[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38

[12] 发明专利说明书

[21] ZL 专利号 98807747.7

[45] 授权公告日 2003 年 10 月 15 日

[11] 授权公告号 CN 1124766C

[22] 申请日 1998.7.31 [21] 申请号 98807747.7
[30] 优先权
[32] 1997. 8. 1 [33] US [31] 60/054,440
[86] 国际申请 PCT/US98/15995 1998.7.31
[87] 国际公布 WO99/07178 英 1999.2.11
[85] 进入国家阶段日期 2000.1.31
[71] 专利权人 夸尔柯姆股份有限公司
地址 美国加州圣地埃哥
[72] 发明人 S·K·布罗伊勒斯
小 R·F·奎克
审查员 凌 林

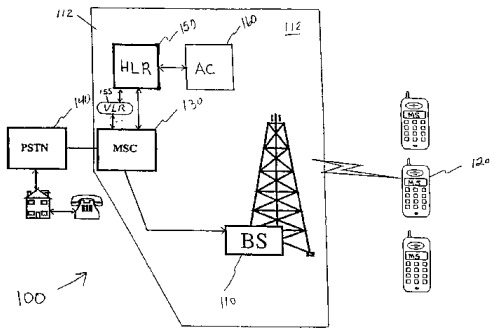
[74] 专利代理机构 上海专利商标事务所
代理人 李 湘

权利要求书 3 页 说明书 8 页 附图 4 页

[54] 发明名称 在无线通信中防止应答攻击的系统和方法

[57] 摘要

一种确认通信网络内移动站身份的方法和装置。 移动站发送安全值以访问网络。 系统在允许其访问网络之前对移动站认证。 如果移动站发送的安全值与先前发送的安全值匹配，则系统在允许其访问之前完成额外的程序。 利用本发明系统防止了入侵者的重现攻击企图。



ISSN1008-4274

1.一种通信网络内部的基站，其特征在于包括：

接收来自基站范围内至少一个移动站的传输的接收机；

将第一所接收传输与第二所接收传输进行比较的比较器，其中响应于站点发送的询问，第一所接收传输和第二所接收传输每一个都传送认证信息；以及

处理器，配置为处理第一所接收传输中的认证信息以及第二所接收传输中的认证信息，并且如果比较显示第二所接收传输的认证信息匹配第一所接收传输的认证信息，则重新询问发送第二所接收传输的移动站。

2.一种确认通信网络内部移动站身份的方法，其特征在于包括以下步骤：

从基站向移动站发送询问；

将第一所接收传输与第二所接收传输进行比较，其中响应于站点发送的询问，第一所接收传输和第二所接收传输每一个都传送认证信息；以及

如果比较结果显示第二所接收传输的认证信息匹配第一所接收传输的认证信息，则从基站向第二所接收传输的发信方发送重新询问。

3.一种防止通信网络内重现攻击的系统，其特征在于包括

至少一个站点，它被配置为：

从移动站接收公共安全参数和认证签名，所述认证签名使用所述公共安全参数和个人安全参数产生；

将移动站传送的公共安全参数与先前由移动站使用的至少一个公共安全参数进行比较；以及

如果先前使用了由移动站传送的公共安全参数，则向移动站发送信的公共安全参数，并且请求移动站根据个人安全参数和新的公共安全参数产生且向至少一个站点发送新的认证签名。

4.如权利要求3所述的系统，其特征在于所述至少一个站点为基础结构单元的组合。

5.如权利要求4所述的系统，其特征在于基础结构单元的组合包括：

(a)基站；

(b)移动交换中心；以及

(c)主位置寄存器。

6.如权利要求4所述的系统，其特征在于基础结构单元的组合进一步包括：

(a)认证中心；以及

(b)访问者位置寄存器。

7. 一种认证通信网络内站点的系统，其特征在于包括：

至少一个基站，用于：

从移动站接收公共安全参数和认证签名，其中所述认证签名使用所述公共安全参数和个人安全参数产生；

将移动站传送的公共安全参数与先前从移动站接收的至少一个公共安全参数进行比较；以及

如果移动站传送的公共安全参数匹配先前接收的移动站的公共安全参数，则要求对来自移动站的身份进行额外验证。

8. 一种用于对通信网络内移动站认证的系统，其特征在于包括：

从移动站接收公共安全参数和认证签名的装置，其中所述认证签名使用所述公共安全参数和个人安全参数产生；

将移动站传送的公共安全参数与先前从移动站接收的至少一个公共安全参数进行比较的装置；以及

如果移动站传送的公共安全参数匹配先前接收的移动站的公共安全参数，则要求对移动站的身份进行额外验证的装置。

9. 一种用于对通信网络内移动站认证的系统，其特征在于包括

从移动站接收信号并在允许访问通信网络之前对移动站进行认证的至少一个基站，每个站点配置为如果移动站试图利用与由相似识别的移动站先前试图访问网络时所用公共安全参数相同的公共安全参数访问网络，则执行唯一性询问程序。

