[19] 中华人民共和国国家知识产权局

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

[12] 发明专利说明书

[21] ZL 专利号 02139508.X

[45] 授权公告日 2005 年 3 月 2 日

[11] 授权公告号 CN 1191696C

[22] 申请日 2002.11.6 [21] 申请号 02139508.X

[71] 专利权人 西安西电捷通无线网络通信有限公司

地址 710075 陕西省西安市高新二路 12 号协同大厦 4F.C 座

[72] 发明人 铁满霞 唐厚俭 张变玲 张 宁 叶续茂

审查员 戴 磊

[74] 专利代理机构 北京同立钧成知识产权代理有限公司

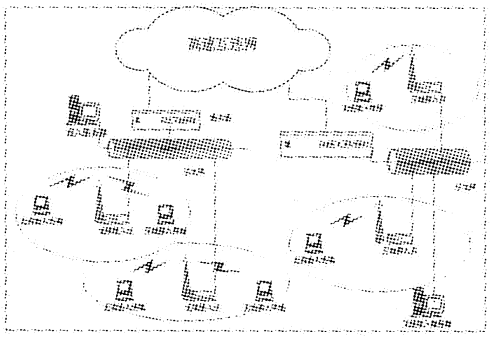
代理人 刘 芳

权利要求书 5 页 说明书 10 页 附图 2 页

[54] 发明名称 一种无线局域网移动设备安全接入及数据保密通信的方法

[57] 摘要

一种无线局域网移动设备安全接入及数据保密通信的方法，MT 向 AP 发起接入认证请求；AP 向 AS 发起证书认证请求；AS 对 AP 以及 MT 的证书进行认证；AS 将认证结果通过证书认证响应回复 AP；若 MT 认证未通过，AP 拒绝 MT 接入 AP；移动终端 MT 对接收到的 AP 证书认证结果进行判断；若 AP 认证通过，开始进行通信；否则，MT 拒绝登录至 AP。 本发明通过双向认证机制，解决了无线局域网 WLAN 中没有对移动终端 MT 进行有效的安全接入控制，保障了移动终端 MT 接入的安全性、通信的高保密性。



ISSN1008-4274

知识产权出版社出版

1、一种无线局域网移动设备安全接入及数据保密通信的方法，其特征在于，接入认证过程包括如下步骤：

步骤一，移动终端 MT 将移动终端 MT 的证书发往无线接入点 AP 提出接入认证请求；

步骤二，无线接入点 AP 将移动终端 MT 证书与无线接入点 AP 证书发往认证服务器 AS 提出证书认证请求；

步骤三，认证服务器 AS 对无线接入点 AP 以及移动终端 MT 的证书进行认证；

步骤四，认证服务器 AS 将对无线接入点 AP 的认证结果以及将对移动终端 MT 的认证结果通过证书认证响应发给无线接入点 AP，执行步骤五；若移动终端 MT 认证未通过，无线接入点 AP 拒绝移动终端 MT 接入；

步骤五，无线接入点 AP 将无线接入点 AP 证书认证结果以及移动终端 MT 证书认证结果通过接入认证响应返回给移动终端 MT；

步骤六，移动终端 MT 对接收到的无线接入点 AP 证书认证结果进行判断；若无线接入点 AP 认证通过，执行步骤七；否则，移动终端 MT 拒绝登录至无线接入点 AP；

步骤七，移动终端 MT 与无线接入点 AP 之间的接入认证过程完成，双方开始进行通信。

2、根据权利要求 1 所述的方法，其特征在于，所述的接入认证请求为移动终端 MT 将移动终端 MT 证书与一串随机数据组成接入认证请求发往无线接入点 AP，以随机数据串为接入认证请求标识。

3、根据权利要求 1 所述的方法，其特征在于，所述的证书认证请求为无线接入点 AP 收到移动终端 MT 的接入认证请求后，将移动终端 MT 证书、接入认证请求标识、无线接入点 AP 证书及无线接入点 AP 对前三项的签名构成证书认证请求发送给认证服务器 AS。

4、根据权利要求 1 所述的方法，其特征在于，所述的证书认证响应为认证服务器 AS 收到无线接入点 AP 的证书认证请求后，验证无线接入点 AP 的签名与无线接入点 AP 证书的合法性，若不正确，则认证过程失败；否则再验证移动终端 MT 证书的合法性；然后认证服务器 AS 将移动终端 MT 证书认证结果信息、无线接入点 AP 证书认证结果信息及认证服务器 AS 对前两项的签名构成证书认证响应发回给无线接入点 AP；所述的移动终端 MT 证书认证结果信息包括移动终端 MT 证书、认证结果及认证服务器对前两项的签名，所述的无线接入点 AP 证书认证结果信息包括无线接入点 AP 证书、认证结果、接入认证请求标识及认证服务器对前三项的签名。

