可执行的程序，其可以被嵌入在网页之内。许多软件浏览器程序，诸如 Microsoft Internet Explorer 具有显示上述的网页和调用嵌入的 ActiveX 控件的能力，其可以从远程服务器(例如，web 服务器 24)下载。ActiveX 控件的执行受到置入该浏览器软件中的安全机制限制。在实践中，大多数浏览器程序具有若干不同的可选择的安全级别。在最低的级别上，可以没有限制地调用来自 web 的任何 ActiveX 控件。在最高的级别上，不能从浏览器软件调用 ActiveX 控件。

通常地，该安全级别被设置为中等，在这样的情况下，仅仅那些具有数字签名的 ActiveX 控件可以被调用。对于这样的 ActiveX 控件，在调用 ActiveX 控件之前，该浏览器软件首先检查签名的有效性，以确信存在以下的条件：(1)可以跟踪该 ActiveX 控件的来源，和(2)除了对其签名的实体之外，ActiveX 控件没有被其他任何人篡改。在所示的实施例中，该 web 服务器 24 使用 ActiveX 控件去传送和在移动通信设备 12_1 上设置安全密钥。该 ActiveX 控件是非常简单的，并且其唯一的功能是通过给该设备提供具有嵌入的 ActiveX 控件的网页来在移动通信设备 121 上设置密钥。

一旦移动设备和 AP 两者已经设置了安全密钥，那么，允许按照该安全密钥进行安全数据通信。

用于允许安全无线局域网接入的上述方法对于大多数移动通信设备都将

无缝地工作，因为大多数设备采用支持 ActiveX 控件的浏览器软件，并且在大多数设备中该浏览器软件的安全级别通常被设置为中等。对于那些其浏览器软件当前被设置以最高安全级别的移动通信设备，将向该设备发送请求，以要求用户临时地将浏览器软件的安全设置更改为中等。对于那些没有采用能够支持 ActiveX 控件的浏览器软件的移动通信设备，可以使用浏览器软件插件。如果 AP 18 检测到在寻求接入的移动通信设备 12_1 中的该浏览器软件不支持 ActiveX 控件，则该移动通信设备 12_1 的用户将被提示去下载和安装小的插件。该插件的功能实质上与 ActiveX 控件的密钥设置功能相同。一旦该插件程序被安装在移动通信设备 12_1 中，就可以通过将该安全密钥封装在用该插件的特别文件中将该安全密钥设置在移动通信设备上。随后，该插件读取安全密钥文件，并且在移动通信设备 121 中设置该密钥。

从实践的观点来看，设置 ActiveX 控件的该安全密钥应当被参数化。换句话说，该 ActiveX 控件应当把该安全密钥作为一个参数。以这种方法，该 web 服务器 24 只需要保留单个编译的 ActiveX 控件，并且通过给请求的移动通信设备提供不同的参数来将其用于不同的会话。否则，该 web 服务器 24 将不得不在 ActiveX 控件内建立安全密钥，即，对于每个会话建立不同的 ActiveX 控件，一个效率低的进程。

图 2B 也是一个梯形图，描绘为了允许对访客网络的安全无线局域网接入而在无线局域网和移动通信设备之间按时间顺序发生的通信。但是，这个实施例指向手动的情形，这里 web 服务器 24 向用户显示安全密钥，然后，该用户被指示遵循在显示器上的指令来在移动通信设备上设置安全密钥。在这个实施例中，发生以下的事件：

1. 该 AP 截获由在移动通信设备上运行的 web 浏览器软件产生的 HTTP 接入请求。该 AP 产生对于用户唯一的安全密钥。该 AP 被配置成丢弃除了 HTTP/HTTPS 分组之外的所有分组。

2. 该 AP 将用户重定向到 web 服务器。所产生的安全密钥被作为参数传送给 web 服务器。因为使用 HTTPS 与 web 服务器通信，所以这是安全的。作为进一步的措施，可以使用在 AP 和 web 服务器之间共享的密钥来加密安全密钥参数。