10. 如权利要求 9 所述的系统，其特征在于第一安全参数包含至少一个RAND。

11. 一种对通信网络内用户认证的方法，其特征在于包括以下步骤：

执行公共广播询问程序；

判断对公共广播询问程序响应的用户先前是否对公共广播询问程序成功地响应；以及

如果对公共广播询问程序响应的用户重新使用在先前公共广播询问程序中使用的广播安全参数，则进行唯一性询问程序。

12. 一种对通信网络内用户认证的方法，其特征在于包括以下步骤：

执行公共广播询问程序；

判断对公共广播询问程序响应的用户先前是否对公共广播询问程序成功地响应；以及

如果对公共广播询问程序响应的用户重新使用在先前公共广播询问程序中使用的认证签名，则进行唯一性询问程序。

13. 一种对通信网络内用户认证的方法，其特征在于包括以下步骤：

执行公共广播询问程序；

从响应公共询问程序的用户接收广播安全参数和认证签名；

判断用户发送的公共安全参数是否与先前从用户发送的参数匹配，其中从先前的公共询问程序接收先前发送的参数；

如果公共安全参数与先前发送的参数不同，则利用用户发送的广播安全参数产生认证签名，作为签名生成算法的输入，并且核查生成的认证签名是否与从用户接收的认证签名匹配；

如果广播安全参数与先前用户发送的广播安全参数匹配，则进行唯一性询问程序。

在无线通信中防止应答攻击的系统和方法

发明领域

本发明通常涉及诸如移动电话系统之类的无线通信系统。具体而言本发明涉及移动电话系统中的认证程序。

背景技术

当电话公司最初将蜂窝通信引入一个地区时，其主要的着眼点是建立一定容量、覆盖率的系统并增加新的客户。随着网络的增长，电话公司期望从用户使用其设备中获取利润。但是，蜂窝电话诈骗和烧机可能对通信系统运营的利润产生明显的冲击。烧机就是复制合法用户的蜂窝电话单元以窃取其身份并获取未授权的电话服务。这种行为也带来了问题并给系统用户带来较大的不便。按照蜂窝电信工业协会(CTLA)的统计，全球每年因为烧机而造成的收益损失超过 10 亿美元。

目前采用认证程序来抵御对移动电话服务的诈骗性访问。这里所用的认证指的是交换并处理存储的信息以确认用户单元的身份。认证程序由网络完成以验证标准兼容的电话单元(例如 IS-54B、IS-136、IS-91 或 IS-95 标准电话)的身份。一般情况下，认证程序独立于所用的空中接口协议(例如 CDMA 或 TDMA)。

图 1 为典型移动通信系统的示意图，该系统具有一个或多个移动站。移动电话系统(MTS)100 一般包括基础结构单元 112，它利用射频(RF)信道与多个移动站(MS)120 通信。基础结构单元包括基站(BS)110、移动交换中心(MSC)130、主位置寄存器(HLR)150、认证中心(AC)160、以及访问者位置寄存器(VLR)155。BS110 在 MS120 与 MSC130 之间提供空中接口。MSC130 协调处理所有的通信信道和进程，并为 BS110 提供对网络(例如公用电话交换网(PSTN)140)的访问。HLR150 包含用户数据库 152。用户数据库维护着每个用户的移动身份号(MIN)和电子序列号(ESN)。MIN 和 ESN 一起唯一地识别每个 MS 的身份。

MSC130 一般还包含访问者位置寄存器(VLR)155。但是 VLR155 可以是系统以外的单元。VLR155 包含与 HLR150 中永久用户数据库类似的局部临时用户数据库 157。利用 HLR150 和 VLR155 的信息来授权系统访问并授权向特定的帐户付帐。MSC130 还通过 HLR150 与 AC160 接口。

VLR155 和 MS120 包含了至少三段构成认证用数据的信息：移动单元的 MIN、移动单元的 ESN 和与移动单元相关的共享秘密数据(SSD-A)。SSD-A 一般由认

证密钥(A-密钥)导出。每个 MIN 和相关的 ESN 代表唯一的组合，可以用来识别特定的合法用户。A-密钥是一个对每个定购唯一的秘密数值。例如 A-密钥可以是存储在 MS120 存储器内的 64 位加密可变密钥。A-密钥例如可以在移动站首次为特定用户服务时从 MS120 的小键盘键入。除非 A-密钥已经损坏，否则一般保持不变。MIN 和 ESN 可通过空中发送，但是 A-密钥不能通过空中发送。

在北美系统中，MS 的认证利用称为“CAVE”(蜂窝认证和语音加密)算法的处理。CAVE 算法是一种软件兼容的非线性混合函数，它具有 1 个 32 位线性反馈移位寄存器(LFSR)、16 个 8 位混合寄存器和 256 个输入的查询表。有关 CAVE 算法的详细情况参见公共加密算法蜂窝标准。认证需要系统的 MS120 和基础结构单元 112 借助一公共数据组执行 CAVE 算法以产生认证签名。如果 MS120 产生的认证签名与基础结构单元产生的认证签名一致，则 MS120 的身份被确认并且允许访问电话服务。否则，拒绝 MS120 对网络访问的企图。

可以通过唯一性询问或广播询问完成认证。在唯一性询问中，“RAND”被发送至请求访问系统的 MS120。RAND 一般是用于认证过程的随机产生的数值。唯一性询问的 RAND 一般为 24 位的数字值。MS120 接收 RAND 并利用接收的 RAND、SSD-A 和其他数据执行 CAVE 算法以计算认证签名。认证签名一般为 18 位数字值。MS120 向基础结构单元 112 发送 RAND 和计算的认证签名。基础单元 112 同样采用 CAVE 算法，根据存储的 SSD-A、MIN 和 ESN 值计算认证签名。如果从 MS120 接收的认证签名与基础结构单元 112 独立计算的认证签名一致，则允许 MS120 访问服务。否则拒绝 MS120 访问服务。