5、根据权利要求 1 所述的方法，其特征在于，所述的接入认证响应为无线接入点 AP 对认证服务器 AS 返回的证书认证响应进行签名验证，得到移动终端 MT 证书的认证结果；无线接入点 AP 将移动终端 MT 的认证结果信息、无线接入点 AP 证书认证结果信息及认证服务器 AS 对前两项的签名组成接入认证响应回送至移动终端 MT，移动终端 MT 对无线接入点 AP 返回的接入认证响应进行签名验证，便得到无线接入点 AP 证书的认证结果，移动终端 MT 与无线接入点 AP 之间的证书认证过程完成。

6、根据权利要求 1 所述的方法，其特征在于，接入认证过程完成，移动终端 MT 与无线接入点 AP 之间进行会话密钥协商，密钥协商成功后，两者之间开始保密通信。

7、根据权利要求 6 所述的方法，其特征在于，所述的移动终端 MT 内设置有指定的无线接入点 AP 的信息或无线接入点 AP 的证书，以接入指定的无线接入点 AP。

8、根据权利要求 6 所述的方法，其特征在于，所述的会话密钥协商为静态会话密钥协商，包括无线接入点 AP 利用移动终端 MT 的公钥与自己的私钥生成会话密钥，移动终端 MT 利用无线接入点 AP 的公钥与自己的私钥生成会话密钥。

9.根据权利要求 6 所述的方法，其特征在于，所述的会话密钥协商为动态会话密钥协商包括:

步骤一，移动终端 MT 向无线接入点 AP 发出密钥协商请求；移动终端 MT 秘密选取一个整数a，由此计算出整数$f(a)$，将整数$f(a)$与移动终端 MT 对其的签名构成密钥协商请求，传给无线接入点 AP；所述的f为一函数，其使得由整数$f(a)$得出整数a在计算上不可行；

步骤二，无线接入点 AP 向移动终端 MT 发出密钥协商响应；无线接入点 AP 收到密钥协商请求并验证签名正确后，秘密选取一个整数b，由此计算出整数$f(b)$，将整数$f(b)$与无线接入点 AP 对其的签名构成密钥协商响应，传给移动终端 MT；所述的f为一函数，其使得由整数$f(b)$得出整数b在计算上不可行；

步骤三，移动终端 MT 收到密钥协商响应并验证签名正确后计算$g(a,f(b))$，无线接入点 AP 计算$g(b,f(a))$，双方以其作为通信过程中的会话密钥；所述的g为一函数，其使得$g(a,f(b))=g(b,f(a))$。

10、根据权利要求 6 所述的方法，其特征在于，所述的会话密钥协商为动态会话密钥协商包括：

步骤一， 无线接入点 AP 向移动终端 MT 发出密钥协商请求；无线接入点 AP 秘密选取一个整数b，由此计算出整数$f(b)$，将整数$f(b)$与无线接入点 AP 对其的签名构成密钥协商请求，传给移动终端 MT；所述的f为一函数，其使得由整数$f(b)$得出整数b在计算上不可行；

步骤二，移动终端 MT 向无线接入点 AP 发出密钥协商响应，移动终端 MT 收到密钥协商请求并验证签名正确后，秘密选取一个整数a，由此计算出整数$f(a)$，将整数$f(a)$与移动终端 MT 对其的签名构成密钥协商响应，传给无线接入点 AP；所述的f为一函数，其使得由整数$f(a)$得出整数a在计算上不可行；

步骤三，移动终端 MT 计算$g(a,f(b))$，无线接入点 AP 收到密钥协商响应并验证签名正确后计算$g(b,f(a))$，双方以其作为通信过程中的会话密钥；所述的g为一函数，其使得$g(a,f(b))=g(b,f(a))$。

11、根据权利要求 6 所述的方法，其特征在于，所述的会话密钥协商为动态会话密钥协商包括：

步骤一，移动终端 MT 向无线接入点 AP 发出密钥协商请求，移动终端 MT 产生一串随机数据，利用无线接入点 AP 的公钥加密后构成密钥协商请求，传递给无线接入点 AP;

步骤二，无线接入点 AP 向移动终端 MT 发出密钥协商响应，无线接入点 AP 收到移动终端 MT 发来的密钥协商请求后，利用自己的私钥进行解密，得到对方产生的随机数据；然后无线接入点 AP 再产生一串随机数据，利用移动终端 MT 的公钥加密后构成密钥协商响应，传递给移动终端 MT;

步骤三，移动终端 MT 与无线接入点 AP 均利用自己与对方分别产生的随机数据生成会话密钥。

12、根据权利要求 6 所述的的方法，其特征在于，所述的会话密钥协商为动态会话密钥协商包括:

步骤一，无线接入点 AP 向移动终端 MT 发出密钥协商请求，无线接入点 AP 产生一串随机数据，利用移动终端 MT 的公钥加密后构成密钥协商请求，传递给移动终端 MT;

