



(12) 发明专利

(10) 授权公告号 CN 101335798 B

(45) 授权公告日 2013. 11. 06

(21) 申请号 200810144700. 2

(22) 申请日 2008. 06. 27

(30) 优先权数据

11/769342 2007. 06. 27 US

(73) 专利权人 霍尼韦尔国际公司

地址 美国新泽西州

(72) 发明人 C·D·马丁

(74) 专利代理机构 中国专利代理(香港)有限公司
72001

代理人 王庆海 魏军

(51) Int. Cl.

H04M 11/00(2006. 01)

(56) 对比文件

WO 0137589 A1, 2001. 05. 25, 说明书第 6 页

最后一段-第 9 页 19 行, 第 12 页 29 行-14 页 22 行, 图 1-2, 8-12, 权利要求 1-19.

US 2003160681 A1, 2003. 08. 28, 全文.

审查员 李振华

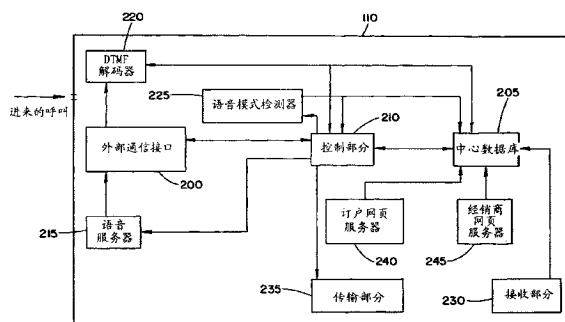
权利要求书3页 说明书9页 附图5页

(54) 发明名称

远程管理与订户账户关联的多个安全系统的方法和网络运行中心

(57) 摘要

本发明涉及利用电话装置对安全系统进行远程控制。用于从电话设备远程控制至少一个本地安全系统的系统和方法。该系统包括用于接收电话呼叫的接收部分, 用于解码呼叫者输入的解码部分和用于接收信息并基于检测出的信息鉴定呼叫者的控制器。该系统也包括语音服务器, 其由控制器控制以用于在系统和呼叫者之间的接口。语音服务器提示呼叫者输入用于鉴定呼叫者的信息, 报告每个本地安全系统的状态并提示呼叫者选择一个特定的本地安全系统以进行控制。该系统包括中心数据库, 其包括分成多个订户记录的订户信息。订户记录包括被授权控制每个本地安全系统的至少一个订户标识符。传输部分发送控制指令到所选定的本地安全系统。



1. 一种远程管理与订户账户相关联的多个安全系统的方法,包括步骤:
 - a) 从电话设备接收电话呼叫;
 - b) 基于呼叫者输入的信息鉴定呼叫者;
 - c) 基于所述鉴定检索所述多个安全系统中的每一个的状态;
 - d) 将所述多个安全系统中的每一个的所述状态转发给该电话设备;
 - e) 从该电话设备接收控制指令和控制密码以用于所述多个安全系统中所选择的一个;
 - f) 将该控制指令和控制密码发送给所选择的安全系统;以及
 - g) 执行控制指令,其中所述方法进一步包括:
判定与订户账户相关联的所述多个安全系统的数目;
分配至少一个电话号码数字给每个确定的安全系统;和
提示订户从所述确定的安全系统中选择特定的安全系统进行控制,其中通过唯一的名称来识别每个所述安全系统并且通过所分配的至少一个电话号码数字来指示每个所述安全系统,所述提示包括确定数目的本地安全系统的列表。
2. 根据权利要求1所述的方法,其中对于与订户账户相关联的所述多个安全系统中的每一个重复步骤 e) -g)。
3. 根据权利要求1所述的方法,进一步包括基于有关电话设备的信息来鉴定呼叫者的步骤。
4. 根据权利要求3所述的方法,其中所述有关电话设备的信息是呼叫者 ID 或 ANI 号码,且基于有关电话设备的信息来鉴定呼叫者包括将从电话呼叫检测到的呼叫者 ID 或 ANI 号码与存储在订户数据库中的呼叫者 ID 或 ANI 号码的列表进行比较。
5. 根据权利要求4所述的方法,其中订户标识符与存储的和所述电话设备相关联的订户标识符进行比较,且订户密码与所存储的和对应于匹配的订户标识符的订户账户相关联的订户密码进行比较。
6. 根据权利要求4所述的方法,其中在所述呼叫者 ID 或 ANI 号码与预先存储的呼叫者 ID 或 ANI 号码相匹配、订户标识符与存储的标识符相匹配以及订户密码与存储的订户密码相匹配且所有存储的匹配信息被包括在相同的订户账户的情况下,允许所述电话呼叫越过鉴定步骤而进行。
7. 根据权利要求1所述的方法,其中所述多个安全系统的每一个位于不同的位置。
8. 根据权利要求1所述的方法,进一步包括步骤:从所述选择的安全系统发送一个确认;且将该确认转发给所述呼叫者。
9. 根据权利要求1所述的方法,进一步包括步骤:基于至少一个授权标准,授予针对所选择的安全系统的呼叫者的控制权力。
10. 根据权利要求9所述的方法,其中所述至少一个授权标准对于多个安全系统中的每一个来说是不同的。
11. 根据权利要求10所述的方法,其中至少一个授权标准是在一天中所述呼叫被接收到的时间。
12. 根据权利要求10所述的方法,其中所述至少一个授权标准是输入的控制指令。
13. 根据权利要求1所述的方法,进一步包括步骤:分配呼叫者使用的经销商特定电话

号码,以便利用所述电话设备访问所述多个安全系统。

14. 根据权利要求 1 所述的方法,进一步包括步骤:维护订户或经销商可访问的网站,所述网站适于接收至少一个订户标识符以使订户授权从其接收控制指令;并且将所述至少一个订户标识符号码存储在中心数据库中的订户记录中。

15. 根据权利要求 14 所述的方法,其中订户记录被经销商修改。

16. 根据权利要求 1 所述的方法,其中所述输入的信息是订户标识符和订户密码。

17. 根据权利要求 16 所述的方法,其中订户标识符与存储的订户标识符相比较并且所述订户密码与存储的订户密码相比较,所述存储的订户密码与对应于匹配的订户标识符的订户帐户相关联。

18. 根据权利要求 17 所述的方法,其中在所述订户标识符与存储的标识符相匹配、以及订户密码与存储的订户密码相匹配、并且匹配信息被包含在相同的订户账户中的情况下,所述电话呼叫允许越过鉴定步骤而进行。

19. 根据权利要求 1 所述的方法,进一步包括基于语音识别鉴定呼叫者的步骤。

20. 根据权利要求 1 所述的方法,进一步包括维护呼叫者访问的历史日志的步骤,包括呼叫时间、订户号码、所访问的信息和控制指令。

21. 一种网络运行中心(NOC),包括:

接收部分,用于从呼叫者接收电话呼叫,所述呼叫者试图控制与订户账户相关联的多个安全系统中的至少一个安全系统;

解码部分,用于解码来自使用电话设备的呼叫者的输入;

控制器,用于接收解码信息且基于检测到的信息鉴定该呼叫者;