相反，在广播询问中，基础结构单元在专用广播信道(例如蜂窝寻呼信道)上向所有的 MS120 广播 RAND 而不是仅仅向请求访问的 MS120 发送 RAND。广播询问有时称为“全球询问”。一般情况下，新的 RAND 将经常产生和发送。当 MS120 请求访问服务时，MS120 根据与基础结构单元 112 通信之前最近广播的 RAND 计算身份签名。在一个实例中，MS120 向基础结构单元 112 发送 8 个最高有效位的 RAND 和计算的认证签名供验证。由于基础结构单元 112 将认证签名与服务请求一起发送，所以可以在 MS120 请求访问服务时立即开始验证认证签名，从而最大程度减少呼叫处理的延迟。

虽然广播询问可以比唯一性询问更快地建立呼叫，但是烧机或其他诈骗入侵者可以利用一种称为“重现攻击”的方法对系统作未授权访问。重现攻击使入侵者以合法用户的身份出现。因此入侵者可以将呼叫记在合法用户帐户上。根据重现攻击，入侵者监视授权 MS120 与基础结构单元 112 之间发送的信息。入侵者存储授权的 MS120 向基础结构单元 112 发送的 RAND 和授权签名。当呼叫结束时，入侵者发送包含了与合法用户先前发送的相同的 RAND 和授权签名

的服务请求。如果自从授权的 MS120 计算被截获的认证签名以来 RAND 未变化，则拥有授权 MS120 的用户将为入侵者使用服务付帐。

以前防止重现攻击的尝试例如是利用拨号数字作为 CAVE 算法的输入，但这未获得成功。对于移动主叫呼叫，采用拨号数字子集作为 CAVE 算法的输入来代替 MIN。由于拨号数字一般随每次呼叫而变化，所以利用拨号数字作为 CAVE 算法的输入使得每次呼叫具有唯一的认证签名，除非两次呼叫的号码相同。但是由于预定数量的最末几位数字极有可能对每次呼叫都是唯一的，所以授权过程一般采用这些预定数量的最末几位拨号数字。在许多情况下，授权呼叫的拨号数字可以附属在未授权呼叫的拨号数字后面而不会对呼叫产生不利影响。因此基础结构将生成与授权 MS120 呼叫一样的认证签名。而且如果未授权的 MS 截获操作员辅助呼叫或者通过目录辅助操作员的呼叫并利用截获的信息(例如 RAND 和认证签名)访问系统，则达到以诈骗手段访问系统的目的。由于目前许多无线服务提供商提供了将用户直接与要求号码相连的目录辅助服务，所以许多用户将只拨号“411”即访问系统。因此通过等候授权用户的操作员辅助呼叫，诈骗性用户可以对系统作未授权访问。

因此在无线通信技术领域需要一种认证过程，它能更好地防止对系统的未授权访问。

发明内容

本发明揭示了一种确认通信网络(例如移动电话系统)内站点身份的方法和装置。所揭示的方法和装置不易受到重现攻击。而且所揭示的方法和装置以较短的延迟实现认证过程。所揭示的方法和装置包括由所附权利要求定义的本发明。

所揭示的方法和装置包含第一站点(例如移动站)，它向通信网内第二站点(例如基础结构单元)传送第一“安全参数”(例如 RAND)和认证签名。为了揭示方便，安全参数被定义为任何信号、图案或数值，它们可以用作诸如普通 CAVE(蜂窝认证和语音加密)算法之类的签名生成(“SG”)算法的输入以生成认证签名。认证签名被定义为任何信号、图案或数值，它们是 SG 算法响应输入的一个或多个安全参数作出的输出。比较好的是每个输入安全参数组生成一个认证签名，该签名与作为其他任何输入安全参数组结果输出的认证签名不同。

第二站点从第一站点接收第一安全参数和认证签名。如果第一安全参数与先前从第一站点接收的预定数量第一安全参数的每个不同，则第二站点完成普通的第一站点认证程序(即确认第一站点的身份)。一旦第二站点认证了第一站点，则允许第一站点访问通信网络。如果第一安全参数与第一站点最近一次为

试图访问服务而发送的其中一个第一安全参数一致，则第二站点完成“唯一性询问”。

在所揭示方法和装置的另一实施例中，判断第一站点是否先前访问过通信网络。如果第一站点先前访问过通信网络，则在允许第一站点访问之前由第二站点启动唯一性询问程序。

附图的简要说明

通过以下结合附图对本发明的描述可以进一步理解本发明的特征和优点，其中：

图 1 为具有一个或多个移动站的典型移动通信系统的示意图；

图 2 为移动交换中心与移动站之间询问/响应对话的示意图；

图 3 为 MSC 单元的示意图；以及

图 4 为实现认证过程步骤的流程图。

实施发明的较佳方案

所揭示的方法用于确认移动电话系统(MTS)中移动站的身份。所揭示的方法和装置确保每个移动站(MS)在预先确定的时间内对一个特定安全值组(例如“RAND”或由特定信息组(包括 RAND)生成的认证签名)只可以使用一次。通过确保每个 MS 在预先确定时间内对特定安全值只可使用一次消除了“重现攻击”的危险。所揭示的方法和装置包括被要求权利的本发明。但是本发明的范围应该唯一由所附权利要求确定。