步骤二，移动终端 MT 向无线接入点 AP 发出密钥协商响应，移动终端 MT 收到无线接入点 AP 发来的密钥协商请求后，利用自己的私钥进行解密，得到对方产生的随机数据；然后移动终端 MT 再产生一串随机数据，利用无线接入点 AP 的公钥加密后构成密钥协商响应，传递给无线接入点 AP;

步骤三，移动终端 MT 与无线接入点 AP 均利用自己与对方分别产生的随机数据生成会话密钥。

13、根据权利要求 6 所述的方法，其特征在于，所述的会话密钥协商为动态会话密钥协商，包括:

步骤一，移动终端 MT 产生一串随机数据，利用无线接入点 AP 的公钥加密后，再附上自己的签名传送给无线接入点 AP;

步骤二，无线接入点 AP 收到此请求后，先利用移动终端 MT 的公钥对请求中的签名进行验证，再利用自己的私钥将收到的密文进行解密，得到移动终端

MT 产生的一串随机数据，

步骤三，双方以此随机数据作为会话密钥进行保密通信。

14、根据权利要求 6 所述的方法，其特征在于，所述的会话密钥协商为动态会话密钥协商，包括:

步骤一，无线接入点 AP 产生一串随机数据，利用移动终端 MT 的公钥加密后，再附上自己的签名传送给移动终端 MT;

步骤二，移动终端 MT 收到此请求后，先利用无线接入点 AP 的公钥对请求中的签名进行验证，再利用自己的私钥将收到的密文进行解密，得到无线接入点 AP 产生的一串随机数据，

步骤三，双方以此随机数据作为会话密钥进行保密通信。

一种无线局域网移动设备安全接入及数据保密通信的方法

技术领域

本发明涉及一种无线局域网移动设备安全接入及数据保密通信的方法，尤其是一种无线局域网移动终端与接入设备之间经过双向认证的安全接入，并在无线链路数据通信时进行有效保密通信的方法。属于通信技术领域。

背景技术

个人通信的目标，就是使人们能够在任何时候、任何地点和其他任何人进行任意的通信联系，自由地享用网络提供的多种业务。无线局域网技术融合目前最热门的两大技术——IP 技术和无线通信技术，顺应宽带化的发展趋势，为移动主机或移动终端提供方便、快捷、高速的因特网接入服务，以适应人们对高速网络和多媒体通信业务不断增长的需求。无线局域网 WLAN(Wireless Local Area Network）不仅支持移动计算，而且具有构架的灵活性、快捷性及可扩展性。图 1 所示为以无线局域网为基础的宽带无线接入网络结构示意图。它主要由移动终端 MT（Mobile Terminal）、无线接入点 AP（Access Point）及无线接入服务器 WAS（Wireless Access Server）等设备组成，其中移动终端 MT 可在网中任意移动，无线接入点 AP 实现包括越区切换在内的小区管理、对移动终端 MT 的管理和桥接功能，无线接入服务器 WAS 实现移动终端 MT 的网间漫游管理。从固定接入到移动无线接入因特网，基于无线局域网的宽带无线 IP 技术为世界网络环境带来了全新的观念和巨大的冲击。该系统的应用非常广泛，在商务网络，如主要是公司内部网、机构用户网络，如公安、金融、政府各部门等、小区网如学校、医院、住宅区等、远程监测或集中监控等、临时网络，如临时会议等、户外移动用户以及布线不易的场合、需要经常变动的场合等都非常有用。

对于无线局域网来说，其安全问题远比有线网严重的多，为此无线局域网

引入了几个层次的手段来解决安全问题。首先是通过对每个无线接入点 AP 设置不同的业务组标识符 SSID（Service Set ID），并强迫移动终端 MT 接入时提供相应的业务组标识符 SSID，从而可以允许不同群组的用户接入，并对资源访问的权限进行区别限制。但利用业务组标识符 SSID 是最直观的一种认证方式，是较低级的安全认证，因为任何人只要知道业务组标识符 SSID 就可以接入网络。其次是地址限制，即通过在无线接入点 AP 上设置被授权的移动终端 MT 无线网卡的媒体访问控制 MAC（Medium Access Control）地址来杜绝非授权的访问。但是无线网卡的 MAC 地址并不难获得，而且可以伪造，因此这也属于较低级别的授权认证。总之，以上两种方式都不能有效地控制移动终端 MT 的接入，更无法保障通信的保密性。