3. 在某些浏览器交互(例如，web 服务器返回欢迎页面，该用户点击这个页面上的“登录”按钮)之后，在步骤 107 该用户浏览器到达安全的 HTTPS

内部网页，该网页显示安全密钥给用户，并且可选择地，给出有关如何在移动通信设备上设置安全密钥的命令。

4. 该用户遵循该指令(如果提供有的话)，并且在移动设备上设置该安全密钥。

5. 相同的安全密钥被设置在该 AP 上。这使无线链路安全。

在该 web 服务器与 AP 不在同一地点的情况下，经由安全手段在 web 服务器和 AP 之间交换该安全密钥。例如，AP 和 web 服务器可以预先共享专门地用于在 AP 和 web 服务器之间通信的另一个安全密钥，并且使用这个密钥去加密在所述 AP 和 web 服务器之间的通信。

此外，该安全密钥可以由 web 服务器而不是 AP 产生，然后经由如上所述的安全手段交换给 AP。

图 3 是在提供安全匿名无线局域网接入时涉及的部件的方框图。HTTP 请求 305 经过分组过滤器，后者丢弃所有不是 HTTP/HTTPS 分组的分组。未被丢弃的任何分组被转发给重新定向器 310，后者经由 web 服务器 315 将用户的 web 浏览器重定向到站点 320 的 ActiveX/插件。

应该理解，本发明可以例如在移动终端、接入点或者蜂窝网络内以不同的硬件、软件、固件、专用处理器或者其组合的形式实现。最好是，本发明作为硬件和软件的组合实现。此外，该软件最好是作为在程序存储设备上具体实施的应用程序来实现。该应用程序可以被上载并且由包括任何适宜结构的机器执行。最好是，该机器是在具有硬件，诸如一个或多个中央处理单元(CPU)、随机存取存储器(RAM)和输入/输出(I/O)接口的计算机平台上实现的。该计算机平台还包括操作系统和微指令代码。在此处描述的各种各样的处理和功能或者可以是微指令代码的一部分，或者是应用程序的一部分(或者其组合)，其经由操作系统执行。此外，各种各样其他的外围设备可以连接到计算机平台，诸如，附加的数据存储设备和打印设备。

应该进一步理解，因为在该附图中描述的一些构成的系统部件和方法步骤最好是以软件实现，取决于本发明编程的方式，在系统部件(或者处理步骤)之间的实际连接可以不同。在此处给出教导，本领域技术人员将能够构思出本发明的这些和类似的实施或者结构。

