



(12) 发明专利

(10) 授权公告号 CN 1985494 B

(45) 授权公告日 2011.10.12

(21) 申请号 200580023589.6

(22) 申请日 2005.07.12

(30) 优先权数据

04016665.4 2004.07.15 EP

60/591,192 2004.07.26 US

(85) PCT申请进入国家阶段日

2007.01.12

(86) PCT申请的申请数据

PCT/EP2005/007545 2005.07.12

(87) PCT申请的公布数据

W02006/005576 EN 2006.01.19

(73) 专利权人 艾利森电话股份有限公司

地址 瑞典斯德哥尔摩

(72) 发明人 S·鲁尼森

(74) 专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 曾祥交 刘杰

(51) Int. Cl.

H04L 29/06(2006.01)

(56) 对比文件

US 20030165121 A1, 2003.09.04, 全文.

US 20030012149 A1, 2003.01.16, 第【0159】
段,【0166】段.

EP 1424826 A2, 2003.09.09, 全文.

审查员 孙迪

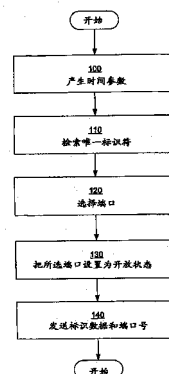
权利要求书 2 页 说明书 5 页 附图 3 页

(54) 发明名称

拒绝服务保护的方法和设备

(57) 摘要

通信设备(1)以及用于操作所述通信设备的方法。该方法包括:通过端口选择函数来选择多个端口之一以使它对于接收特定类型的电子消息是可访问的;以及把所述所选端口设置为开放状态。



1. 一种用于操作通信设备 (1) 的方法, 所述方法在应用层协议与传输协议一起运行时被执行, 所述方法包括:

通过端口选择函数来选择多个端口之一, 以使它对于接收特定类型的电子消息是可访问的; 以及

把所述所选端口设置为开放状态,

其特征在于,

所述选择函数是所述通信设备 (1) 的唯一标识符的函数, 所述方法包括在选择所述端口之前检索所述通信设备的所述唯一标识符。

2. 如权利要求 1 所述的方法, 其特征在于, 还包括向网络服务器 (4) 发送用于标识通信设备 (1) 的数据以及设置为开放状态的所述所选端口的端口号。

3. 如权利要求 1 或 2 所述的方法, 其特征在于, 应用层协议为 SIP, 并且所述消息为 SIP 消息, 以及所述传输协议为 UDP 或 TCP。

4. 如权利要求 2 所述的方法, 其特征在于, 用于标识通信设备 (1) 的数据包括通信设备的电子地址和网络地址。

5. 如权利要求 1、2、4 中的任一项所述的方法, 其特征在于, 所述选择函数还是时间参数的函数, 所述方法包括在选择所述端口之前产生所述时间参数。

6. 如权利要求 1、2、4 中的任一项所述的方法, 其特征在于, 所述选择函数还是用于随机选择多个端口之一的随机函数。

7. 一种通信设备 (1), 包括用于当应用层协议与传输协议在所述通信设备中一起运行时接收电子消息 (21) 的部件, 所述通信设备包括:

端口选择部件 (25), 适合于通过端口选择函数来选择多个端口之一, 以使它对于接收特定类型的电子消息是可访问的; 以及

控制器 (23), 适合于把所述所选端口设置为开放状态,

其特征在于,

所述选择函数是所述通信设备 (1) 的唯一标识符的函数, 所述端口选择部件 (25) 适合于在选择所述端口之前从存储器 (24) 中检索所述通信设备的所述唯一标识符。

8. 如权利要求 7 所述的通信设备, 其特征在于, 还包括适合于向网络服务器 (4) 发送用于标识所述通信设备 (1) 的数据以及设置为开放状态的所述所选端口的端口号的发射机 (22)。

9. 如权利要求 7 或 8 所述的通信设备, 其特征在于, 所述应用层协议为 SIP, 并且所述消息为 SIP 消息, 以及所述传输协议为 UDP 或 TCP。