图 2 示出了 MTS300 基础结构单元 312 与授权 MS320(例如在运营 MTS300 的服务提供商处拥有合法帐户的 MS)之间询问/响应的对话。MS321 为入侵者(例如未授权用户)。在所揭示方法和装置的一个实施例中，基础结构单元 312 包括基站(BS)310、移动交换中心(MSC)330、主位置寄存器(HLR)350、认证中心(AC)360 和访问者位置寄存器(VLR)355。MTS300 比较好的是能够进行唯一性询问和广播询问。基础结构单元 312(借助 BS310)经空中链路 340 向所有的 MS320 发送广播安全值(例如“广播 RAND”)。如下所述，广播安全值比较好的是用于“广播认证”过程的随机产生数值。广播安全值时常变化，并且向所有 MS320 广播新的广播安全值。由以下描述可见，在较为频繁地改变广播安全值以减少所需唯一性询问次数与较少改变广播安全值以减少生成和广播新广播安全值所需开销之间有所折衷。如果广播安全值为 RAND，则所揭示的方法和装置比较好的是能符合工业标准(这些标准规定了 RAND 的改变频度)工作。

当特定 MS320 尝试通过基础结构单元 312 第一次访问电话服务时，MS320

必须首先接收广播安全值。广播安全值作为签名生成(“SG”)算法(例如 CAVE(蜂窝认证和语音加密)算法)的其中一个输入提供以生成认证签名。SG 算法的其他输入比较好的是包括移动身份号码(“MIN”)、电子序列号(“ESN”)和与 MS320 相关的共享秘密数据(“SSD-A”)。每个特定的 ESN 和 MIN 数值对标识一个特定的 MS。SSD-A 值利用加密算法的“密钥”值生成。密钥值和 SSD-A 值不经空中发送。

一旦 MS320 生成认证签名，它就经空中向基础结构单元 312 发送一组安全值。根据所揭示方法和装置的一个实施例，一组安全值包括：(1)认证签名；(2)作为 SG 输入的整个广播安全值、一部分广播安全值或者代表广播安全值的一些数值；(3)ESN；以及(4)用于生成认证签名的 MIN。由于 SSD-A 值和特定的 SG 算法对于可能截获信息的任何人来说是未知的，因此入侵者不可能以后在安全值改变时利用该信息独立生成认证签名。

基础结构单元 312 至少记录发送的一组安全值内的一些数值。例如在一个实施例中，基础结构单元 312 记录下 MS320 使用了哪个广播安全值以生成认证签名。被基础结构单元 312 记录的安全值也可以是认证签名本身。在所揭示方法和装置的一个实施例中，基础结构单元 312 存储一部分安全信息，例如广播安全值或者认证签名。在所揭示方法和装置的某一实施例中，基础结构单元 312 配备了足够的存储器容量以存储每个 MS320 的若干安全值(或者代表安全值的数值)。基础结构单元 312 可以为每个 MS320 存储的一个安全值(或者代表安全值的数值)分配存储器。

下一次 MS320 试图访问电话服务时，MS320 利用当前的广播安全值和 MIN、ESN 以及 SSD-A 计算认证签名。如果广播安全值从上次试图访问系统起发生变化，则 MS320 将发送 ESN 和 MIN 连同新的广播安全值(或代表值)和认证签名。在这种情况下，该过程与 MS320 第一次试图访问系统时的情况一样。

但是如果广播安全值从上次试图访问系统起未发生变化，则认证签名的计算值将与先前试图访问系统时的数值相同。即给定的 SG 输入相同，则第二次访问企图的 SG 输出也相同。

MS320 经空中链路 340a 向基础结构单元 312 发送广播安全值(或代表值)、计算的认证签名以及 ESN 和 MIN。基础结构单元 312 将接收的一个或多个安全值组与其先前从 MS320 接收的存储安全值(或代表值)比较。例如，在所揭示方法和装置的一个实施例中，基础结构单元 312 将接收的广播安全值与其先前从 MS320 接收的存储值比较。基础结构单元 312 可以核查 MS320 发送的整组信息。在另一实施例中，只要每次 MS320 在访问尝试中使用不同的广播安全值时待核查信息已经发生变化，则要核查了除安全值或代表值(例如认证签名)以外的一

部分信息。由于在这种情况下基础结构单元 312 已经从 MS320 接收了相同的安全信息(例如具有相同值的 RAND 或认证签名)，所以在允许 MS320 访问系统之前基础结构单元 312 需要对 MS320 的身份作额外的确认。根据所揭示方法和装置的实施例，通过由基础结构单元 312 启动唯一性询问认证程序完成额外确认。基础结构单元 312 也可以强行改变广播安全值并要求 MS320 利用新的安全值响应广播询问。在另一实施例中，可以采用另一种方法迫使 MS320 验证其身份。

如果额外确认程序表明 MS320 被授权(例如顺利通过唯一性询问)，则 MS320 被视为合法用户而不是入侵者(例如 MS321)。因此基础结构单元 312 允许 MS320 访问电话服务。

