(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101790155 A
(43)申请公布日 2010.07.28

(21)申请号 200910215596.6

(22)申请日 2009.12.30

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 陈波 鞠飞 袁磊 阳翰凌

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华

(51)Int.Cl.
H04W 8/24(2009.01)
H04W 12/02(2009.01)

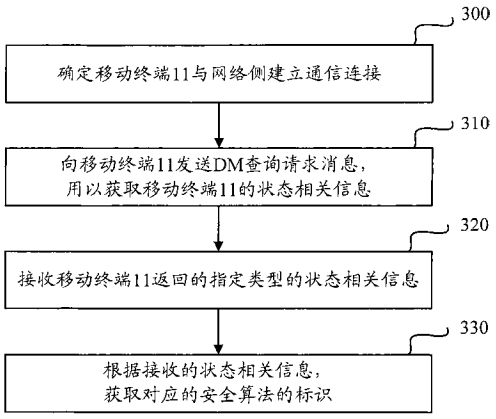
权利要求书 2 页 说明书 5 页 附图 3 页

(54)发明名称

一种更新移动终端安全算法的方法、装置及系统

(57)摘要

本发明涉及通信领域，公开了一种更新移动终端安全算法的方法、装置及系统，该方法为：确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的终端管理DM请求消息；接收移动终端返回的指定类型的状态相关信息；获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法。这样，可以令同型号同批次的移动终端使用不同的安全算法，有效地提高了安全算法的强壮性，避免了某一安全算法被破解时造成的批量破解风险，进而保障了移动终端的使用安全性。本发明同时公开了一种管理服务器、一种移动终端和一种通信系统。



CN 101790155 A

1. 一种更新移动终端安全算法的方法，其特征在于，包括：

确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的终端管理 DM 请求消息；

接收移动终端返回的指定类型的状态相关信息；

获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法。

2. 如权利要求 1 所述的方法，其特征在于，所述确定移动终端与网络侧建立通信连接，包括：

确定移动终端在注册过程中与网络侧建立通信连接；

或者

确定移动终端在申请使用指定类型的通信业务过程中与网络侧建立通信连接。

3. 如权利要求 1 或 2 所述的方法，其特征在于，所述状态相关信息包括所述移动终端的型号、所述移动终端申请使用的通信业务的类型标识和所述移动终端申请保密业务的标志中的一种或任意组合。

4. 一种管理服务器，其特征在于，包括：

发送单元，用于在确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的终端管理 DM 请求消息；

接收单元，用于接收移动终端返回的指定类型的状态相关信息；

处理单元，用于获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法。

5. 如权利要求 4 所述的管理服务器，其特征在于，所述发送单元确定移动终端与网络侧建立通信连接，包括：确定移动终端在注册过程中与网络侧建立通信连接，或者，确定移动终端在申请使用指定类型的通信业务过程中与网络侧建立通信连接。

6. 一种移动终端，其特征在于，包括：

接收单元，用于在本移动终端与网络侧建立通信连接时，接收管理服务器发送的用于获取指定类型的状态相关信息的终端管理 DM 请求消息；

发送单元，用于向所述管理服务器返回指定类型的状态相关信息；

更新单元，用于根据所述管理服务器对应所述状态相关信息下发的算法标识，对本地使用的安全算法进行更新。

7. 如权利要求所述的移动终端，其特征在于，还包括：

Flash 存储单元，用于保存预设的至少两种安全算法。

8. 一种通信系统，其特征在于，包括：

管理服务器，用于在确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的终端管理 DM 请求消息，并接收移动终端返回的指定类型的状态相关信息，以及获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法；

移动终端，用于与网络侧建立通信连接，并根据所述管理服务器的指示对本地使用的安全算法进行更新。

9. 如权利要求 8 所述的通信系统，其特征在于，所述管理服务器确定移动终端与网络

侧建立通信连接，包括：确定移动终端在注册过程中与网络侧建立通信连接；或者，确定移动终端在申请使用指定类型的通信业务过程中与网络侧建立通信连接。

10. 如权利要求 8 或 9 所述的通信系统，其特征在于，所述移动终端在本地 Flash 存储区域内保存预设的至少两种安全算法。

一种更新移动终端安全算法的方法、装置及系统

技术领域

[0001] 本发明涉及通信领域，特别涉及一种更新终端解锁算法的方法、装置及系统。

背景技术

[0002] 随着技术的发展，移动终端已经日益成为个人消费者和商务用户生活中不可缺少的一部分。在移动终端不断演化的过程中，各类网络服务也在不断增多，例如，电子邮件服务、图片信息服务、互联网访问服务、互动游戏服务以及企业应用服务等等。随着移动终端功能的日益复杂，为了提高其运行的安全性，需要对移动终端进行加锁 / 解锁控制。