由控制器控制的语音服务器,其用于在 NOC 和呼叫者之间接口,该语音服务器针对用于鉴定呼叫者的信息而提示呼叫者,报告所述多个安全系统的每一个的状态,并且提示呼叫者选择特定的安全系统来控制并输入控制指令,所述提示包括确定数目的本地安全系统的列表;

中心数据库,其包括分成多个订户记录的订户信息,该多个订户记录包括至少一个订户标识符,该订户标识符被授权以控制所述至少一个安全系统中的每一个,该订户记录还包括所述安全系统中的每一个的状态,该语音服务器和控制部分被用来访问来自中心数据库的订户信息;以及

传输部分,用于发送控制指令到所选择的安全系统;

其中所述控制器还用于判定与订户账户相关联的所述多个安全系统的数目;分配至少一个电话号码数字给每个确定的安全系统;其中通过唯一的名称来识别每个所述安全系统并且通过所分配的至少一个电话号码数字来指示每个所述安全系统。

22. 根据权利要求 21 所述的 NOC,进一步包括接收部分,用于接收来自所选择的安全系统的确认信号,其指示执行控制指令。

23. 根据权利要求 22 所述的 NOC,其中语音服务器将确认信号转发给呼叫者。

24. 根据权利要求 21 所述的 NOC,其中解码部分是 DTMF 解码器。

25. 根据权利要求 21 所述的 NOC,其中解码部分是语音模式识别单元。

26. 根据权利要求 22 所述的 NOC,进一步包括订户网页服务器,其维护订户可访问的订户网站,该网站适于接收至少一个订户记录,订户授权发送控制指令,该网页服务器将所有

接收到的信息转发到中心数据库。

远程管理与订户账户关联的多个安全系统的方法和网络运行中心

技术领域

[0001] 本发明涉及一种系统和方法,用于从远处控制安全系统。更特别地,本发明涉及从电话装置远程管理安全系统。

背景技术

[0002] 随着人们寻求保护他们自己和他们的财产,例如同时用于商业和家用的安全系统变得平常起来。安全系统包括任何生命、安全、和财产保护系统。典型的安全系统包括位于商业或家庭财产处的安全装置、本地监控站,和网络运行中心。本地监控站和网络运行中心都远离安全装置。

[0003] 典型的,一个用户(或安装者)将安全装置预定或注册到一个中心监控站。该用户将有关安全装置所保护的财产的信息和个人信息提供给本地监控站。每个用户分配一个唯一的账户号码。这些账户号码被存储在本地监控站和网络运行中心的服务器中。

[0004] 安全装置典型地包括中心控制面板,通过有线或无线路径与多个传感器进行通信。控制面板具有下述能力,即通过电话拨号器拨号到远端监控设备或本地紧急状况服务站,将警报情况通知到本地紧急状况服务站和/或本地监控站。一种通信网络装置,例如调制解调器,允许控制面板通过连接到通信网络的通信链路发送和接收信息。通信网络可以是一种电话网络,通信链路可以是电话线;但是,控制面板也可以通过计算机网络发送和接收信息,比如因特网或 GSM。举例来说,计算机网络可以包括 DSL 或线缆调制解调器,和网络接口卡。

[0005] 安全系统还包括用户接口装置,例如具有字母数字键的键盘。这个键盘可以是有线或无线的。典型地,安全装置的所有者可以利用键盘上的按键访问和控制安全装置。可选择地,所有者可能具有远程控制装置,用来发送无线频率信号到键盘以控制所述系统。举例来说,控制装置可以通过按下控制装置上的按钮来允许所有者装备或解除所述装置。

[0006] 可选择地,转让给 Honeywell 国际有限公司的申请号为 11/546865,题为利用近程通信控制安全系统的方法和系统的美国专利,描述了当远程物体邻近目标设备时,通过发送无线频率信号到目标设备,利用远程物体控制安全设备。所有者能够通过持有的远程物体装备或解除安全设备,所述远程物体具备近程通信的能力,当靠近键盘或装备和解除站时控制安全系统。

[0007] 此外,转让给 Honeywell 国际有限公司的申请号为 11/451973,题为利用 SMS 短码消息以方便发送用于安全系统的状态更新的方法和装置的美国专利,描述了一种方法和系统,允许用户从远程装置发送一个状态更新的请求到监控站并且在该远程装置接收状态更新。所有者或操作者可以发送一个预先定义的 SMS 消息到一个接入服务器以产生一个用于远程状态更新的请求。所有者可以预先注册这样的服务,并且定义所有者可以接收什么样的信息。基于预先定义的 SMS 消息,所有者将接收特定的信息。此外,所有者可以发送一个特定的 SMS 以远程修改安全装置的状态,例如装备或解除安全装置。

[0008] 可选择地, Honeywell 国际有限公司已经开发了一种交互式的电话模块, 利用电话装置远程控制安全系统。电话键盘或键区以相同的方式作为用户接口键盘安装在所有者的家里或办公室。利用所述电话装置, 所有者可以在任何地点装备, 解除或检查安全系统的状态。举例来说, VISTA 4286VIP, 它是一种可以从 Honeywell 国际有限公司获得的产品, 用于输入一个想要的控制命令到电话装置, 从而与本地的安全系统直接通信。

[0009] 所有者或操作者可以直接拨打安装有安全设备的家庭或办公室的电话号码, 并且输入电话代码和用户口令码, 随后是电话命令。

[0010] 此外, 申请号为 11/647918, 题为利用电子邮件远程控制安全系统的美国专利描述了一种通过发送电子邮件信息到网络运行中心来远程控制本地安全系统的方法和系统。申请号为 11/647918 的美国专利转让给 Honeywell 国际有限公司。网络中心鉴定发送者并在电子邮件中生成一个针对控制信息的响应。

[0011] 然而, 上述每一种方法和系统一般用于在同一时间控制一个本地安全系统。举例来说, 利用 VISTA4286VIP 模块, 用户直接拨打一个特定的位置并访问本地安全系统本身。该用户只能控制它所拨打的本地安全系统。但是, 订户可能有多个本地安全系统。举例来说, 某一订户可能在主要居住地有一个系统, 另一个在休假地的家里, 并且还有一个在办公室。此外订户可能有一个系统位于多个办公地点。

[0012] 因此, 需要一种系统和方法使得订户或用户无需拨打或发送电子邮件到每一个系统而管理多个本地安全系统。

发明内容

[0013] 因此, 揭示了一种方法和系统, 允许订户或用户通过简单地打电话到一个预先确定的目的地来管理至少一个本地安全系统。订户无需具有一个特定的连接到本地安全系统的模块。所揭示的系统和方法提供一种控制多个本地安全系统的安全方式。

[0014] 远程管理至少一个本地安全系统的方法与订户的账户相关, 包括步骤从一个电话装置接收一个电话呼叫, 基于呼叫者输入的信息鉴定呼叫者, 基于所述鉴定捕获至少一个本地安全系统中每一个的状态, 将至少一个本地安全系统中每一个的状态转发给订户, 接收一个控制指令和控制密码用于选择至少一个本地安全系统中的一个, 发送所述控制指令和控制密码到被选择的本地安全系统, 并由所选择的本地安全系统执行所述控制指令。

