[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/20
H04B 7/26 H04K 1/00
H04L 9/00

[12] 发明专利说明书

[21] ZL 专利号 02116600.5

[45] 授权公告日 2005 年 3 月 9 日

[11] 授权公告号 CN 1192649C

[22] 申请日 2002.4.12 [21] 申请号 02116600.5

[71] 专利权人 华为技术有限公司
地址 517057 广东省深圳市科技园科发路华为用户服务中心大厦知识产权部
[72] 发明人 程 军
审查员 杨瑞丽

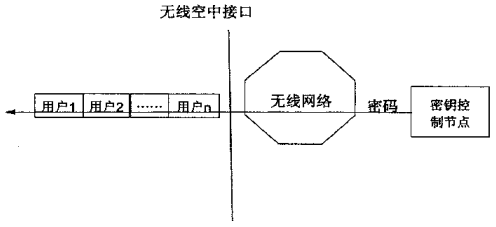
[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 逯长明

权利要求书 1 页 说明书 5 页 附图 3 页

[54] 发明名称 移动通信系统中向移动终端发送密码信息的方法

[57] 摘要

本发明涉及一种移动通信系统中向移动终端发送密码信息的方法。该方法包括：首先，移动通信系统中网络侧将需要向多个移动终端发送的密码信息分别采用公开密钥加密机制进行加密；然后，将加密后的密码信息进行封装，封装后的消息包通过广播/多播的方式向各移动终端发送；最后移动终端采用私有密钥对接收的加密后的密码信息进行解密，便可获取相应的密码信息。本发明中密钥控制节点与移动终端之间仅需要建立一条连接，即可以进行多个移动终端密码信息的发送；并且密码信息都作了加密处理，移动终端通过私有密钥进行解密后便可获取相应的业务密码。本发明具有节省移动通信系统中的带宽资源和信道资源及可以减少网络结点的负荷的优点。



ISSN1008-4274

1、一种移动通信系统中向移动终端发送密码信息的方法，包括：

(1)移动通信系统中网络侧将需要向多个移动终端发送的密码信息分别采用公开密钥加密机制进行加密；

(2)将加密后的密码信息进行封装，封装后的消息包通过多媒体广播/多播业务向各移动终端发送；

(3)移动终端采用私有密钥对接收的加密后的密码信息进行解密，获取相应的密码信息。

2、根据权利要求 1 所述的移动通信系统中向移动终端发送密码信息的方法，其特征在于所述的封装后的消息包包括：移动终端身份标识字段、移动终端的密码信息长度字段及密码信息内容字段。

3、根据权利要求 1 所述的移动通信系统中向移动终端发送密码信息的方法，其特征在于所述的封装后的消息包包括：移动终端身份标识字段和移动终端的密码信息内容字段。

4、根据权利要求 2 或 3 所述的移动通信系统中向移动终端发送密码信息的方法，其特征在于所述的步骤(3)包括：

(41)移动终端根据移动终端的身份标识接收消息包中相应的加密后的密码信息：

(42)移动终端采用私有密钥对加密后的密码信息进行解密，获取相应的密码信息。

移动通信系统中向移动终端发送密码信息的方法

技术领域

本发明涉及移动通信领域(GSM/WCDMA/CDMA)，尤其涉及一种移动通信系统中向移动终端发送密码信息的方法。

背景技术

在移动通信网络中，移动终端为了完成特定业务需要通信网络为其发送相应的业务密码，包括对用户相应的业务密码的更新，例如进行MBMS（多媒体广播/多播系统）业务密码的更新，MBMS业务由于是收费项目，所以需要进行加密传送，当有的用户出现欠费时，网络应当更新密码禁止该用户继续接收相应消息。目前，移动通信网络需要进行业务密码发送时，首先需要在网络侧与移动终端之间建立点对点连接，然后通过建立的连接进行密码信息的发送，如图1所示。这样，密码分发模块需要与每个需要接收密码的移动终端之间建立点对点连接，以实现分别为每个移动终端发送密码。

由上述现有技术可以看出，目前移动通信系统中所采用的向移动终端发送密码的方法存在以下缺点：1、在移动通信系统的网络侧同时需建立多条连接，当系统中用户很多时会降低网络结点的性能，影响网络通信的正常进行；2、通过每个连接发送的消息都具有独立的消息包头，大大地浪费了通信网络的带宽资源；3、在移动通信系统的无线空中接口，需为