[0003] 目前采用的加锁 / 解锁制式分为软件锁和硬件锁两种。

[0004] 所谓软件锁即是采用诸如 Hash 算法、DES 算法、RSA 公钥密码算法等等对移动终端内的各种信息 / 应用进行加 / 解锁。而所谓硬件锁即是通过锁卡机或锁网机对移动终端内的各种信息 / 应用进行加 / 解锁；锁卡机机制是令移动终端只认插入的第一张卡，其他卡均不能使用，锁网机机制则是令移动终端只认指定运营商网内的 SIM 卡，其他运营商提供的 SIM 卡均不能使用。由于移动终端通常是被批量生产的，因此，同批次或者同型号的移动终端往往采用相同的软件锁或硬件锁，那么，一旦某个移动终端的软件锁或硬件锁被破解，其他移动终端就存在被批量破解的危险，大大降低了移动终端的使用安全性。

发明内容

[0005] 本发明实施例提供一种更新移动终端安全算法的方法、装置及系统，用以提高移动终端的使用安全性。

[0006] 本发明实施例提供的具体技术方案如下：

[0007] 一种更新移动终端安全算法的方法，包括：

[0008] 确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的 DM 请求消息；

[0009] 接收移动终端返回的指定类型的状态相关信息；

[0010] 获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法。

[0011] 一种管理服务器，包括：

[0012] 发送单元，用于在确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的 DM 请求消息；

[0013] 接收单元，用于接收移动终端返回的指定类型的状态相关信息；

[0014] 处理单元，用于获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法。

[0015] 一种移动终端，包括：

[0016] 接收单元，用于在本移动终端与网络侧建立通信连接时，接收管理服务器发送的用于获取指定类型的状态相关信息的 DM 请求消息；

[0017] 发送单元，用于向所述管理服务器返回指定类型的状态相关信息；

[0018] 更新单元，用于根据所述管理服务器对应所述状态相关信息下发的算法标识，对本地使用的安全算法进行更新。

[0019] 一种通信系统，包括：

[0020] 管理服务器，用于在确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的 DM 请求消息，并接收移动终端返回的指定类型的状态相关信息，以及获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法；

[0021] 移动终端，用于与网络侧建立通信连接，并根据所述管理服务器的指示对本地使用的安全算法进行更新。

[0022] 本发明实施例中，网络侧的管理服务器基于 DM 业务对移动终端进行控制管理，根据移动终端上报的状态相关信息指示其选择相应的安全算法进行更新，从而令同型号同批次的移动终端可以使用不同的安全算法，这样，有效地提高了安全算法的强壮性，避免了某一安全算法被破解时造成的批量破解风险，进而保障了移动终端的使用安全性。

附图说明

[0023] 图 1 为本发明实施例中通信系统体系架构图；

[0024] 图 2A 为本发明实施例中管理服务器功能结构图；

[0025] 图 2B 为本发明实施例中移动终端功能结构图；

[0026] 图 3 为本发明实施例中更新终端解锁算法流程图；

[0027] 图 4 为本发明实施例中 Flash 存储单元示意图。

具体实施方式

[0028] 为了提高移动终端的使用安全性，本发明实施例中，在移动终端内设置了多种加密 / 解锁算法，并在移动终端本身的应用环境发生变化时，由网络侧指示移动终端自动更新其使用的加锁 / 解锁算法（以下称为安全算法），以提高移动终端的使用安全性。其具体为：确定移动终端与网络侧建立通信连接时，向所述移动终端发送用于获取指定类型的状态相关信息的终端管理 (DeviceManagement，DM) 请求消息；接收移动终端返回的指定类型的状态相关信息；获取对应所述状态相关信息保存的算法标识，并指示所述移动终端根据所述算法标识更新其本地使用的安全算法。

