[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04Q 7/20
H04L 9/14

# [12]发明专利申请公开说明书

[21]申请号 99110263.0

[43]公开日 2000年4月5日

[11]公开号 CN 1249637A

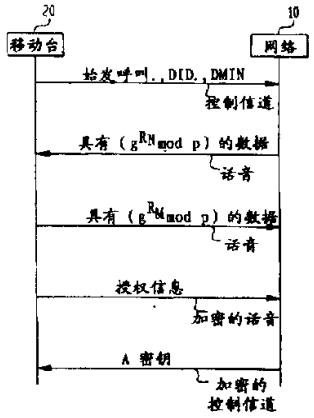
[22]申请日 1999.7.29 [21]申请号 99110263.0
[30]优先权
[32]1998.7.31 [33]US [31]09/127,045
[71]申请人 朗迅科技公司
地址 美国新泽西
[72]发明人 萨瓦·帕特尔
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 罗亚川

权利要求书3页 说明书6页 附图页数1页

[54]发明名称 在无线系统中加密无线通信的方法

[57]摘要

在无线通信的方法中,移动台发送系统接入请求和与系统接入 请求相关的哑数据到网络。网络响应系统接入请求和哑数据发送包 含第一数据部分的第一数据流。移动台提取从第一数据流中提取第 一数据部分和发送第二比特流到网络。第二比特流包含第二数据部分。移动台和网络基于第一数据部分和第二数据部分产生一个密钥 和利用密钥共同建立第一加密和认证的通信信道。然后,移动台通 过该第一加密和认证的通信信道传送授权信息到网络。如果被接 受,则建立第二加密和认证的通信信道。




ISSN1008-4274

# 权 利 要 求 书

1.一种利用网络加密无线通信的方法，包括:

（a）发送系统接入请求和与所述系统接入请求相关的哑数据到网络;

（b）从所述网络接收包含第一数据部分的第一比特流;

（c）从所述第一比特流中提取所述第一数据部分;

（d）发送第二比特流到所述网络，所述第二比特流包含第二数据部分 ;

（e）基于所述提取的第一数据部分和第二数据部分产生一个密钥;

（f）利用所述密钥建立第一加密的通信信道。

2.权利要求 1 的方法，其中所述步骤（c）从在所述第一比特流的第一预定位置提取所述第一数据部分。

3.权利要求 1 的方法，其中所述步骤（d）在所述第二比特流中的第一预定位置发送所述第二数据部分。

4.权利要求 1 的方法，其中

所述第一数据部分代表（模 p g∧$R_N$），其中 p 是一个素数，g 是由所述素数 p 产生的一个群的生成元且 $R_N$ 是第一随机数; 和

所述第二数据部分代表（模 p g∧$R_M$），其中 $R_M$ 是第二随机数。

5.权利要求 4 的方法，其中所述步骤（e）产生所述密钥作为（模 p g∧$R_N$ $R_M$）。

6.权利要求 1 的方法，其中所述步骤（f）建立所述第一加密通信信道作为利用所述密钥的加密和认证的通信信道。

7.权利要求 1 的方法，还包括:

（g）利用所述密钥建立第二加密的通信信道; 和

（h）通过所述第二加密的通信信道传送授权信息到所述网络; 和其中

在所述步骤（h）后，如果所述网络接受所述授权信息，则所述

步骤（f）被执行。

8.权利要求7的方法，其中

所述步骤（f）利用所述密钥，建立所述第一加密的通信信道作为加密和认证通信信道；和

所述步骤（g）利用所述密钥，建立所述第二加密的通信信道作为加密和认证通信信道。

9.权利要求7的方法，其中所述第二加密通信信道是话音信道。

10.权利要求1的方法，其中所述步骤（a）发送始发呼叫请求作为所述系统接入请求。

11.权利要求1的方法，还包括：

（g）通过所述第一加密通信信道从所述网络接收机密信息。

12.权利要求11的方法，其中所述机密信息是根密钥。

13.一种利用网络加密无线通信的方法，包括：

（a）从所述移动台接收系统接入请求和与所述系统接入请求相关的哑数据；

（b）响应于所述系统接入请求和所述哑数据，发送包含第一数据部分的第一比特流到所述移动台；

（c）从所述移动台接收第二比特流，所述第二比特流包含第二数据部分；

（d）从所述第二比特流提取所述第二数据部分；

（e）基于所述提取的第二数据部分和第一数据部分产生一个密钥；

（f）利用所述密钥建立第一加密的通信信道。

14.权利要求13的方法，其中所述步骤（d）从在所述第二比特流中的第一预定位置提取所述第二数据部分。

15.权利要求13的方法，其中所述步骤（b）在所述第一比特流中的第一预定位置发送所述第一数据部分。

16.权利要求13的方法，其中

所述第一数据部分代表（模p g∧$R_N$），其中p是一个素数，g

是由所述素数 p 产生的一个群的生成元且 $R_N$ 是第一随机数；和

所述第二数据部分代表（模 p g∧ $R_M$），其中 $R_M$ 是第二随机数。

17.权利要求 16 的方法，其中所述步骤（e）产生所述密钥为（模 p g $R_N$ $R_M$）。

18.权利要求 13 的方法，其中所述步骤（f）建立所述第一加密通信信道作为加密和认证的通信信道。

19.权利要求 13 的方法，还包括：

（g）利用所述密钥建立第二加密的通信信道；和

（h）通过所述的第二加密的通信信道从所述移动台接收授权信息；和其中

如果所述授权信息被接受，则所述步骤（f）建立所述第一加密的通信信道。

20.权利要求 19 的方法，其中

所述步骤（f）利用所述密钥，建立所述第一加密的通信信道作为加密和认证通信信道；和

所述步骤（g）利用所述密钥，建立所述第二加密的通信信道作为加密和认证通信信道。

21.权利要求 19 的方法，其中所述第二加密通信信道是话音信道。

22.权利要求 13 的方法，其中所述步骤（a）接收始发呼叫请求作为所述系统接入请求。

23.权利要求 13 的方法，还包括：

（g）通过所述第一加密通信信道，发送机密信息到所述移动台。

24.权利要求 23 的方法，其中所述机密信息是根密钥。

# 说　　明　　书

## 在无线系统中加密无线通信的方法

与本申请同时提交的下列各申请是与本申请的主题相关的，并以这些申请的整体援引于此以资参考，这些申请是：发明人为本申请的发明人、申请号未定的、名称为 METHOD FOR TWO PARTY AUTHENTICATION AND KEY AGREEMENT 的申请；发明人为本申请的发明人、申请号未定的、名称为 METHOD FOR UPDATING SECRET SHARED DATA IN A WIRELESS COMMUNICATION SYSTEM 的申请；发明人为本申请的发明人、申请号未定的、名称为 METHOD FOR TRANSFERRING SENSITIVE INFORMATION USING INTIALLY UNSECURED COMMUNICATION 的申请；和发明人为本申请的发明人和 Adam Berenzweig、申请号未定的、名称为 METHOD FOR ESTABLISHING A KEY USING OVER-THE-AIR COMMUNICATION AND PASSWORD PROTOCOL AND PASSWORD PROTOCOL 的申请。

本发明涉及一种用于在无线系统中加密无线通信的方法。

在无线通信系统中，一般被移动用户购买的经常称为移动台的手机人网要到网络服务提供商处，和将长的密钥和各参数输入到该手机以启动服务。服务提供商的网络还保持和与该移动台用于该移动台的长密钥和各参数的联系。众所周知，基于这些长密钥和各参数，信息可以在网络和移动台之间无线保密地进行传递。

另外一种情况下，与电话/陆地线路一样，用户通过加密的通信信道从服务提供商接收长(long)密钥，和一般必须输入这些码到该移动台中。

因为长密钥和参数的传送是经电话/陆地线路或在与无线方式不同的网络提供商的方式执行的，这种传送在防备无线攻击是保密的。但是，这种保密传送信息的方法对移动用户来说增加了某些负

担和限制。最好是，移动用户将能够购买他的手机，然后从任何服务提供商获得服务，而不必须实地带着手机到提供商的地点或者必须手动地和无差错地输入长密钥到移动台中。远端启动和装备移动台的能力是北美无线标准的一部分，和被称为“无线装备”（OTASP）。

当前，北美蜂窝标准 IS41-C 规范了 OTASP 协议，该协议利用公知的 Diffe-Hellban（HD）密钥协定建立两方之间的加密密钥。图 1 表示建立移动台 20 和 IS41-C 中使用的网络 10 之间的加密密钥的 HD 密钥协定的应用。即，图 1 以简化以便清楚的方式表示按照 HD 密钥协定在网络 10 和移动台 20 之间的通信。按照在这里的使用，术语网络是指；认证中心、原始位置寄存器、正在访问位置寄存器、移动通信交换中心、和由网络服务提供商操作的基站。

网络 10 产生随机数 $R_N$，和计算（模 p g∧$R_N$）。如图 1 所示，网络 10 发送 512 比特素数 p、由素数 p 产生的群的生成元 g、和（模 p g∧$R_N$）到移动台 20。接下来，移动台 20 产生随机数 $R_M$，计算（模 p g∧$R_M$），和发送（模 p g∧$R_M$）到网络 10。