除上述两种方法外，目前更多采用的一种措施是依据无线局域网 WLAN 的国际标准（IEEE802.11），在无线局域网 WLAN 中引入基于 RC-4 的有线等价保密协议 WEP（Wired Equivalent Privacy）保密机制对数据进行加密传输。WEP 算法采用单钥体制，即加解密为同一密钥，其密钥长度为 64 位或 128 位。其中 40 位或 104 位为固定部分，称为初始化密钥，即在无线接入点 AP 和移动终端 MT 设置的密钥，余下的 24 位为可变部分，称为初始化矢量，该矢量在通信过程中由网卡的驱动软件来改变，也就是说用于加密的密钥可变，这在某种程度上保证了无线通信的保密性。但由于初始化矢量变化的规律性，因此 WEP 算法的安全程度并不高，这一点由美国加利福尼亚大学一研究小组最先于 2001 年 3 月发现，他们指出采用 WEP 算法的无线局域网 WLAN 仅在 5 个小时即可被攻破。其中的原因解释如下：假设初始化矢量值以每帧递增 1 的速度改变，每帧长度为 1500 字节，数据发送速率为 11 兆位/秒，则初始化矢量重复的周期为：

$$1500\text{字节}/\text{帧}\times 8\text{位}/\text{字节}\times 1\text{秒}/(11\times 10^{6}\text{位})\times 2^{24}\text{帧}\approx 18300\text{秒}\approx 5\text{小时}$$

，即每隔 5 小时就可得到经过同一密钥加密的两帧密文，由此便可猜测到或计算出初始密钥值。这里必须指出的是密钥的长度并不影响其破译的时间，只是增加了猜测或计算的复杂度。2001 年 8 月两名以色列魏兹曼研究所的专家与一位思科公司的研究

人员——三位全球顶尖译码专家进行了 WEP 安全测试，他们根据窃取网络中的一小部分资料，不到一小时即破解了无线局域网 WLAN 使用的密钥，同时 AT&T 实验室研究团体也以同样的方法成功破解，这充分说明 WEP 协议不能保障无线局域网的安全。安全问题已成为阻碍无线局域网应用普及的主要障碍之一，安全接入和保密通信也已成为无线局域网技术研究的重中之重。

发明内容

本发明的目的在于克服现有技术的不足，提供一种无线局域网移动设备安全接入及数据保密通信的方法，其采用公钥密码技术，通过双向认证机制，解决了无线局域网 WLAN 中没有对移动终端 MT 进行有效的安全接入控制，克服了无线链路的数据通信保密的局限性，保障了移动终端 MT 接入的安全性、通信的高保密性。

为实现上述目的，本发明提供了如下技术方案如下:

一种无线局域网移动设备安全接入及数据保密通信的方法，当移动终端 MT 登录至无线接入点 AP 时，移动终端 MT 与无线接入点 AP 通过认证服务器 AS 进行双向证书认证；认证成功后，移动终端 MT 与无线接入点 AP 进行会话密钥协商。

它包括如下步骤:

步骤一，移动终端 MT 将移动终端 MT 的证书发往无线接入点 AP 提出接入认证请求;

步骤二，无线接入点 AP 将移动终端 MT 证书与无线接入点 AP 证书发往认证服务器 AS 提出证书认证请求;

步骤三，认证服务器 AS 对无线接入点 AP 以及移动终端 MT 的证书进行认证;

步骤四，认证服务器 AS 将对无线接入点 AP 的认证结果以及将移动终端认

证结果通过证书认证响应发给无线接入点 AP，执行步骤五；若移动终端 MT 认证未通过，无线接入点 AP 拒绝移动终端 MT 接入；

步骤五，无线接入点 AP 将无线接入点 AP 证书认证结果以及移动终端 MT 证书认证结果通过接入认证响应返回给移动终端 MT；

步骤六，移动终端 MT 对接收到的无线接入点 AP 证书认证结果进行判断；若无线接入点 AP 认证通过，执行步骤七；否则，移动终端 MT 拒绝登录至无线接入点 AP；

步骤七，移动终端 MT 与无线接入点 AP 之间的接入认证过程完成，双方之间开始进行通信。

建立通信后，为保障数据保密，还可在移动终端 MT 与无线接入点 AP 之间进行会话密钥协商。具体包括静态会话密钥协商与动态会话密钥协商。

移动终端 MT 将移动终端 MT 证书与一串随机数据组成接入认证请求发往无线接入点 AP，以随机数据串为接入认证请求标识；完成接入认证请求。

无线接入点 AP 收到移动终端 MT 接入认证请求后，将移动终端 MT 证书、接入认证请求标识、无线接入点 AP 证书及无线接入点 AP 对前三项进行的签名构成证书认证请求发送给认证服务器 AS；完成证书认证请求。