[0029] 本发明实施例中，对移动终端进行管理的流程是基于终端管理 (DeviceManagement，DM) 业务进行的，DM 业务是基于 OMA DM 相关标准的移动数据增值业务，它使得运营商实现了通过无线方式对移动终端进行远程管理，即通过 HTTP、WAP 和 OBEX 等通讯方式，利用设备管理命令和命令执行结果，令设备管理服务器对移动终端进行控制和诊断，参数采集和配置，软件升级和安全控制等等操作。DM 业务是基于 OMA SyncML DM 相关标准的移动数据增值业务，运行于手机中的 DM 客户端需要同管理服务器进行协议规定的交互以完成 SyncML DM 功能。

[0030] 下面结合附图对本发明优选的实施方式进行详细介绍。

[0031] 参阅图 1 所示，本发明实施例中，通信系统内包括若干管理服务器 10 和移动终端

11，其中，

[0032] 管理服务器 10，用于在确定移动终端 11 与网络侧建立通信连接时，向移动终端 11 发送用于获取指定类型的状态相关信息的 DM 请求消息，并接收移动终端 11 返回的指定类型的状态相关信息，以及获取对应所述状态相关信息保存的算法标识，并指示移动终端 11 根据所述算法标识更新其本地使用的安全算法；

[0033] 移动终端 11，用于与网络侧建立通信连接，并根据管理服务器 10 的指示对本地使用的安全算法进行更新。

[0034] 参阅图 2A 所示，本发明实施例中，管理服务器 10 包括发送单元 100、接收单元 101 和处理单元 102，其中，

[0035] 发送单元 100，用于在确定移动终端 11 与网络侧建立通信连接时，向移动终端 11 发送用于获取指定类型的状态相关信息的 DM 请求消息；

[0036] 接收单元 101，用于接收移动终端 11 返回的指定类型的状态相关信息；

[0037] 处理单元 102，用于获取对应所述状态相关信息保存的算法标识，并指示移动终端 11 根据所述算法标识更新其本地使用的安全算法。

[0038] 参阅图 2B 所示，本发明实施例中，移动终端 11 包括接收单元 110、发送单元 111 和更新单元 112，其中，

[0039] 接收单元 110，用于在本移动终端 11 与网络侧建立通信连接时，接收管理服务器 10 发送的用于获取指定类型的状态相关信息的 DM 请求消息；

[0040] 发送单元 111，用于向管理服务器 10 返回指定类型的状态相关信息；

[0041] 更新单元 112，用于根据管理服务器 10 对应所述状态相关信息下发的算法标识，对本地使用的安全算法进行更新。

[0042] 如图 2B 所示，移动终端 11 内进一步包括一 Flash 存储单元 113，用于保存至少两种预设的安全算法，采用 Flash 媒介对安全算法进行存储，是为了提供其保存的安全性。

[0043] 基于上述系统架构，本发明实施例中，先在移动终端 11 内预设多种安全算法，以供后续选择时，并默认使用其中的一种算法，本实施例中，假设移动终端 11 内预设有三种安全算法，分别为算法 A、算法 B 和算法 C，其中，算法 A 为移动终端 11 出厂时默认的安全算法。接着，当移动终端 11 进行网络注册时，管理服务器 10 通过 DM 业务对移动终端进行配置，令其不再使用默认的算法 A，而是根据当前的运行环境，选择更为适合的另一种安全算法。这样，移动终端 11 在发生锁卡事件时，就可以根据更新后的安全算法进行鉴权认证（如，PIN 码认证）了。

[0044] 参阅图 3 所示，本发明实施例中，管理服务器 11 对移动终端 10 内的安全算法进行更新的详细流程如下：

[0045] 步骤 300：确定移动终端 11 与网络侧建立通信连接。

[0046] 本发明实施例中，可以所谓移动终端 11 与网络侧建立通信连接，可以是在移动终端 11 进行网络注册的过程中，也可以是移动终端 11 使用指定的通信业务的过程中。

[0047] 步骤 310：向移动终端 11 发送 DM 查询请求消息，用以获取指定类型的状态相关信息。

[0048] 本发明实施例中，所谓状态相关信息可以是移动终端 11 的型号、移动终端 11 申请使用的通信业务的类型标识、或者移动终端 11 是否申请了保密业务的标志，可以是其中的