移动台 20 将从网络 10 接收到的（模 p g∧$R_N$）提高到功率 $R_M$ 以得到（模 p g∧$R_MR_N$）。网络 10 将从网络 20 接收到的（模 p g∧$R_M$）提高到功率 $R_N$ 以得到（模 p g∧$R_MR_N$）。移动台 20 和网络 10 得到同样的结果，并且建立 64 个最低有效位作为被称作 A 密钥的长存密钥的或根密钥。A 密钥作为用于得到在移动台 20 和网络 10 之间的保密通信中使用的其它密钥的根密钥。

利用 HD 密钥交换的问题之一是对人在中间的攻击（man-in-the-middle attack）的未经认证和敏感的问题。例如，在上述移动通信网的双方的例子中，一个攻击者可以假冒网络 10 和然后再对网络假冒移动台 20。这种方式的攻击者可以选择和知道 A 密钥，按照 A 密钥它在移动台 20 和网络 10 之间中继消息，满足认证的要求。该 HD 密钥交换还对号码簿攻击敏感。

按照本发明的在无线系统中用于加密无线通信的方法哑装

OTASP 呼叫作为正常系统接入来挫败攻击。按照本发明，移动台发送系统接入请求和与系统接入请求相关的哑数据到网络。网络响应该系统接入请求和哑数据发送包含第一数据部分的第一数据流到移动台。移动台从该第一比特流中提取该第一数据部分和发送包含第二数据部分的第二比特流到网络。网络从第二数据流中提取第二数据部分。

移动台和网络两者基于第一数据部分和第二数据部分产生一个密钥，和利用该密钥建立第一加密的和经认证的通信信道。然后，移动台通过第一加密的和经认证的通信信道传送授权信息到网络。如果被接受，则建立第二加密的和经认证的通信信道。通过第二加密的和经认证的通信信道，然后网络发送诸如根或 A 密钥之类的机密信息到移动台。

监视按照本发明的移动台和网络之间通信的一个攻击者可能认为该通信作为一种正常的系统接入，和可能发动一次攻击失败。但是，如果发动攻击，攻击者必须中断相当数量的系统接入，找到哑装的 OTASP 呼叫。这种否定许多移动用户的服务使得定位和停止一个攻击者相当容易。

从下面给出的详细描述和各个附图使得本发明变得更全面的被理解，这些描述和附图仅以说明的方式给出的，其中相同的标号在各个附图中代表对应的部件，和其中：

图 1 表示按照本发明的 Diffe-Hellban 密钥协定网络和移动台之间的通信；和

图 2 表示按照本发明的实施例在网络和移动用户之间的通信。

按照本发明的系统和方法通过哑装作为正常系统接入，保护移动台 20 和网络 10 之间无线的信息传送。仅为了讨论的目的，按照本发明的系统和方法将相对于通过哑装作为呼叫方接入系统的传送来描述 A 密钥的传送。

正如前面所描述的那样，在服务提供期间，移动台 20 和网络 10 需要建立 A 密钥，以便以后的加密通信。按照本发明在这个初始化

处理期间，诸如当移动台 20 首次被启动时，移动台 20 产生一个随机数 DID 作为对移动台 20 的哑识别数，和产生另外的随机数 DMIN 作为对移动台 20 的哑电话号码。然后，如图 2 所示，移动台 20 通过一个接入信道发送始发呼叫请求、哑识别数 DID 和哑电话号码 DMIN 到网络 10。图 2 表示按照本发明的一个实施例网络 10 和移动台 20 之间的通信。

因为哑识别数 DID 和哑电话号码 DMIN 是哑数值,网络 10 不能识别哑识别数 DID 和哑电话号码 DMIN 作为合法的号码。这种情况可能由于差错或因为移动台进行尝试建立一个哑装 OTASP 而发生。网络 10 通过话音信道发送一个第一比特流到移动台 20 继续“假装”该呼叫正常。该第一比特流可以是预定的和预先存储的的比特流或随机产生的比特流，但是，是从加密的话音信道中的比特流无法区分的。然而，网络 10 在第一比特流的第一预定位置发送（模 p g $\wedge R_N$），它是由移动台 20 和网络 10 双方预先存储的。

移动台 20 从第一比特流中提取（模 p g$\wedge R_N$），和产生随机数 $R_M$。移动台 20 计算（模 p g$\wedge R_M$），和还计算（模 p g$\wedge R_N$）$\wedge R_M$，它等于（模 p g$\wedge R_N R_M$）。移动台 20 选择（模 p g$\wedge R_N R_M$），它的一个散列、或它的一部分作为对话密钥 SK。移动台 20 还通过话音信道发送第二比特流到网络 10。第二比特流可以是一个预定的和预先存储的比特流或者随机产生的比特流，但是无法区别于加密信道中的其他比特流。然而，移动台在第二比特流的第二预定位置发送（模 p g$\wedge R_M$），它是由移动台 20 和网络 10 两者预先存储的。该第一和第二预定位置可以是相同的或是不同的。