认证服务器 AS 收到无线接入点 AP 的证书认证请求后，验证无线接入点 AP 的签名与无线接入点 AP 证书的合法性，若不正确，则认证过程失败；否则再验证移动终端 MT 证书的合法性；然后认证服务器 AS 将移动终端 MT 证书认证结果信息、无线接入点 AP 证书认证结果信息及认证服务器 AS 的签名构成证书认证响应发回给无线接入点 AP；所述的移动终端 MT 证书认证结果信息包括移动终端 MT 证书、认证结果及认证服务器对前两项的签名，所述的无线接入点 AP 证书认证结果信息包括无线接入点 AP 证书、认证结果、接入认证请求标识及认证服务器对前三项的签名；完成证书认证响应。

无线接入点 AP 对认证服务器 AS 返回的证书认证响应进行签名验证，得到移动终端 MT 证书的认证结果；无线接入点 AP 将移动终端 MT 的认证结果信息、

无线接入点 AP 证书认证结果信息及认证服务器 AS 对前两项的签名组成接入认证响应回送至移动终端 MT，移动终端 MT 对无线接入点 AP 返回的接入认证响应进行签名验证，便得到无线接入点 AP 证书的认证结果，移动终端 MT 与无线接入点 AP 之间的证书认证过程完成。

移动终端 MT 接入指定的无线接入点 AP 时，认证之前移动终端 MT 须得到该无线接入点 AP 的相关信息或无线接入点 AP 的证书。

静态会话密钥协商是指移动终端 MT 或无线接入点 AP 利用无线接入点 AP 或移动终端 MT 的公钥与自己的私钥生成会话密钥.

动态会话密钥协商可包括:

密钥协商请求。移动终端 MT 秘密选取一个整数 a，由此计算出整数 $f(a)$，将整数 $f(a)$ 与移动终端 MT 对其的签名构成密钥协商请求，传给无线接入点 AP; 所述的 f 为一函数，其使得由整数 $f(a)$ 得出整数 a 在计算上不可行;

密钥协商响应。无线接入点 AP 收到密钥协商请求并验证签名正确后，秘密选取一个整数 b，由此计算出整数 $f(b)$，将整数 $f(b)$ 与无线接入点 AP 对其的签名构成密钥协商响应，传给移动终端 MT; 所述的 f 为一函数，其使得由整数 $f(b)$ 得出整数 b 在计算上不可行;

移动终端 MT 收到密钥协商响应并验证签名正确后计算 $g(a,f(b))$，无线接入点 AP 计算 $g(b,f(a))$，以其作为通信过程中的会话密钥。其中 g 为一函数，其使得 $g(a,f(b))=g(b,f(a))$。

动态会话密钥协商亦可为从无线接入点 AP 发起密钥协商请求。无线接入点 AP 秘密选取一个整数 b，由此计算出整数 $f(b)$，将整数 $f(b)$ 与无线接入点 AP 对其的签名构成密钥协商请求，传给移动终端 MT; 所述的 f 为一函数，其使得由整数 $f(b)$ 得出整数 b 在计算上不可行;

移动终端 MT 收到密钥协商请求并验证签名正确后，秘密选取一个整数 a，由此计算出整数 $f(a)$，将整数 $f(a)$ 与移动终端 MT 对其的签名构成密钥协商响应，传给无线接入点 AP; 所述的 f 为一函数，其使得由整数 $f(a)$ 得出整数 a 在计算

上不可行。完成密钥协商响应；

移动终端 MT 计算$g(a,f(b))$，无线接入点 AP 收到密钥协商响应并验证签名正确后计算$g(b,f(a))$，以其作为通信过程中的会话密钥。

同样，g为一函数，其使得$g(a,f(b))=g(b,f(a))$。

再有，动态会话密钥协商可为：

移动终端 MT 或无线接入点 AP 产生一串随机数据，发起密钥协商请求。利用无线接入点 AP 或移动终端 MT 的公钥加密后构成密钥协商请求，传递给无线接入点 AP 或移动终端 MT；

无线接入点 AP 或移动终端 MT 收到移动终端 MT 或无线接入点 AP 发来的密钥协商请求后，利用自己的私钥进行解密，得到对方产生的随机数据；然后无线接入点 AP 或移动终端 MT 再产生一串随机数据，利用移动终端 MT 或无线接入点 AP 的公钥加密后构成密钥协商响应，传递给移动终端 MT 或无线接入点 AP；

移动终端 MT 与无线接入点 AP 均利用自己与对方分别产生的随机数据生成会话密钥。

进一步地，会话密钥协商为移动终端 MT 或无线接入点 AP 产生一串随机数据，利用无线接入点 AP 或移动终端 MT 的公钥加密后，再附上自己的签名传送给无线接入点 AP 或移动终端 MT；无线接入点 AP 或移动终端 MT 收到此报文后，先利用移动终端 MT 或无线接入点 AP 的公钥对报文中的签名进行验证，再利用自己的私钥将收到的密文进行解密，得到移动终端 MT 或无线接入点 AP 产生的一串随机数据，双方以此随机数据作为会话密钥进行保密通信。