[0015] 输入的信息包括订户识别和订户密码。如果订户识别和订户密码都与中心数据库中相应的数据不匹配, 且所述匹配不是来自于同一个订户记录, 将不允许呼叫者控制任何本地安全系统或获得一个本地安全系统的状态。

[0016] 此外, 对于额外的安全, 呼叫者可以通过和电话装置相关联的信息被识别和鉴定, 比如呼叫者 ID 和 ANI 号码。类似地, 如果呼叫者 ID/ANI 与中心数据库中的相应数据不匹配, 且所述匹配不是来自于同一个与订户识别和密码相匹配的订户记录, 将不允许呼叫者控制任何本地安全系统或获得一个本地安全系统的状态。

[0017] 该方法也包括步骤确定与订户的账户相关的本地安全系统的数目, 分配至少一个电话号码数字给每一个确定的本地安全系统并提示订户从所述至少一个本地安全系统中选择一个特定的本地安全系统来控制, 其中每一个所述本地安全系统通过一个唯一的名字被识别并且被电话键盘上的至少一个数字指示。确定数目的本地安全系统目录被提供给呼

叫者。

附图说明

[0018] 参考后面的文本和附图,本发明的这些和其他特性、好处和优点将变得明显,相同的附图标记表示相同的元件,其中:

[0019] 附图 1 是根据本发明一个实施例的系统中的组件的图表。

[0020] 附图 2 示出了根据本发明一个实施例中的网络运行中心的结构图。

[0021] 附图 3-5 示出了根据本发明第一实施例远程控制本地安全系统的方法的流程图。

具体实施方式

[0022] 本发明包括一种方法和系统,允许用户在一个远程的地点通过呼叫一个网络运行中心并在鉴定完用户后输入指令来控制他的本地安全系统。

[0023] 术语“用户”指的是授权控制和访问本地安全系统的特性的任何人,举例来说,一个家庭或办公室的所有者,雇员、或有关的人。用户可以是本地安全公司的一个订户。一个“本地安全系统”指得是安装在家里或办公财产上的设备,用于检测不希望的访问、进入、占有、或在目标空间里出现危险或发生的事件。一个“经销商”指的是一个公司,从安全系统生产者手中买来安全系统,并且将该系统安装给最终用户。经销商监控操作中的本地安全系统。术语自动号码识别(ANI)是电话公司使用的系统,用以识别呼叫者的电话号码。

[0024] 根据本发明,用户可以预先注册订户身份,其被授权发送指令或接收本地安全系统的状态。注册过程将在后面详细描述。可选地,用户可以预先注册一个或多个电话识别号码,这些号码被授权发送一个指令或接收一个状态。可以利用订户标识符和密码两者或电话识别号码识别呼叫者,订户标识符,和订户密码保持安全系统。

[0025] 用户可以有二个安全级别用以访问远程控制系统。在一个实施例中,用户可以决定使用哪个级别鉴定。在另一个实施例中,经销商可以选择鉴定的级别。

[0026] 在另一个实施例中,鉴定也可以利用语音识别来实现。

[0027] 附图 1 示出了根据本发明的控制系统的图表。用户可以利用电话设备 100 呼叫一个预定确定的号码。所述预先确定的号码是经销商特定号码,用以呼叫网络运行中心(NOC)。电话设备 100 可以是能够实现呼叫的任何设备,例如但不限于,计算机、PDA,膝上型电脑,蜂窝电话、电缆电视机顶盒、或 POTS 电话。电话设备 100 将会利用第一通信网络 105 发送呼叫。第一通信网络 105 可以是蜂窝网络,例如 CDMA、GSM,或 PSTN 网络。

[0028] NOC110 将会接收呼叫,识别呼叫者,鉴定呼叫者,接收输入的控制指令,并利用第二通信网络 115 将指令转发到至少一个本地安全系统。第二通信网络可以是任何能够在两个设备间传输数据的通信网络,例如因特网、蜂窝网络(GSM)、PSTN 等等。

[0029] 附图 2 示出了根据本发明的一实施例的网络运行中心 110 的结构图。

[0030] NOC110 包括外部的通信接口,中心数据库 205、控制部分 210、语音服务 215、解码部分或检测部分、例如 DTMF 解码器 220 或语音模式检测器 225、接收部分 230 和传输部分 235。NOC110 也包括订户网页服务器 240 和经销商网页服务器 245。

[0031] 外部通信接口 200 从电话设备 100 接收电话呼叫者。外部通信接口 200 可以是电话插座或蜂窝天线阵列。

[0032] 中心数据库 205 包括所有订户、用户和经销商的信息,包括账户号码、电话号码(呼叫者 ID/ANI)(如果使用的话)、用户密码、控制密码、以及每个本地安全系统的状态。中心数据库也包括语音服务器 215 使用的信息。控制部分 210 控制 NOC110 的功能性。控制部分识别呼叫者并且基于从 DTMF 解码器 220 或语音模式检测器 225 接收到的信息和来自中心数据库 205 的信息授权呼叫者。控制部分 210 可以是微处理器或 FPGA。

[0033] 附图 3-5 中的图表示出了根据本发明的一实施例中的管理方法。附图 3 描述识别和鉴定呼叫者的方法。如图所示,该方法使用了多个级别的识别以保证管理系统的安全。如果不满足任何识别标准的话,系统将不会允许呼叫者控制任何本地系统或接收状态。

[0034] 当用户试图远程控制本地安全系统时,用户产生电话呼叫到 NOC110。该呼叫从电话设备 100 通向预先分配的经销商电话号码。该经销商电话号码是分配给特定的本地经销商的特殊号码。经销商号码是呼叫者联系 NOC110 的一种方式。在步骤 300,外部的通信接口 200 从电话设备 100 接收呼叫。可选地,NO110 可以利用呼叫者 ID 或 ANI 识别呼叫者的电话设备。利用包括在外部通信接口 200 中的标准 DNIS 设备(拨叫号码识别系统)检测 ANI。如果经销商或用户启动了电话号码识别,呼叫者 ID 或 ANI 号码被转发到控制部分 210。在步骤 305,控制部分 210 将判定检测到的呼叫者 ID 或 ANI 号码是否与预先存储在中心数据库 205 中的电话号码匹配。如果检测到的呼叫者 ID 或 ANI 号码与预先存储的号码不匹配,那么语音服务器 215 可选地发出一个访问拒绝消息(步骤 310),呼叫将在步骤 315 被停止。

[0035] 如果呼叫者 ID 或 ANI 号码与预先存储的电话号码匹配,那么在步骤 320,语音服务器 215 发出欢迎消息并且提示呼叫者输入订户标识符。如果呼叫者 ID 被阻塞,也就是说,不可获得的话,控制部分 210 可以拒绝对本地安全系统的控制。经销商可以定制所述欢迎消息。经销商利用经销商网页服务器 245 维护的经销商网站定制欢迎消息。定制的经销商欢迎消息使得经销商能够将他自己与其他与 NOC110 有关的经销商区分开来。