但是如果未授权的 MS321 通过监视授权 MS320 的发射情况而截获认证数据(例如 RAND、认证签名以及 ESN 和 MIN)，则未授权的 MS321 无法通过额外的确认程序。例如如果基础结构单元 312 要求 MS321 响应唯一性询问，则由于 MS321 必须由基础结构单元 312 提供的唯一性询问安全值独立生成新的认证签名，所以无法正确响应。另外，如果基础结构单元 312 改变了广播安全值并随后要求 MS321 利用新的广播安全值响应广播询问，则 MS321 无法成功做到。这是因为广播询问现在要求根据新的广播安全值独立生成新的认证签名。

显而易见的是，基础结构单元 312 内每个特定单元的功能随所揭示方法和装置的实施例不同而不同。但是除了确定 MS320 是否先前尝试访问系统以及要求 MS320 进一步确认身份的功能之外，每个这样的单元基本上都是普通的单元。

在所揭示方法和装置的一个实施例中，基础结构单元 312 包括基站 310、MSC330、HLR350、AC360 和 VLR335，MSC330 生成广播安全值。该广播安全值被送至 BS310。BS310 向 MS320 发送广播安全值。当 MS320 尝试从网络 300 访问通信服务时，它向 BS310 回送下列信息。MS320 发送广播安全值(或根据安全值生成的值)的一部分、MIN、ESN 副本和 MS320 利用这些参数生成的认证签名。每个参数都送至 HLR350。HLR350 确定 MS320 是否被登记在系统 300 内。如果 HLR350 确定 MS320 已被登记，则传送至 HLR350 的参数被送至 AC360。AC360 核查 MS320(由 MIN 和 ESN 确认身份)先前是否尝试利用同一广播安全值访问系统。如果不是，则 AC360 利用 MIN、ESN、SSD-A 和广播安全值独立生成认证签名。随后 AC360 进行核查以确保生成的认证签名与从 MS320 接收到认证签名一致。

如果 AC360 生成的认证签名与从 MS320 接收的不一致，或者如果 AC360 判断 MS320 已经尝试利用同一广播安全值从网络访问服务，则 AC 将生成唯一性

询问安全值。AC360 将利用唯一性安全值生成新的认证签名(“唯一的认证签名”)。唯一性询问安全值和唯一性认证签名被送至 MSC330。MSC330 只将唯一性询问安全值送至 BS310。BS310 向 MS320 发送唯一性询问安全值。MS320 随后以唯一性认证签名作出响应，该签名由 MS320 利用 MIN、ESN、唯一性询问安全值和 SSD-A 独立计算得到。BS310 从 MS320 接收唯一性认证签名。BS310 随后将签名送至 MS330。MSC330 将接收自 MS320 的唯一性认证签名与 AC360 提供给 MSC330 的唯一性认证签名比较。如果相互匹配，则 MS320 被视为合法用户。

如果 MSC330 判断 MS320 是访问者，则 VLR355 被用来完成 HLR350 完成的功能。

但是显而易见的是，上述由诸如 AC360 单元完成的功能也可以由诸如 HLR350、VLR355 或 MSC330 之类的其他单元完成。

图 3 为 MSC330 单元的示意图。如图 3 所示，MSC 比较好的是包括处理器 301、接收机 303 和存储器 305。接收机是可以接收来自外部信号源信号的任何接收装置。按照所揭示方法和装置的一个实施例，接收机是经地面线路与基站耦合的设备中常用的普通接收机。处理器 301 与接收机 303 耦合。这里所示处理器为单处理器。但是对于本领域内技术人员显而易见的是，处理器仅仅代表处理功能，这些功能既可以由微处理器之类的单处理器单元实现，也可以由分布在基础结构单元 312 内的若干处理单元实现。毫无疑问，所需的处理属于普通微处理器和/或数字信号处理器能够实现的为所揭示方法和装置全部必要的功能。

图 4 为流程图，它示出了在所揭示方法和装置的一个实施例中认证过程中执行的步骤。图 2 所示系统可以用来实现图 4 的步骤。如图 4 所示，过程开始于步骤 400。在步骤 410，当特定 MS320 试图访问电话服务时，MS320 发送一组安全值(包括识别数据(例如 MIN/ESN))、先前接收的安全值和相关的认证签名。如果需要 MS120 也可发送其他数据。一般情况下，MS320 在 MSC320 前一次广播期间或者在与基础结构单元 312 前一次唯一性询问程序期间从基础结构单元 312 获取先前接收的广播安全值。在步骤 430，基础结构单元 312 确定 MS320 是否已经利用同一组安全值从基础结构单元 312 获取服务。在另一实施例中，基础结构单元 312 核查该组安全值的某些部分先前是否被 MS320 在访问服务时使用。

如果基础结构单元 312 确定 MS320 先前未利用同一组安全值访问服务，则在步骤 440，基础结构单元 312 存储从 MS320 接收的安全值。在步骤 450，基础结构单元 312 验证从 MS320 接收的授权签名值。即，核查授权签名的值(例

如基础结构单元 312 利用与 MS320 所用一致的 SG 输入独立计算得到的值)是否与预期的一致。在验证授权签名之后，过程转入步骤 470。

另一方面，如果基础结构单元 312 在步骤 430 确定 MS320 先前已经利用同一组安全值访问服务，则过程转入步骤 460。在步骤 460，基础结构单元 312 例如通过要求 MS320 对唯一性询问程序作出响应额外验证 MS320 的身份。如上所述，唯一性询问程序牵涉到至少是唯一性安全值在基础结构单元 312 与 MS320 之间的交换和唯一性询问签名在 MS320 与基础结构单元 312 之间的交换。