本发明与现有技术相比具有如下优点：

它解决了无线局域网 WLAN 中没有对移动终端 MT 进行有效的安全接入控制的问题，克服了无线链路数据通信保密的局限性。它利用公钥密码体系，实现了移动终端 MT 和无线接入点 AP 的双向认证，更进一步提高了接入的安全性；通过动态会话密钥协商完成每认证每密钥及会话过程中密钥的动态修改，以实

现数据的保密通信，大大增加了破解的难度。总之，该方法不仅实现了对移动终端 MT 的接入控制，而且保障了移动终端 MT 接入的安全性、通信的高保密性。

附图说明

图 1 为已有技术宽带无线 IP 系统的结构示意图；

图 2 为本发明基于认证服务器 AS 的无线局域网安全认证系统的逻辑结构示意图；

图 3 为本发明移动终端 MT 接入时的一种认证实施例流程图。

具体实施方式

下面将结合附图及具体技术方案，对本发明做进一步地详述。

图 2 所示是基于认证服务器 AS（Authentication Server）的无线局域网安全认证系统的逻辑结构示意图。采用公钥密码技术，当移动终端 MT 登录至无线接入点 AP 时，必须利用认证服务器 AS 进行双向身份认证，只有持有合法证书的移动终端 MT 才能接入持有合法证书的无线接入点 AP，否则无线接入点 AP 拒绝移动终端 MT 接入或移动终端 MT 拒绝登录至无线接入点 AP。认证成功后，移动终端 MT 与无线接入点 AP 进行会话密钥协商，以实现无线链路的数据保密通信。整个过程如图 3 所示。其中证书内容主要包含证书的序列号、证书颁发者的名称、证书的有效期、证书持有者的名称、证书持有者的公钥信息、证书颁发者采用的签名算法以及证书颁发者对证书的签名等内容。

移动终端 MT 登录至无线接入点 AP 时，认证服务器 AS 证书认证流程如下：

接入认证请求。移动终端 MT 向无线接入点 AP 发出接入认证请求报文，即将移动终端 MT 证书与一串随机数据发往无线接入点 AP，其中随机数据串被称为接入认证请求标识；

证书认证请求。无线接入点 AP 收到移动终端 MT 接入认证请求后，向认证服务器 AS 发出证书认证请求，即将移动终端 MT 证书、接入认证请求标识、无

线接入点 AP 证书及用无线接入点 AP 的私钥对它们的签名构成证书认证请求报文发送给认证服务器 AS;

证书认证响应。认证服务器 AS 收到无线接入点 AP 的证书认证请求后，验证无线接入点 AP 的签名与无线接入点 AP 证书的合法性，若不正确，则认证过程失败；否则再验证移动终端 MT 证书的合法性。验证完毕，认证服务器 AS 将移动终端 MT 证书认证结果信息包括移动终端 MT 证书、认证结果及认证服务器对前两项的签名，以及无线接入点 AP 证书认证结果信息包括无线接入点 AP 证书、认证结果、接入认证请求标识及认证服务器对前三项的签名,还有认证服务器 AS 的签名构成证书认证响应报文发回给无线接入点 AP;

接入认证响应。无线接入点 AP 对认证服务器 AS 返回的证书认证响应报文的签名进行验证，便得到移动终端 MT 证书的认证结果。无线接入点 AP 将移动终端 MT 的认证结果信息、认证服务器 AS 对无线接入点 AP 证书认证结果信息及认证服务器 AS 的签名组成接入认证响应报文回送至移动终端 MT，移动终端 MT 便得到无线接入点 AP 证书的认证结果。

至此移动终端 MT 与无线接入点 AP 之间完成了证书的双向认证过程。

若双方证书验证成功，则无线接入点 AP 允许移动终端 MT 接入，否则拒绝其接入或者移动终端 MT 拒绝登录到无线接入点 AP。至此，具有合法证书的移动终端 MT 才成功地接入具有合法证书的无线接入点 AP，从而完成无线接入点 AP 对移动终端 MT 的安全接入控制功能。

本发明移动终端 MT 与无线接入点 AP 证书认证成功之后，即完成了移动终端 MT 的成功登录后，通过移动终端 MT 与无线接入点 AP 之间的会话密钥协商，保障数据保密通信。

此时双方在本机利用对方的公钥与自己的私钥生成会话密钥，用于通信数据报文的加解密，从而实现移动终端 MT 与无线接入点 AP 之间的无线安全保密通信。然而值得注意的是，在证书有效期内，移动终端 MT 与无线接入点 AP 之间的会话密钥始终不变。为了做到每认证每密钥：则需进行会话密钥的动态协商。动态密钥协商的过程如下:

密钥协商请求。移动终端 MT 或无线接入点 AP 产生一串随机数据，利用无线接入点 AP 或移动终端 MT 的公钥加密后，向无线接入点 AP 或移动终端 MT 发出请求密钥协商报文;