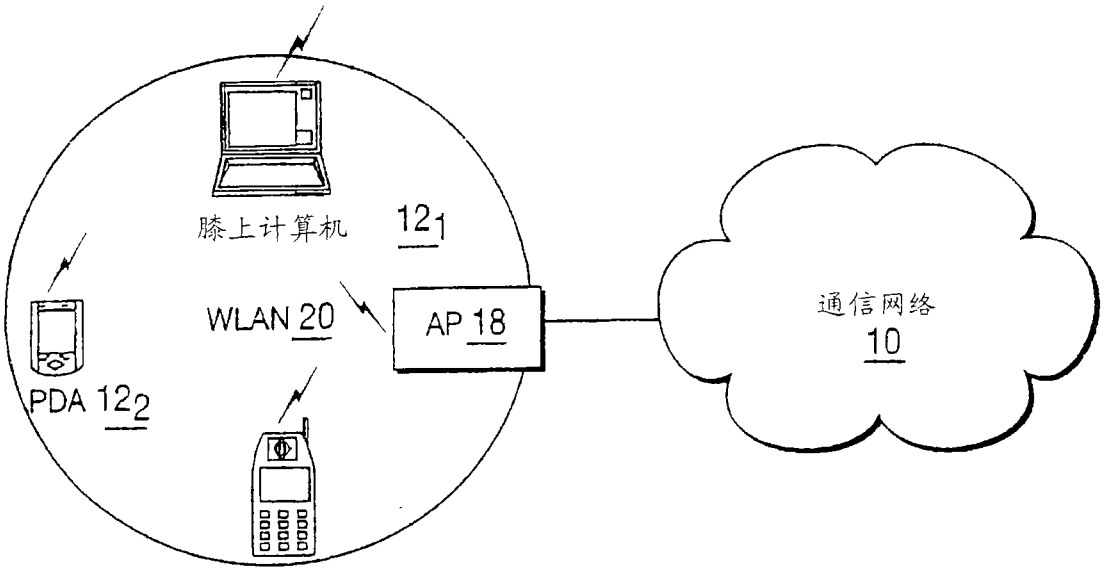

膝上计算机 12₁
WLAN 20
AP 18
通信网络
10
PDA 12₂
无线手机 12₃

图 1

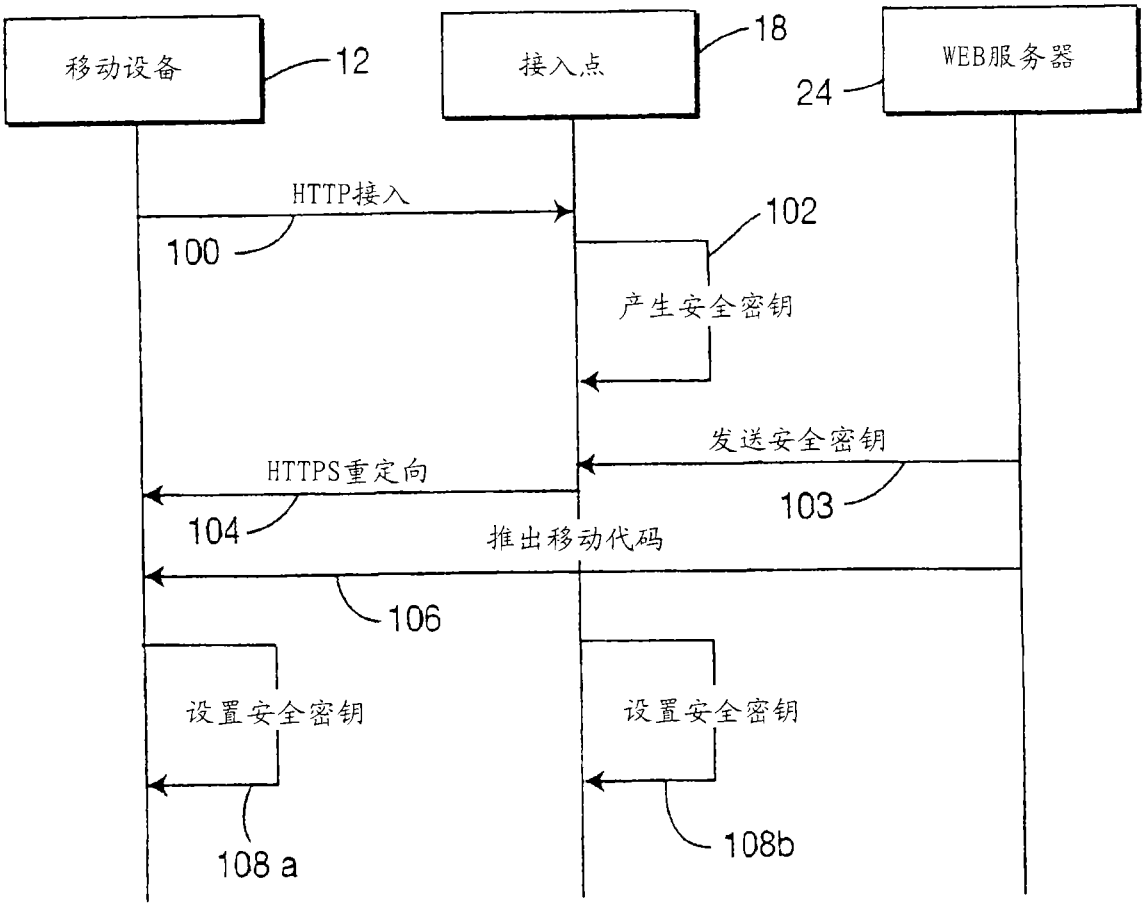

移动设备
12
接入点
18
WEB服务器
24
HTTP接入
100
102
产生安全密钥
发送安全密钥
HTTPS重定向
103
104
推出移动代码
106
设置安全密钥
设置安全密钥
108 a
108b