在步骤 470，基础结构单元 312 判断 MS320 是否通过步骤 450 或 460 完成的认证程序。为此执行与 MS320 计算预期认证签名一样的 SG 算法(例如 CAVE 算法)。基础结构单元 312 将预期的认证签名与 MS320 计算的认证签名比较。如果两个签名匹配，则过程转入步骤 480 并且允许 MS320 访问电话服务。如果两个签名不一致，则过程转入步骤 490 并且拒绝 MS320 访问服务。在步骤 499 结束过程。

由上可见，本发明解决了长期所需的具有抵御入侵者认证程序的无线系统和方法。利用本发明的认证过程，将入侵的可能性降低至最小程度。为了突破本发明的认证处理，入侵者不仅需要获取认证数据，而且需要获取不经空中发送的 SSD-A。在不偏离本发明精神和实质的前提下，本发明可以有多种实现方式。上述实施例仅具有示意性质而无限定作用。本发明的精神和范围由后面所附权利要求限定。

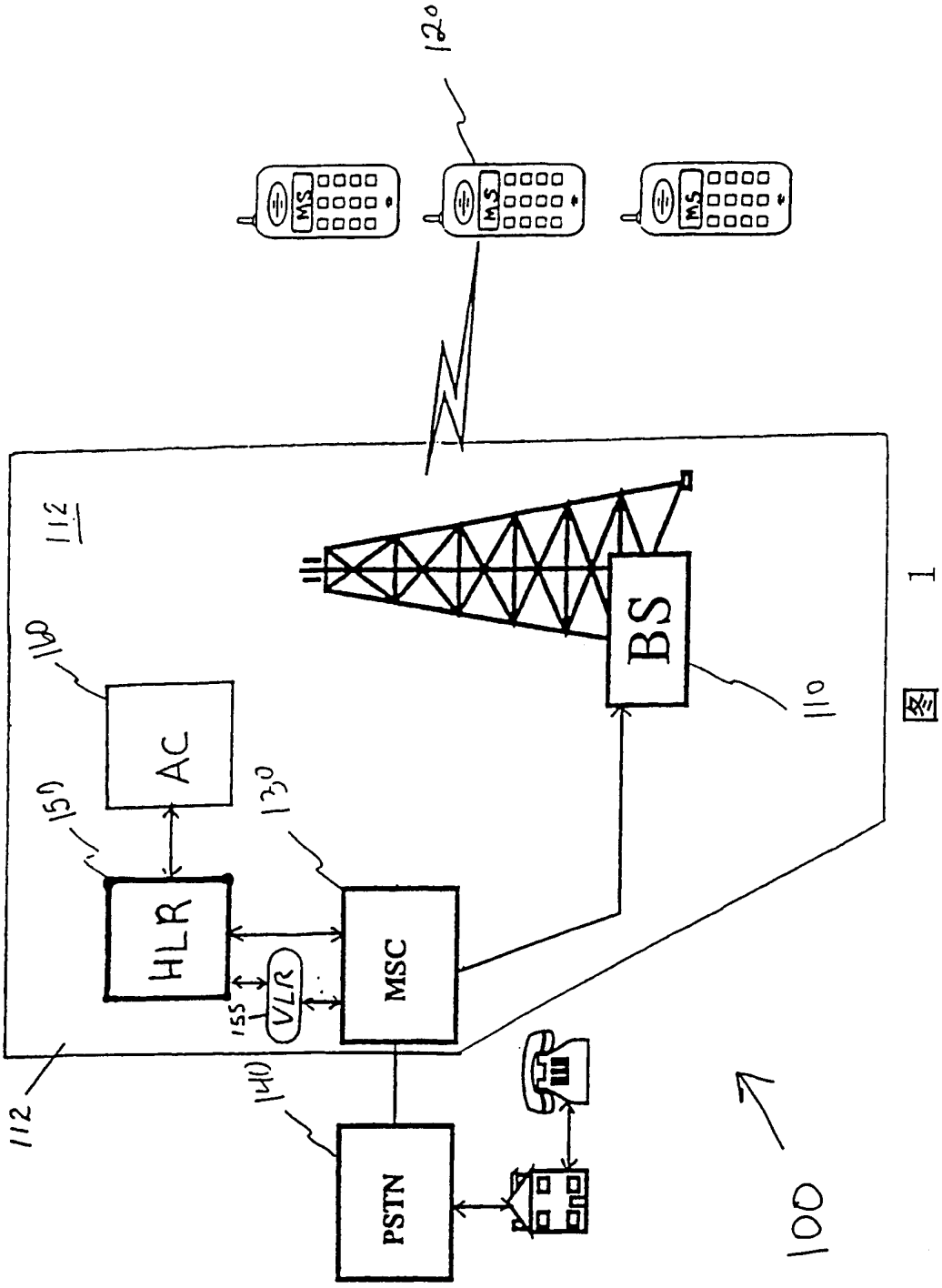

120
MS
MS
MS
112
BS
110
AC
150
130
HLR
MSC
155
VLR
140
PSTN
112
100

图 1

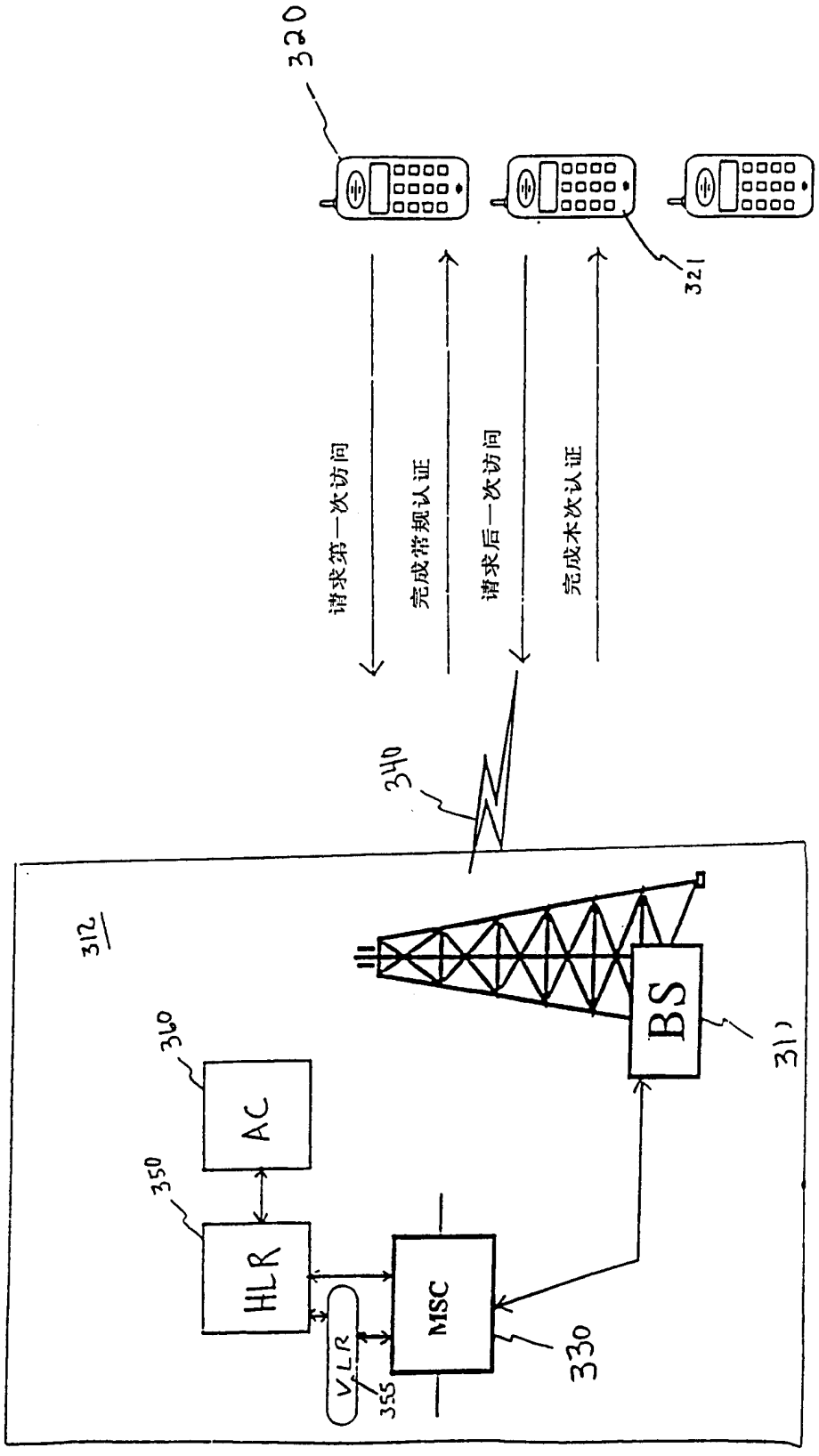

320
321
请求第一次访问
完成常规认证
请求后一次访问
完成本次认证
340
312
360
AC
350
HLR
VLR
355
MSC
330
BS
310
300