[0036] 可选地,如果经销商或用户没有将电话号码识别启动作为鉴定程序的一部分的话,方法直接进行到步骤 320。

[0037] 欢迎消息是一个语音合成消息,用于提示呼叫者到达了某一特定经销商的管理系统。所述欢迎消息也将给呼叫者提供选项,以识别呼叫者、从一个特定的本地安全系统 120 接收状态更新、选择本地安全系统 120 来控制并输入控制消息。

[0038] 使用电话设备 100 来输入数据。可以使用触摸板或通过扬声器将数据输入到电话设备 100。

[0039] 在步骤 320,语音服务器 215 提示呼叫者按下代表订户标识符的按键或者将订户标识符讲给扬声器。呼叫者将利用电话设备 100 输入消费者标识符。NO110 通过外部通信接口 200 接收订户标识符。在步骤 325,NO110 利用 DTMF 解码器 220 或者语音模式检测器 225 检测并解码订户标识符。解码的订户标识符与中心数据库 205 中预先存储的订户标识符相比较。控制部分 210 搜索中心数据库以寻找是否匹配。在另一个实施例中,控制部分 210 在步骤 330 从与匹配的呼叫者 ID 或 ANI 号码相对应的订户账户记录中找回预先存储的订户标识符。如果解码的订户标识符与中心数据库 205 中的订户标识符不相匹配,控制部分 210 将在步骤 310 促使语音服务器 215 宣布访问被拒绝。在步骤 315,呼叫将被停止。

[0040] 如果在步骤 330,解码的订户标识符与中心数据库 205 中的订户标识符相匹配,控

制部分 210 在步骤 335 将促使语音服务器提示呼叫者输入订户密码。语音服务器 215 将指导呼叫者按下电话设备 100 上表示订户密码的按钮上的键或者将订户密码讲给电话设备 100。NOC110 按照与订户标识符相同的方式接收订户密码,也就是说,外部通信接口 200。在步骤 340, NOC110 根据输入订户密码的方式,利用 DTMF 解码器 220 或语音模式检测器 225 检测并解码订户密码。

[0041] 将被解码的订户密码与中心数据库 205 中预先存储的订户密码进行比较。控制部分 210 在步骤 345 从与匹配的订户标识符相对应的订户记录中找回预先存储的订户密码。如果呼叫者 ID 或 ANI 号码被用于鉴定,订户密码必须与匹配的呼叫者 ID 或 ANI 号码以及订户标识符相对应的订户记录中存储的订户密码相匹配。

[0042] 如果被解码的密码与预先存储的密码不相匹配,控制部分 210 将在步骤 310 促使语音服务器 215 宣布访问被拒绝。在步骤 315,呼叫将被停止。

[0043] 在另一实施例中,如果呼叫者输入一个错误的订户标识符和密码,也就是说,不匹配,控制部分 210 可以促使语音服务器 215 提示呼叫者再次输入订户标识符和密码。根据这个实施例,如果呼叫者输入错误的订户标识符和 / 或密码超过预定的次数,控制部分 210 将断开呼叫且呼叫将被停止。

[0044] 如果被解码的密码与预先存储的密码匹配,呼叫将被鉴定且呼叫者的身份将被获知。上述鉴定过程保证了所有本地安全系统的安全。NOC110 将允许呼叫继续进行且进程移动到步骤 400。

[0045] 在本发明的另一个实施例中,语音识别和确认可以用于鉴定一个呼叫者。呼叫者声音的数字记录将被保存到中心数据库中。当该呼叫者呼叫 NOC110 时,语音模式检测器 225 将呼叫者的声音与保存的数字记录进行匹配。语音识别提供了另一个级别的安全和鉴定。

[0046] 在步骤 400,控制部分 210 将从中心数据库 205 中找回与呼叫者订户标识符和密码相对应的订户记录。控制部分 210 在步骤 405 访问与订户记录有关的所有本地安全系统的状态。

[0047] 一个订户记录可以具有与该记录有关的多个本地安全系统,例如,主住宅和避暑住宅的安全系统。控制部分 210 检索所有本地安全系统的装态。每个安全系统通过一个名称和至少一个电话键盘数字被识别。将使用一个“结束”提示符比如“#”来结束本地安全系统的选择。

[0048] 例如,主住宅可以被标识为“住宅 1”,避暑住宅可以被标识为“避暑 2”。可选地,可以使用例如“1234 高街 1”的地址来代替名称。

[0049] 在步骤 410,控制部分确定与订户记录相关联的本地安全系统的号码。

[0050] 如果只有一个本地安全系统,控制部分 210 在步骤 415 促使语音服务器 215 宣布本地安全系统的状态。

[0051] 语音服务器 215 提示呼叫者利用电话设备 100 输入控制指令。语音服务器 215 指导呼叫者按下或讲出用于给定功能的特定现有号码。举例来说,“按下或者说 2 以指示离开”,或者“按下或者说 3 以指示停留”。

[0052] 呼叫者利用电话设备输入控制指令,举例来说,键盘或者麦克风。NOC110 通过外部通信接口 200 和解码器接收在步骤 465 输入的控制指令。根据该输入,NOC110 将利用 DTMF

解码器 220 或语音模式检测器 225。然后在步骤 470, 控制部分 210 指导语音服务器 215 提示用户输入控制密码。当利用标准键盘时, 控制密码与用于控制本地安全系统 120 的密码相同。举例来说, 宣告可以是“现在输入您的安全密码”。密码是 4 个数字码。呼叫者将利用电话设备 100 上的键盘输入密码或者将密码讲给电话设备。如上面对控制指令的描述, NOC110 以相同的方式接收密码并解码所述密码。

[0053] 一旦控制指令被转发到控制部分 210 且在中心数据库 205 中解码, 指令将以后面描述的方式接着被发送到合适的本地安全系统 120。

[0054] 如果在步骤 410, 控制部分 210 判定与订户记录相关联的本地安全系统 120 的数目, 语音服务器 215 将在步骤 420 指导呼叫者选择本地安全系统以接收状态用于控制。给呼叫者提供一个与订户账户相关联的所有本地安全系统 120 的目录。该目录将通过语音服务器 215 被提供为语音数据。每个本地安全系统被预先分配至少一个数字在电话设备上。举例来说, 如果有九个系统, 将给呼叫者提供选项, 按下或说出 1 至 9, “1”表示本地安全系统 1, “2”表示本地安全系统 2, …第十个本地安全系统 120 可以被分配或标记为“10”。

[0055] 呼叫者通过按下数字或者说出至少一个与想要的本地安全系统 120 相对应的数字来输入所选择的本地安全系统。

[0056] 在步骤 430 利用 DTMF 解码器或语音模式 215, NOC110 解码输入的数据。

[0057] 控制部分 210 在步骤 435 接收解码的选择并报告所选的本地安全系统的状态。在报告了状态后, NOC 提示用户输入控制。步骤 435-455 以分别与步骤 415、460、465、470 和 480 相同的方式执行, 将不再描述它们。