一种或任意组合。

[0049] 步骤 320 :接收移动终端 11 返回的指定类型的状态相关信息。

[0050] 步骤 330 :根据接收的状态相关信息,获取对应的安全算法的标识。

[0051] 参阅表 1 所示,状态相关信息与安全算法之间的对应关系可以表示为 :

[0052]

状态相关信息	安全算法标识
移动终端型号为 X	算法 B
申请使用 VIP 类业务	算法 C
申请使用保密服务	算法 C
……	……

[0053] 表 1 所示内容仅为举例,状态相关信息与安全算法之间的对应关系可以由管理员根据具体的应用环境而设置,在此不再赘述。

[0054] 步骤 340 :将获得的安全算法标识发送至移动终端 11,指示移动终端 11 对本地默认的安全算法进行更新。

[0055] 例如,移动终端 11 接收到安全算法标识为算法 B,则将本地默认使用的算法 A 更新为算法 B。

[0056] 基于上述实施例,若移动终端 11 在使用过程中出现锁定情况,如,用户使用了非法的 SIM 卡,或者用户输入非法密码等等,在锁定后,移动终端 11 会按照算法 B 的加锁 / 解锁算法的机制,向用户提示相应的对话框,在用户输入合法的 PIN 码后,调用算法 B 进行 PIN 码的校验,若解码成功则令本移动终端 11 恢复正常工作,否则,保持锁定状态,若用户输入错误 PIN 码的次数超过设定阈值,则对移动终端 11 执行锁死操作。

[0057] 步骤 360 :终端恢复正常的使用状态。流程结束。

[0058] 步骤 370 :终端解锁失败,保持目前的锁定状态。注意,如果用户继续尝试输入的话,需要遵守运营商规定的输入允许次数以及超出尝试次数后的限制措施 (如锁死) 等规定。

[0059] 参阅图 4 所示,本发明实施例中,可以将用于进行加锁 / 解锁运算的安全算法存储在安全性较高的存储区域,如, FLASH 区域,可以存在至少两种安全算法,本发明实施例中,以三种算法举例,但并不限于这一种实现方式,还可以是两种、四种、五种等等,在此不再赘述。

[0060] 综上所述,本发明实施例中,网络侧的管理服务器 10 基于 DM 业务对移动终端 11 进行控制管理,根据移动终端 11 上报的状态相关信息指示其选择相应的安全算法进行更新,从而令同型号同批次的移动终端 11 可以使用不同的安全算法,这样,有效地提高了安全算法的强壮性,避免了某一安全算法被破解时造成的批量破解风险,进而保障了移动终端 11 的使用安全性。

[0061] 显然,本领域的技术人员可以对本发明中的实施例进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明实施例中的这些修改和变型属于本发明权利要求