图 2

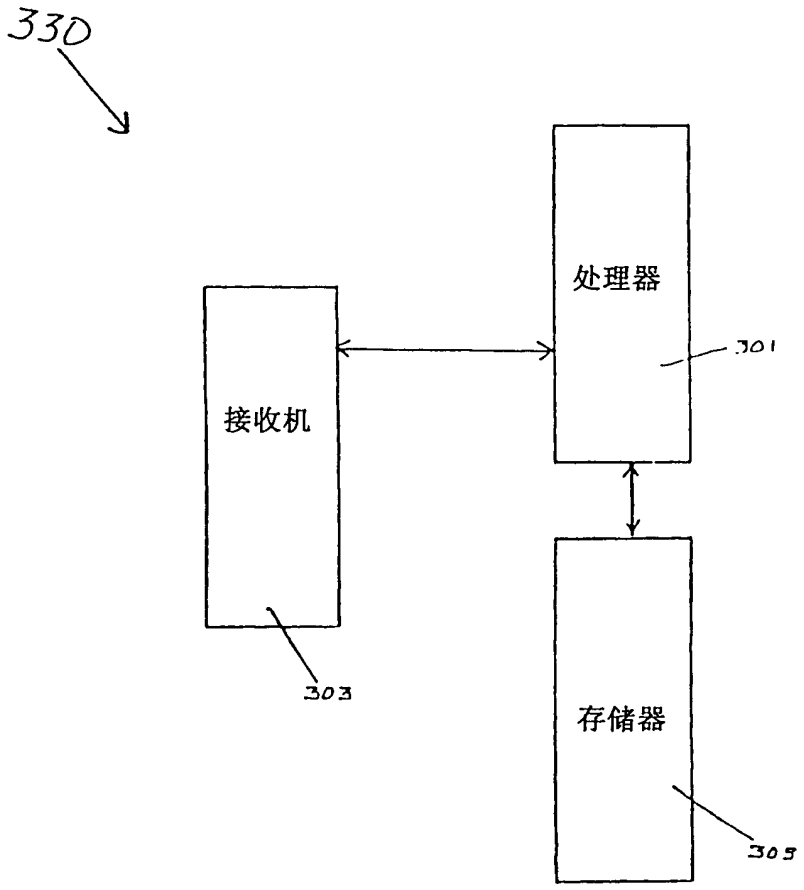


图 3

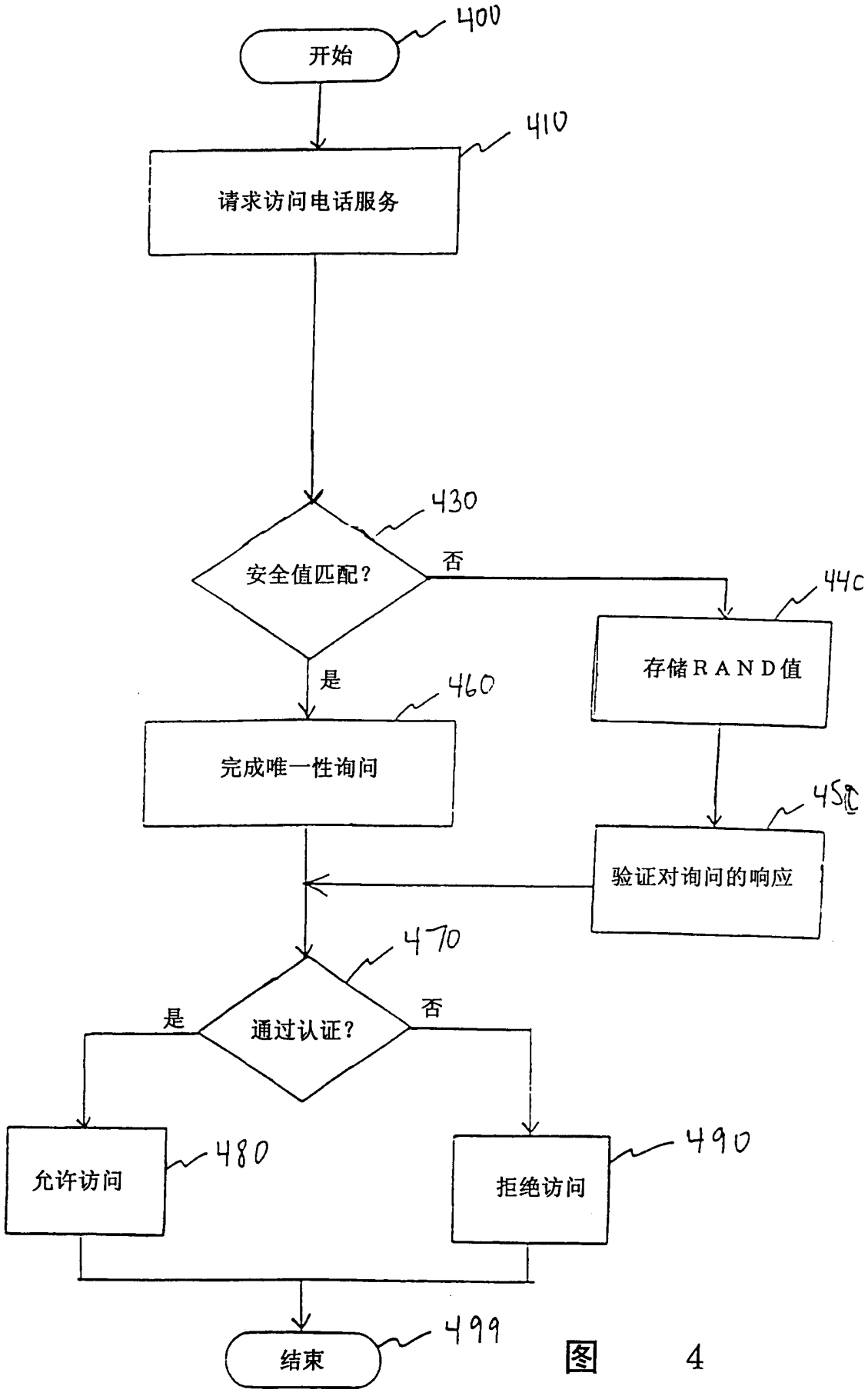

400
开始
410
请求访问电话服务
430
安全值匹配?
否
是
44C
存储RAND值
460
完成唯一性询问
45C
验证对询问的响应
470
通过认证?
是
否
480
允许访问
490
拒绝访问
499
结束

图 4