[0058] 一旦控制指令和密码被解码, 指令就被存储到中心数据库 205 并转发到中心部分 210。然后, 指令和密码被发送到所选择的本地安全系统 120。

[0059] 在步骤 500, 利用第二通信网络 115, 指令和 / 或密码将被发送到本地安全系统 120。在一个实施例中, 第二通信网络是因特网。在本地安全系统 120 和 NOC110 之间的因特网连接可以被用作可靠的安全通信。利用传输部分 235 将指令和 / 或密码发送到本地安全系统 120。

[0060] 在发送指令和 / 或密码之前, 控制部分 210 将加密数据。可以利用一种已知的传输方法从 NOC120 发送控制指令或消息, 例如 AlarmNet, 被 Ademco (Honeywell 国际有限公司的一个品牌) 所运行。AlarmNet—由 Ademco 所运行的通信网络利用英特网, 蜂窝网, GSM, Mobitext, 以及其它专利技术。网络既被用来上传和下载警报系统配置和操作数据, 也被用来基于从被保护的房产路由到 NOC110 的事件而作为警报系统的路径。

[0061] 举例来说, 第二通信网络 115 可以是因特网。为了避开防火墙, NOC110 将等待本地安全系统 120 周期性地启动与 NOC110 的接触。一旦会话被打开, NOC110 将发送数据到本地安全系统 120。NOC110 可以利用 AlarmNet- I 通信网络来发送加密的指令数据。AlarmNet- I 是 Honeywell 国际有限公司利用因特网所运行的专有通信网络。该网络用于上传和下载警报系统配置和操作数据。在这个例子中, NOC110 中的传输部分 215 将是一个到因特网的 AlarmNet- I 发送器并且通过一个 AlarmNet- I 接收器在本地安全系统 120 处接收。可选地, NOC110 可以利用基于以太网的发送器通过因特网发送指令。另一个选择是 NOC110 可以利用调制解调器设备, 例如传输部分 215, 在因特网上发送指令。

[0062] 在另一个实施例中, NOC110 可以利用蜂窝网络, 例如 AMPS 或 GPRS, 来发送指令

到本地安全系统 120。举例来说, NOC110 可以包括如传输部分 215、蜂窝天线, 也就是说, AlarmNet C 发送器或 GPRS 发送器。AlarmNet-C (现在对于 GSM 来说是 AlarmNet-G) 是由 Ademco (Honeywell 国际有限公司的一个品牌) 利用蜂窝通信网络承载所运行的专有通信网络。AlarmNet C 发送器将利用 AlarmNet-C 通信网络路由指令。

[0063] 在另一个实施例中, NOC110 可以利用采用模拟音频、频移键控或其他音频模式的标准电话网络来发送指令到本地安全系统 120。

[0064] 控制指令可以是修改本地安全系统 120 特性的任何指令, 包括但不限于停留、离开和解除。

[0065] 在步骤 505, 本地安全系统 120 接收控制指令和密码。用于本地安全系统 120 的控制板将执行所述指令。指令和密码将显示在控制板上就像从本地键盘上所接收到的一样。举例来说, 如果控制板接收指令以解除系统, 控制板将促使本地安全系统解除。当某一用户携带着某物而不能按下键盘时, 这个特性将非常有用。此外, 当用户忘记装备本地安全系统 120 时, 远程特性很重要。

[0066] 一旦指令被执行, 控制板在步骤 510 发送指令被执行的确认。所述确认通过第二通信网络 115 被发送。确认消息被 NOC110 接收到并按照订户记录索引存储到中心数据库中。此外, 利用语音服务器 215, NOC 将在步骤 515 向呼叫者报告确认和本地安全系统的状态的改变。

[0067] 如果超过一个的本地安全系统 120 与订户记录相关联, 在步骤 520, NOC110 将询问呼叫者是否想要控制任何其它本地安全系统。如果呼叫者想控制或获得另一个安全系统的状态, 进程转到步骤 420, 否则呼叫结束。

[0068] 每次用户呼叫 NOC110 以控制本地安全系统 120 或接收状态; NOC110 维持历史日志或登记该呼叫。历史日志包括呼叫的时间, 呼叫者 ID, 访问信息, 输入的控制指令, 和被控制的本地安全系统的识别。订户可以利用订户网站查看历史日志。在另一个实施例中, 历史日志可以通过电话被访问。

[0069] 如上所述, 订户到安全系统可以利用维护的网站为远程控制系统注册且通过 NOC110 中的订户网页服务器 240 进行管理。利用网站, 订户可以在中心数据库 205 中创建一个控制账户。这个账户可以在用户每次呼叫 NOC110 时通过控制部分 210 来访问。该账户可以通过计算机创建或任何能够利用标准网页浏览器连接到因特网的设备创建。订户利用安全系统安装者提供的密码和登录名登录到网站。网站通过公开的 IP 地址公布在因特网上。在网站上输入的信息由订户网页服务器 240 接收并作为数据记录存储在中心数据库 205。

[0070] 用户将在每个输入域输入个人订户信息。个人订户信息可以包括名字、账单地址、账户号码、和受保护的房产的地址。为了激活远程控制特性, 用户可以输入至少一个订户标识符, 根据该订户标识符, 系统被授权接受一个呼叫。订户可以输入超过一个标识符。可选地, 用户可以输入至少一个电话号码, 根据该电话号码, 系统被授权接受一个呼叫。

[0071] 在另一个实施例中, 如果利用了语音识别, 用户可以呼叫一个预先确定的电话号码并输入一个声音样本。经销商将把该电话号码分配给用户。这个号码与用户用以呼叫 NOC110 的号码不同, 例如, 控制本地安全系统或接收状态。用户将被语音服务器或数字菜单提示输入声音样本。用户可以保存所述声音样本或改变现有的声音样本。可以输入多于一

个的不同的声音样本,即,多于一个的人。所述声音样本将被数字化并按照订户记录索引而存储在中心数据库 205。

[0072] 此外,在一个实施例中,订户可以为每个电话号码设置一个授权表。举例来说,如果订户输入多个号码,例如,办公号码和蜂窝电话号码,该订户在办公时间可以只授权来自工作电话号码的呼叫。

[0073] 此外,在一个实施例中,订户可以分配确定的控制权利给每个电话号码。一个电话号码可以完成控制授权。第二号码可能仅仅能够装备本地安全系统 120 而不能解除该系统。相应地,每个授权的呼叫者或电话号码可以具有不同的控制等级或权力。举例来说,商业建筑中的安全官员可以具有最高等级的权力,也就是说,所有功能的完全控制。一个雇员可能仅仅能够装备或解除安全系统。利用网站,订户可以为每个被授权的呼叫者规划每个功能或特性。可选地,订户可以规划被授权的呼叫者不能控制的功能或特性。

[0074] 此外,在另一个实施例中,订户可以设置一个时段,在其间呼叫者具有控制的权力,例如,一个预先确定的时间段,且在这个时段过去之后,呼叫者将不再有任何控制的权力。这个特性具有多个有点。举例来说,雇主可以简单的基于利用一个有效的呼叫时段来控制访问安全系统。如果在工作期间有高的周转率的话,这个有点非常有用。举例来说,电子邮件授权可以在每个周一自动更新。