及其等同技术的范围之内，则本发明中的实施例也意图包含这些改动和变型在内。

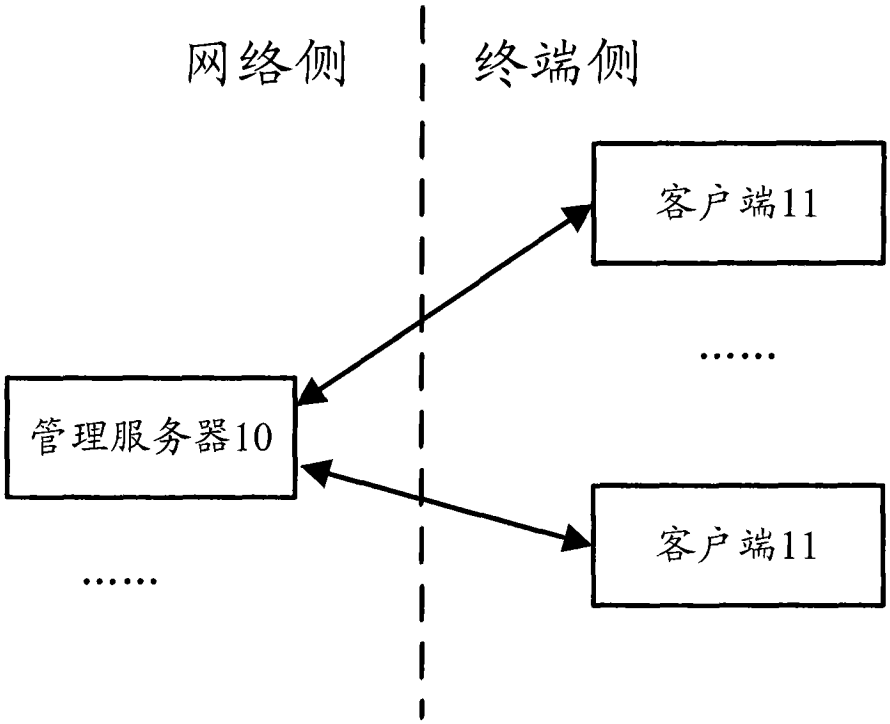

网络侧
终端侧
客户端11
.....
管理服务器10
客户端11
.....