每个移动终端建立一处独立的空中信道进行消息的发送，浪费了有限的无线通信资源。

发明内容

本发明的目的是提供一种移动通信系统中加密消息的发送方法，以使移动通信系统中的网络侧可在节约无线通信资源的情况下可靠地向移动终端发送密码信息。

本发明的目的是这样实现的：移动通信系统中向移动终端发送密码信息的方法，包括：

(1)移动通信系统中网络侧将需要向多个移动终端发送的密码信息分别采用公开密钥加密机制进行加密；

(2)将加密后的密码信息进行封装，封装后的消息包通过多媒体广播／多播业务向各移动终端发送；

(3)移动终端采用私有密钥对接收的加密后的密码信息进行解密，获取相应的密码信息。

所述的封装后的消息包可以包括：移动终端身份标识字段、移动终端的密码信息长度字段及密码信息内容字段。

所述的封装后的消息包还可以包括：移动终端身份标识字段和移动终端的密码信息内容字段。

所述的步骤(3)包括：

(41)移动终端根据移动终端的身份标识接收消息包中相应的加密后的密码信息：

(42)移动终端采用私有密钥对加密后的密码信息进行解密，获取相应的密码信息。

由上述技术方案可以看出，本发明中移动通信系统中采用了多媒体广播／多播业务向移动终端进行密码信息的分发，所发送的密码信息运用公钥机制对其进行加密，以保证每个用户移动终端都可以安全地收到各自的密码信息。参见图 2，本发明中密码分发模块即密钥控制节点与移动终端之间仅需要建立一条连接，即可以进行多个移动终端密码信息的发送，所有移动终端的密码信息都封装在一起通过同一条连接向移动终端发送，同样，无线空中接口也仅需要建立一条广播或多播信道，所有移动终端便可以通过这条信道接收相应的密码信息。另外，为了保证某个移动终端的信息不被其他移动终端窃取，本发明中还将每个移动终端的密码信息都作了加密处理，移动终端只有通过各自的私有密钥进行解密操作方可获取各自所需的密码信息。因此，本发明可以有效地节省移动通信系统中网络侧带宽资源和无线信道资源，并可以减少网络结点的负荷。

附图说明

图 1 为点对点连接的密码信息发送方法示意图；

图 2 为多播密码信息发送方式示意图；

图 3 为公开密钥加密过程示意图；

图 4 为加密封装后的消息包格式 A：

图 5 为加密封装后的消息包格式 B；

图 6 为更新 h4 田 MS 业务密码的处理过程示意图。

具体实施方式

公开密钥加密方法是一种非对称加密机制，每个移动终端(即用户)有两个密钥，一个称为 PuKey(公开密钥)，另一个称为 PrKey(私有密钥)；公开密钥加密机制如图 3 所示，有两个用户 UserA 和 UserB 之间进行通信，UserA 在发送明文信息时，使用 UserB 的 PuKey 对信息进行加密操作，加密后的信息通过网络传送给 UserB，UserB 在收到密文信息后使用自己的 PrKey 对信息进行解密后即可获取明文信息。

本发明所提供的移动通信系统中向移动终端发送密码信息的方法正是采用上述的加密机制对所发送的密码信息进行加密的。

首先，利用公开密钥加密对需向移动终端发送的密码信息进行加密，并将加密后的密码信息进行打包操作；每个移动终端都有 PrKey 和 PuKey 两个密钥，PuKey 为公开信息，通信网络中保存有每个移动终端的 PuKey，网络可利用每个移动终端的 PuKey 对需要发送的密码信息进行加密；而 PrKey 是由移动终端自己保存，用于对移动终端接收的信息进行解密；

然后，再将多个加密后的密码信息组成一个多媒体广播 / 多播消息包进行发送；参见图 4，该消息包包括：用于界定每个用户消息的移动终端消息长度字段、用于移动终端接收自己的密码信息的移动终端 ID(身份标识)及用于承载加密后的密码信息的移动终端消息，其中用户 ID 和消息长度是非加密消息，而为了安全性，移动终端消息内容是经过加密的，加密采用公

开密钥机制实现；如图4所示，加密封装后的消息包中分别承载了需要发送给用户A、用户B、…、用户N的用户ID、用户消息长度及用户消息。

最后，移动终端便可根据自己的ID利用自己的私有密钥获取相应的密码信息，从而获得移动通信系统的网络侧发送给该移动终端的业务密码。

如果每个移动终端消息中只传送密码，并且密码长度相同，则可将消息包中的移动终端消息长度字段省去，令消息包仅包括移动终端 ID 字段和移动终端消息字段，如图5所示，所发送的消息包仅承载了需要发送给用户A、用户B、…、用户N的用户ID及加密后的密码信息。

本发明可应用于 MBMS 业务密码的更新，具体的更新处理过程如图 6 所示，首先，SGSN(服务GPRS业务节点)从密钥控制节点获取每个用户的公钥信息，当MBSC(多媒体广播/多播业务中心)向SGSN发MBMS密钥更新消息时，该消息中带有新的密钥信息，SGSN 则用同一 MBMS 群的每个用户的公钥对新密钥进行加密操作，并生成密钥更新多播消息，将该密钥更新多播消息通过RNC(无线网络控制器)下发给MS(移动终端)，至此便完成一次密码更新的工作过程。移动终端有时可能会错过网络下发的密码更新消息，例如不在服务区或关机；当移动终端无法正常接收业务时，如移动终端的 MBMS 的多播频道信息，移动终端可以向网络侧发起密码更新请求，网络在收到该更新请求后会将更新后的经过加密处理的密码发送给用户，移动终端对收到的加密后的密码进行解密即可获得新密码，如图6中虚线所示。