[0075] 一旦所有想要的控制和授权域被输入到网站,订户网页服务器 205 将把所有的信息转发到中心数据库 205 用于存储作为数据记录。系统接下来将分配一个经销商电话用以呼叫。

[0076] 取决于输入的限制,例如,日期、时间、指令,在进程的不同阶段,控制部分 210 判定限制条件是否满足。举例来说,如果限制是日期或时间,控制部分 210 在检测到呼叫者 ID 或 ANI 号码之后执行判定,也就是说,在步骤 305 之后。控制部分 210 利用它的内部时钟计时并且将接收到的电话呼叫的时间与预先存储的限制时间或时段进行比较,如果有的话。换句话说,即使呼叫者的 ID 或 ANI 匹配,如果电话号码的授权已经超期或者如果接收到的呼叫已经超出了计划安排的时间,访问将被拒绝且呼叫被停止。一旦呼叫者进入一个特定的本地安全系统,也就是说,在步骤 420 之后,这种判定将被重复进行。所述时间是基于订户的本地时间,也就是说安全系统的位置。因此,在存储时间之前,NOC110 将把输入的时间转换成 NOC 本地时间。

[0077] 如果限制是基于输入的控制指令,控制部分 210 在呼叫者输入想要的控制指令之后,也就是说,在步骤 445 和 460 之后,判定限制是否满足。控制部分将输入的控制指令与中心数据库中为特定本地安全系统保存的任何控制限制进行比较。如果输入的指令被禁止,语音服务器 215 通知呼叫者访问被拒绝。

[0078] 每个与订户账户或订户记录相关联的本地安全系统可以对呼叫者具有不同的限制。

[0079] 类似地,经销商可以利用经销商网页服务器维护的经销商网站定制他的经销商参数。经销商参数包括新的订户账户,新的可用特性,和用于远程访问系统的经销商特定欢迎消息。经销商以订户网站相同的方式访问网站,也就是说,利用因特网。一旦数据被输入到经销商网页服务器,该数据就被存储到中心数据库 205。