图 2A

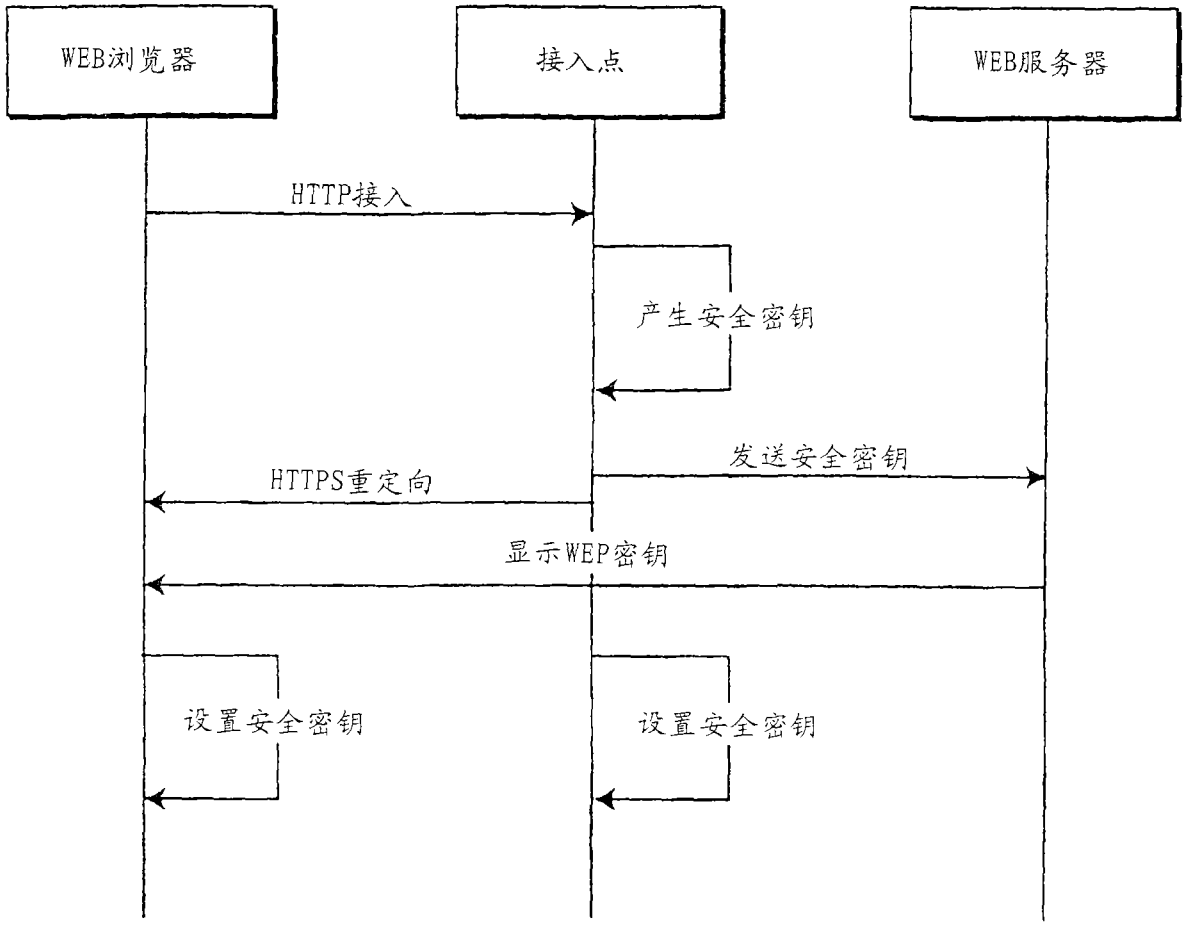

WEB浏览器
接入点
WEB服务器
HTTP接入
产生安全密钥
发送安全密钥
HTTPS重定向
显示WEP密钥
设置安全密钥
设置安全密钥

图 2B

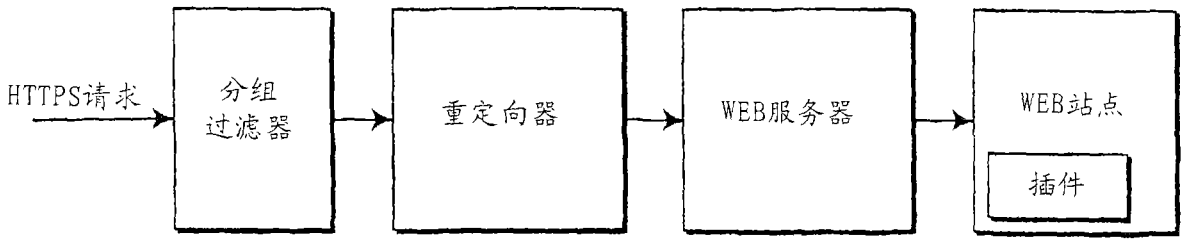

HTTPS请求
分组
过滤器
重定向器
WEB服务器
WEB站点
插件

图 3