图 1

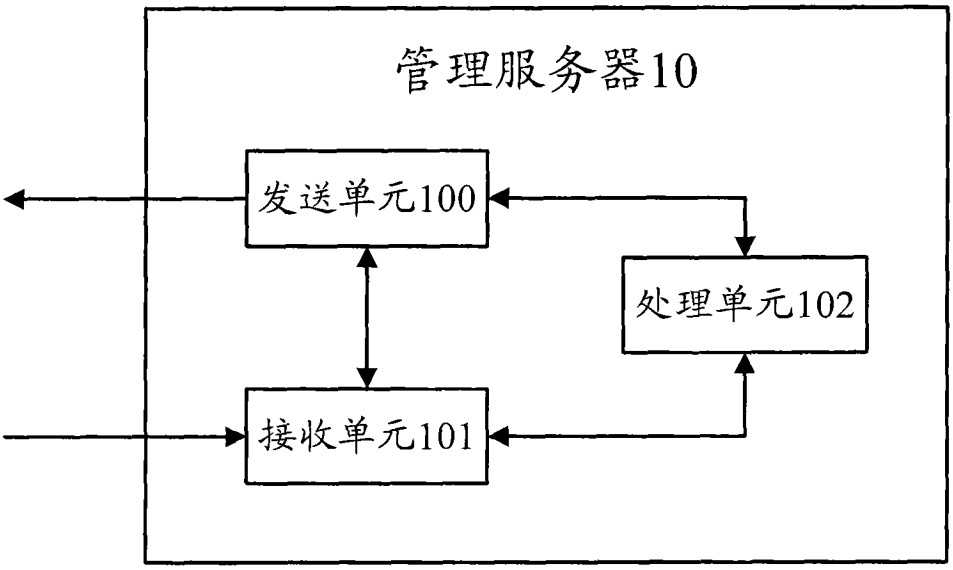

管理服务器10
发送单元100
处理单元102
接收单元101

图 2A

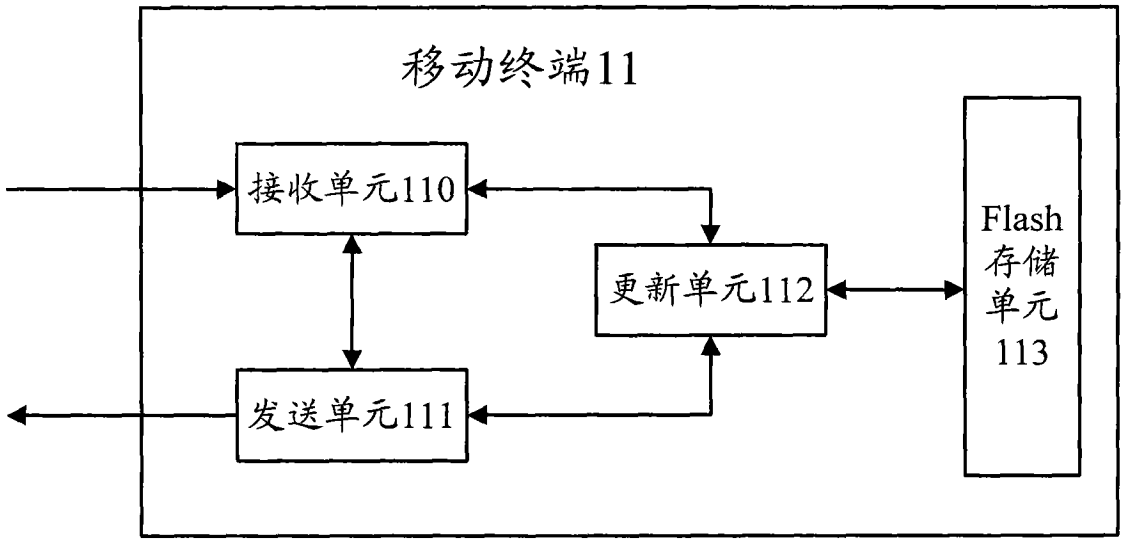

移动终端11
接收单元110
更新单元112
Flash
存储
单元
113
发送单元111

图 2B

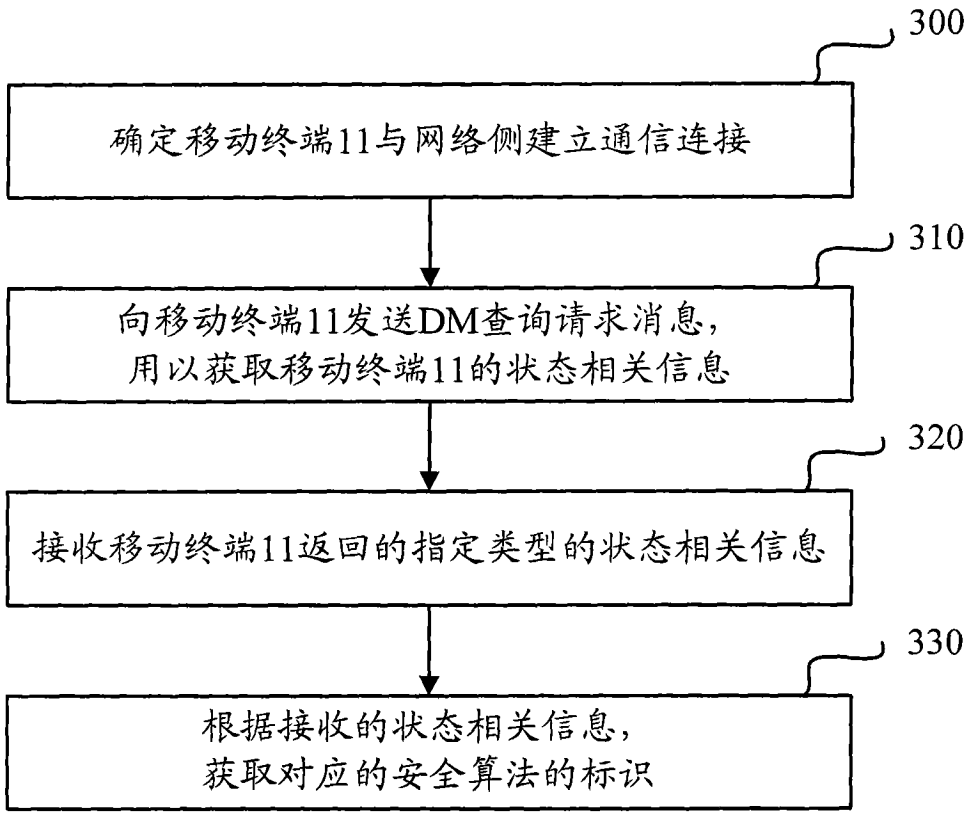

300
确定移动终端11与网络侧建立通信连接
310
向移动终端11发送DM查询请求消息，
用以获取移动终端11的状态相关信息
320
接收移动终端11返回的指定类型的状态相关信息
330
根据接收的状态相关信息，
获取对应的安全算法的标识

图 3

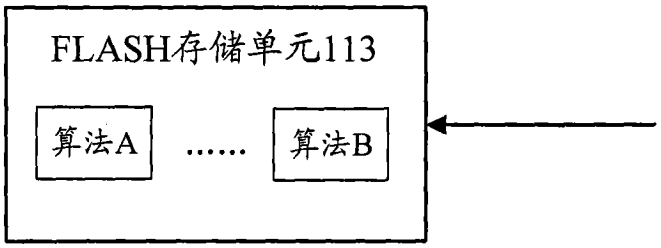


图 4