[0080] 参考特定的示范实施例,在这里描述了本发明。这些替换和修改对本领域技术人

员来说是显而易见的,没有超出本发明的范围。示范实施例只是示例性的,而不是用来限制本发明的范围,本发明的范围由所附的权利要求来定义。

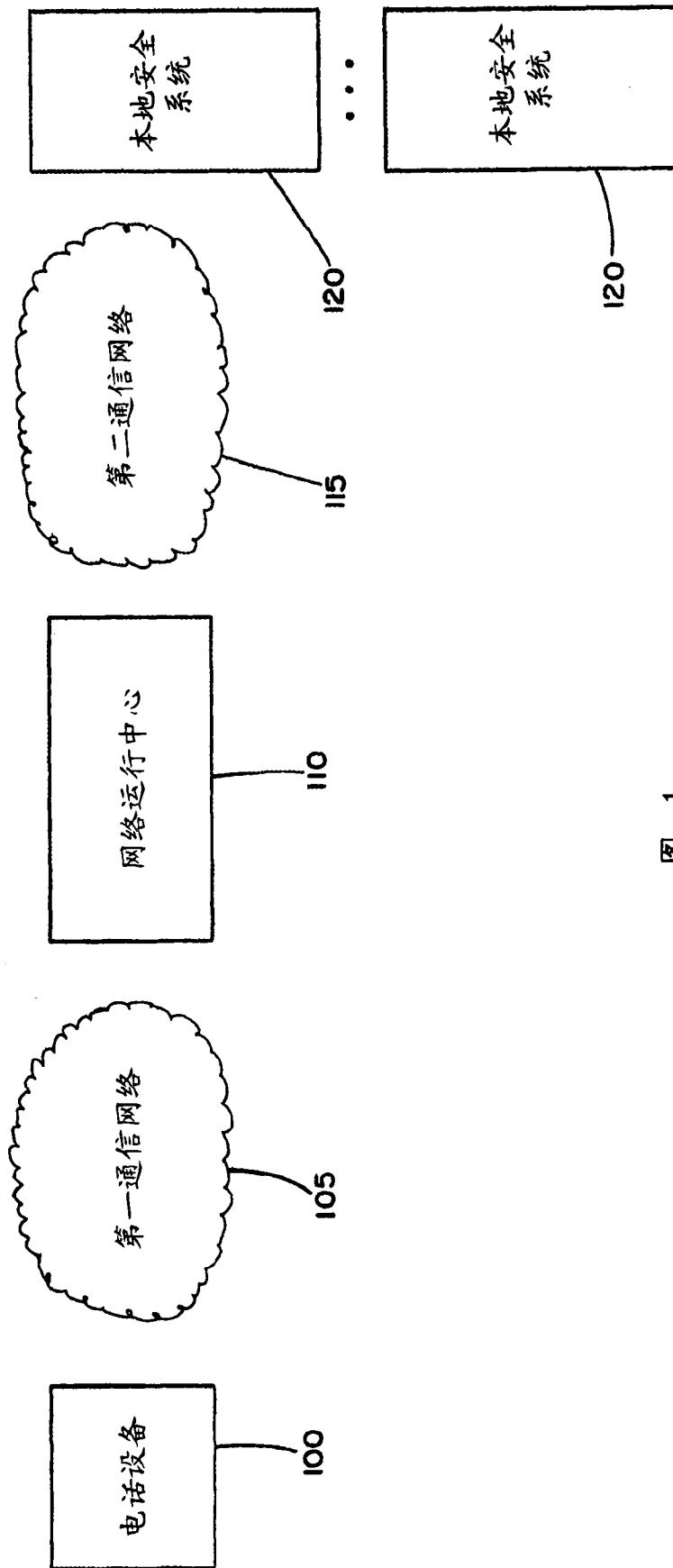


图 1