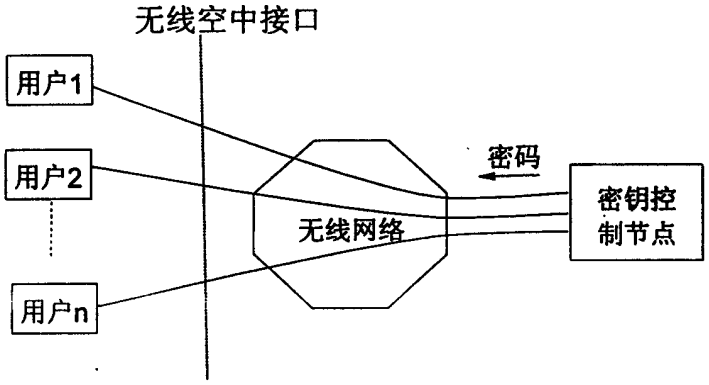

无线空中接口
用户1
用户2
用户n
无线网络
密码
密钥控制节点

图1

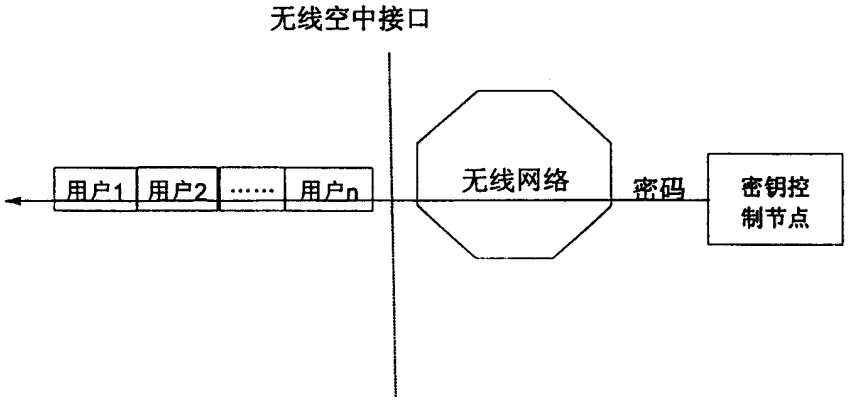

无线空中接口
用户1
用户2
……
用户n
无线网络
密码
密钥控制节点

图2

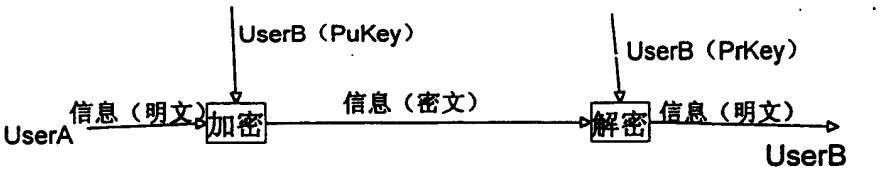


图3

用户A ID	用户A 消息 长度	用户A 消息 内容	用户B ID	用户B 消息 长度	用户B 消息 内容	……	用户N ID	用户N 消息 长度	用户N 消息 内容

图4

用户A ID	用户A 加密密码	用户B ID	用户B 加密密码	……	用户N ID	用户N 加密密码

图5

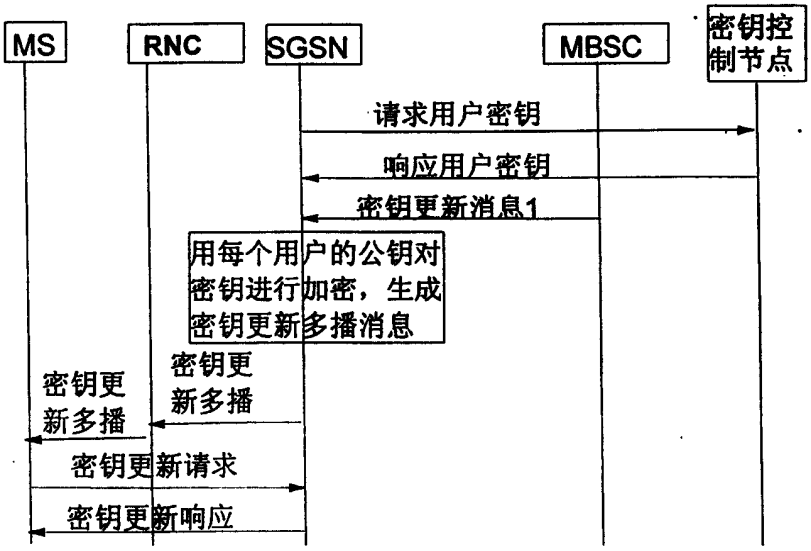

MS
RNC
SGSN
MBSC
密钥控制节点
请求用户密钥
响应用户密钥
密钥更新消息1
用每个用户的公钥对密钥进行加密，生成密钥更新多播消息
密钥更新多播
密钥更新多播
密钥更新请求
密钥更新响应

图6