网络 10 从第二比特流中提取（模 p g$\wedge R_M$），和计算（模 p g $\wedge R_N$）$\wedge R_N$，它等于（模 p g$\wedge R_N R_M$）。网络 10 选择（模 p g$\wedge R_N R_M$），它的一个散列、或它的一部分作为对话密钥 SK。和按照移动台 20 所作的方式一样。因此，网络 10 和移动台 20 已经建立起相同的对话密钥 SK。

接下来，在预定是时间周期以后（例如，10 秒），按照诸如 IS41-C

之类的公知的协议利用对话密钥 SK 作为根密钥（A 密钥），对网络 10 和移动台 20 之间通过话音信道的通信进行加密。再有，话音信道是利用诸如 HMAC 之类的算法的公知消息认证算法进行认证的消息。

然后，移动用户将授权信息（例如，用于计费的信用卡号，等）通过加密和认证的话音信道传送到网络。一旦授权信息已经被网络 10 检验，网络 10 通过控制信道发送 A 密钥到移动台 20，这个信道是按与话音信道一样的方式加密和认证的。

在加密和认证的 A 密钥传送完成后，网络 10 和移动台 20 基于 A 密钥具体形成通信。

最好是，诸如 IS41-C 协议之类用于加密的协议被进行简化，和公开在由同一发明人同时提交的两件申请之一执行认证，这件申请的名称为："METHOD FOR TWO PARTY AUTHENTICATION AND METHOD FOR PROTECTING TRANSFER OF INFORMATION OVER AN UNSECURED COMMUNICATION CHANNEL"。由本发明人同时提交的申请的名称为："METHOD FOR TWO PARTY AUTHENTICATION AND METHOD FOR PROTECTING TRANSFER OF INFORMATION OVER AN UNSECURED COMMUNICATION CHANNEL"。两者都援引在这里供参考。

一个监视网络 10 和移动台 20 之间通信的攻击者可能识别呼叫请求，和接着相信一次呼叫基于通过话音信道上的数据传送已经在进行。因为第一和第二比特流不传送可识别的话音信息，攻击者必须假设话音信道是加密的。但是，在网络 10 产生对话密钥 SK 后直至一个预定的时间周期不将话音信道变为加密的。

对于攻击者按照人在中间的仅有的方法是与正在进行的各呼叫一起进行的，和希望该各呼叫之一是上面描述的 OTASP 呼叫。为了具有找到 OTASP 呼叫的任何明显的概率，攻击者不得不中断大多数呼叫，因为 OTASP 呼叫是一个罕见的事件。但是，始发呼叫是经常的。因此，如果攻击者正在中断大多数呼叫，使得服务被拒绝，这

样变得容易发现攻击者。这样对发现攻击的来源和对移动用户恢复服务也是更重要。

上面讨论的本发明的实施例假设移动台 20 和网络 10 每个都存储一个预定的素数 p 和预定的 p 的生成元 g。作为一种代替方案，素数 p 和生成元 g 利用任何用于安全发送素数 p 和生成元 g 的公知技术被安全地从一方发送到另一方。

本发明从而已经进行了描述，但显而易见本发明可以被按多种方法进行变化。这些变化并不被视为脱离了本发明的精神和范围，和所有这些修改都将被包括在下列权利要求书的范围内。

# 说　明　书　附　图

图1
（现有技术）

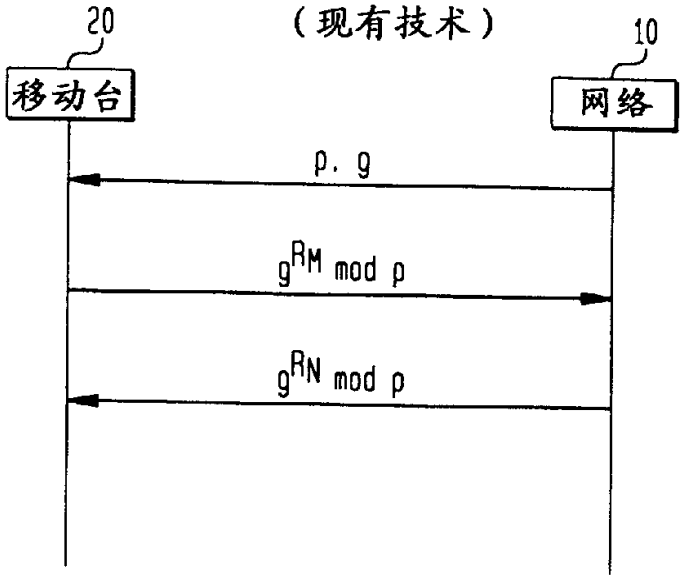



图2