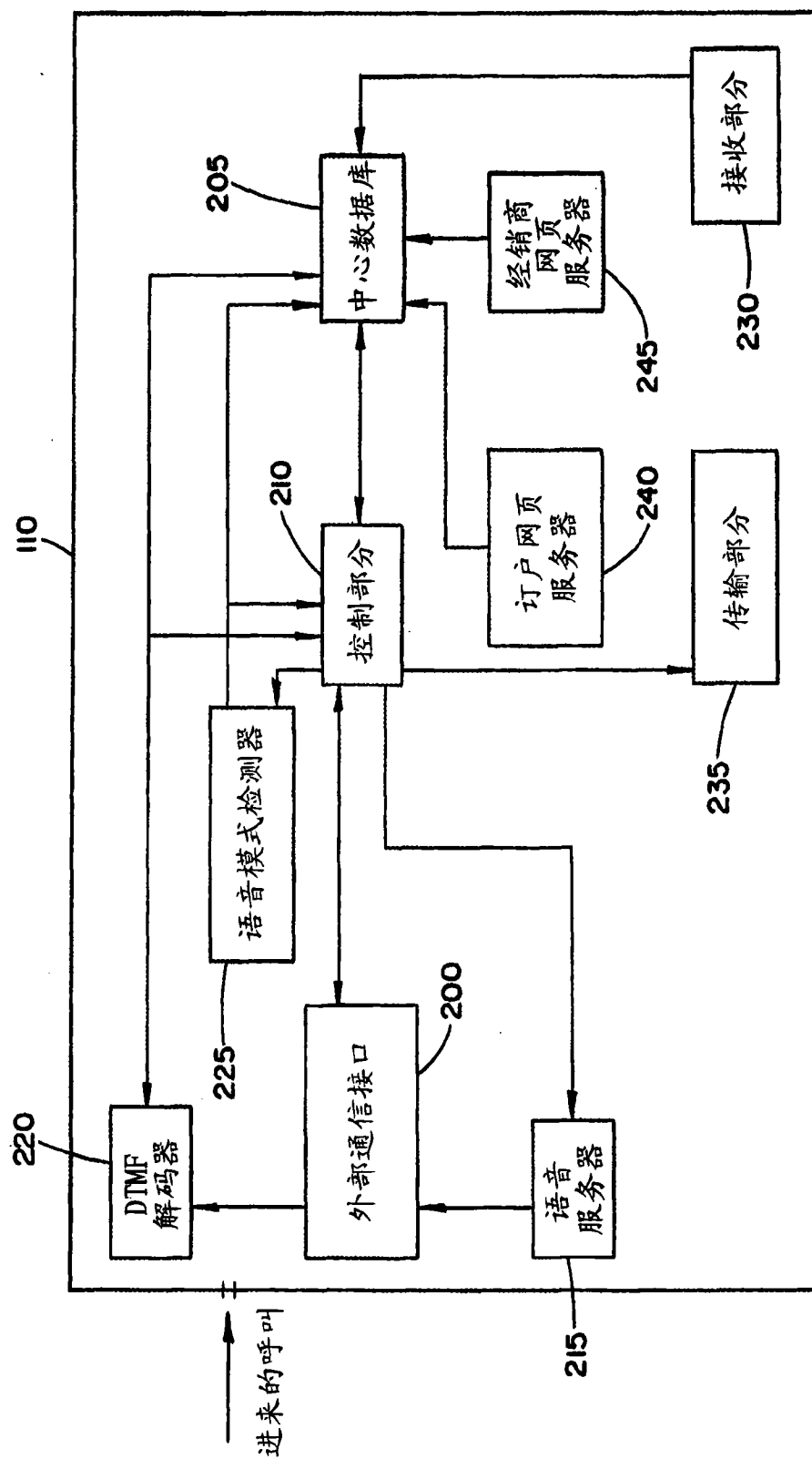


图 2

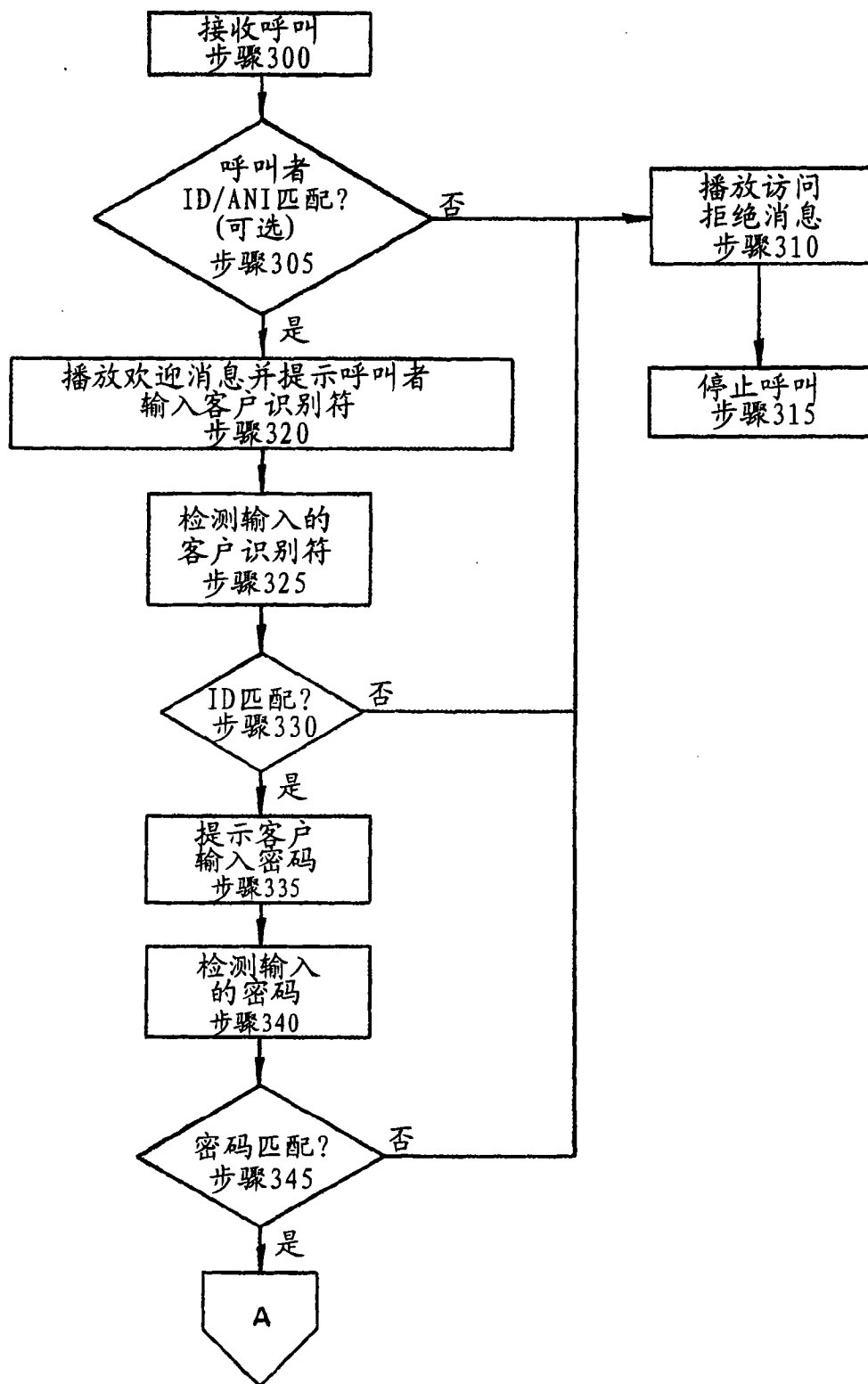


图 3

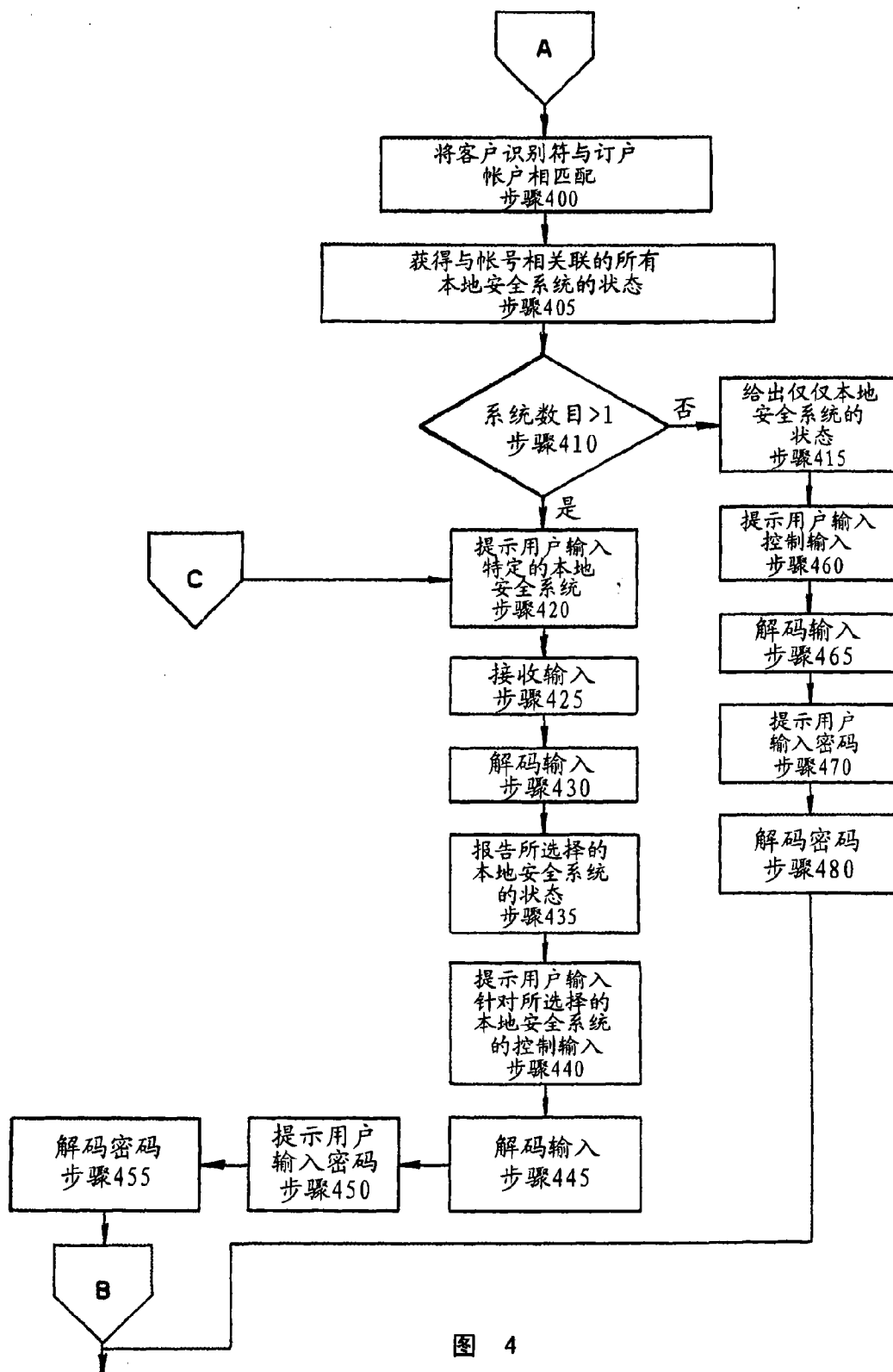


图 4

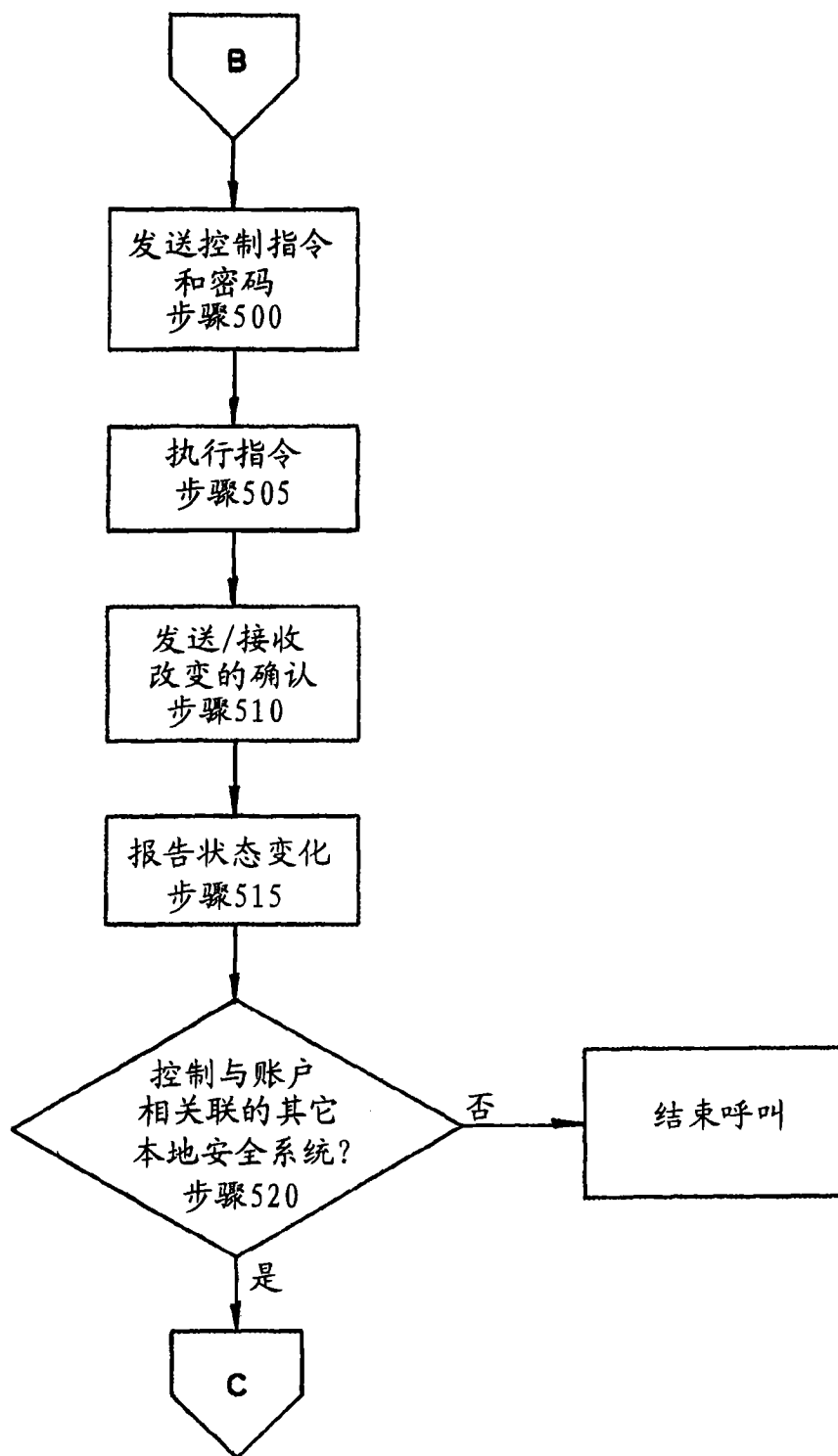


图 5