密钥协商响应。无线接入点 AP 或移动终端 MT 收到移动终端 MT 或无线接入点 AP 发来的密钥协商请求报文后，利用自己的私钥进行解密，得到对方产生的随机数据。然后本地产生一串随机数据，利用移动终端 MT 或无线接入点 AP 的公钥加密后，向移动终端 MT 或无线接入点 AP 回应密钥协商响应报文。移动终端 MT 与无线接入点 AP 均在利用自己与对方分别产生的两个随机数据生成会话密钥，用于对通信数据报文的加解密。

为了进一步提高通信的保密性，在移动终端 MT 与无线接入点 AP 通信一段时间或交换一定数量的报文之后，还可以进行会话密钥的重新协商。

证书认证完成了移动终端 MT 的安全接入，会话密钥协商则充分保证了移动终端 MT 与无线接入点 AP 之间的高保密性通信。

特别指出的是:

1、在具体实现过程中，证书认证与会话钥协商过程不仅没有先后顺序，而且还可合并进行。

2、若移动终端 MT 欲接入指定的无线接入点 AP，则认证之前 MT 应知晓该 AP 的相关信息或存有 AP 的证书，以便 MT 对接收到的接入认证响应报文进行判断。

3、会话密钥的动态协商还可以如下实现，即移动终端 MT 或无线接入点 AP 在本地产生一串随机数据，利用对方的公钥加密后再附上自己的签名传送给对方，无线接入点 AP 或移动终端 MT 先利用对方的公钥验证是否是对方发送的数据，然后利用自己的私钥将收到的密文进行解密，双方将此随机数据作为会话密钥对通信数据进行加解密。

4、会话密钥协商还可如下进行:

密钥协商请求。移动终端 MT 秘密选取一个整数a，计算出$f(a)$，将$f(a)$与

移动终端 MT 对此的签名构成密钥协商请求，传给无线接入点 AP。其中 f 为一函数，使得由 $f(a)$ 得出 a 在计算上是不可行的；

密钥协商响应。无线接入点 AP 收到密钥协商请求并验证签名正确后，秘密选取一个整数 b，计算出 $f(b)$，将 $f(b)$ 与无线接入点 AP 对此的签名传给移动终端 MT。其中 f 函数的定义同 a)；

移动终端 MT 收到密钥协商响应并验证签名正确后计算 $g(a,f(b))$，无线接入点 AP 计算 $g(b,f(a))$，作为通信过程中的会话密钥。g 为一函数，使得 $g(a,f(b))=g(b,f(a))$。

5、会话密钥协商还可如下进行：

密钥协商请求。无线接入点 AP 秘密选取一个整数 b，由此计算出整数 $f(b)$，将整数 $f(b)$ 与无线接入点 AP 对其的签名构成密钥协商请求，传给移动终端 MT；f 为一函数，其使得由整数 $f(b)$ 得出整数 b 在计算上不可行；

密钥协商响应。移动终端 MT 收到密钥协商请求并验证签名正确后，秘密选取一个整数 a，由此计算出整数 $f(a)$，将整数 $f(a)$ 与移动终端 MT 对其的签名构成密钥协商响应，传给无线接入点 AP；所述的 f 为一函数，其使得由整数 $f(a)$ 得出整数 a 在计算上不可行；

移动终端 MT 计算 $g(a,f(b))$，无线接入点 AP 收到密钥协商响应并验证签名正确后计算 $g(b,f(a))$，以其作为通信过程中的会话密钥；g 为一函数，其使得 $g(a,f(b))=g(b,f(a))$。

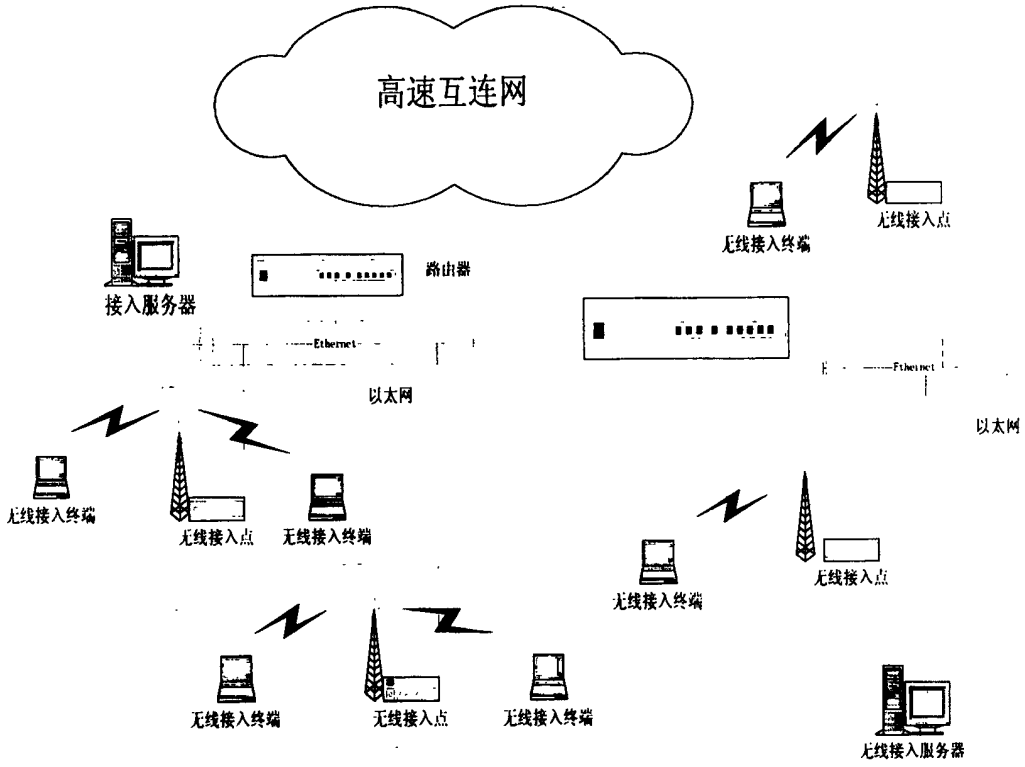

高速互连网
无线接入终端
无线接入点
接入服务器
路由器
Ethernet
以太网
无线接入终端
无线接入点
无线接入终端
无线接入终端
无线接入点
无线接入终端
无线接入点
无线接入终端
无线接入服务器

图 1

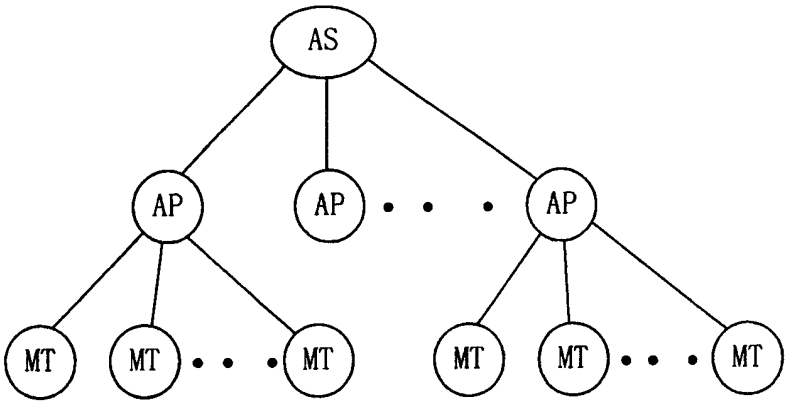

AS
AP
AP
AP
MT
MT
MT
MT
MT
MT

图 2

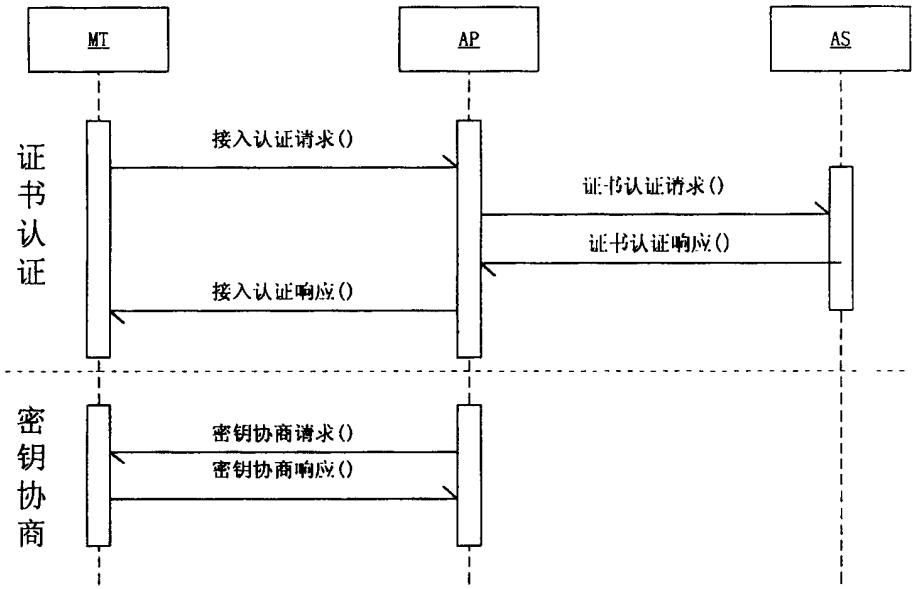

MT
AP
AS
证书认证
接入认证请求()
证书认证请求()
证书认证响应()
接入认证响应()
密钥协商
密钥协商请求()
密钥协商响应()

图 3