10. 如权利要求 8 所述的通信设备, 其特征在于, 用于标识通信设备 (1) 的数据包括通信设备的电子地址和网络地址。

11. 如权利要求 7、8、10 中的任一项所述的通信设备, 其特征在于, 所述选择函数还是时间参数的函数, 所述端口选择部件 (25) 适合于在选择所述端口之前产生所述时间参数。

12. 如权利要求 7、8、10 中的任一项所述的通信设备, 其特征在于, 所述选择函数还是用于随机选择多个端口之一的随机函数。

13. 如权利要求 7、8、10 中的任一项所述的通信设备, 其特征在于, 所述通信设备是移动无线电终端、寻呼机、通信器、电子组织器、智能电话、个人数字助理或计算机。

14. 如权利要求 7、8、10 中的任一项所述的通信设备,其特征在于,所述通信设备为移动电话 (1)。

拒绝服务保护 的方法和设备

技术领域

[0001] 本发明涉及操作通信设备的方法,更具体来说,涉及当通信设备连接到通信网络时把应当在其中接收特定类型的消息的端口设置为开放状态的方法。本发明还涉及实现该方法的通信设备。

背景技术

[0002] 通信设备、如移动电话可配置为连接到各种通信网络,例如移动通信网络、局域网、广域网和/或全球网、如因特网。广域网或全球网可能例如是分组交换 IP 网络,在其中,通过把诸如 URI(通用资源标识符)或 URL(通用资源定位符)之类的电子地址和/或诸如 IP 地址之类的网络地址附加到所传送数据分组,在终端之间传送数据分组。

[0003] 当通信设备连接到网络时,它可能被分配在代理服务器上与电子地址共同登记的 IP 地址。开放以接收特定类型的消息的端口的端口号也可与网络地址和电子地址一起存储在代理中。

[0004] 发送终端可能仅具有接收终端的 URI 或 URL,在其中,消息通过网络服务器传送,它将根据消息类型把消息导向正确的网络地址和正确的端口。

[0005] IP 多媒体子系统(IMS)由 3GPP(第三代合作项目)进行标准化,并且是用于创建多媒体服务的系统。会话发起协议(SIP)是由 IETF(因特网工程特别任务组)标准化的应用层协议,它用来控制 IMS 中的多媒体会话。SIP 采用 UDP(用户数据报协议)或 TCP(传输控制协议)作为传输协议在 IP(因特网协议)之上运行。

[0006] 在 SIP 标准(RFC3261)中,存在为 SIP 消息定义的标准化缺省端口号。

[0007] 只要接收终端、如 IMS 终端开启或处于它连接到网络的特定模式,则它可具有活动 PDP(分组数据协议)上下文和有效网络地址。如果存在用于特定类型的消息、如 SIP 消息的标准化缺省端口,则它对于拒绝服务攻击开放。连接到与终端相同的网络的攻击者可能利用用于特定消息的缺省端口直接向终端发送特定类型的消息。为了确信特定终端接收拒绝服务消息,攻击者最多必须向某个代理服务器提供服务的所有 IP 地址的所述缺省端口发送一个消息。因此,即使目的只是要攻击一个终端,但是接收该消息的所有终端都将受到攻击。

[0008] 拒绝服务攻击的第一实例是发送畸形消息。如果大家知道某种类型的终端在接收某种畸形消息时会崩溃,则通过利用缺省端口向运营商域中的所有 IP 地址发送该畸形消息,运营商或代理服务器域中的那种类型的所有终端可能崩溃。

[0009] 拒绝服务攻击的第二实例是发送良构消息。由于每个消息在接收之后的某个时间段、例如高达数分钟占用终端中的存储资源,因此良构消息的重复传送可能占用可影响终端中其它服务或应用的这种数量的存储资源。

发明内容

[0010] 本发明的一个目的是提供使端口可访问的方法及设备,当所述端口设置为开放状

态时,可在该端口接收特定类型的电子消息。

[0011] 根据本发明的第一方面,此目的通过一种用于操作通信设备的方法来实现。该方法当应用层协议与传输协议一起运行时被执行,并且包括通过端口选择函数来选择多个端口之一以使它对于接收特定类型的电子消息可访问;以及把所述所选端口设置为开放状态。一旦所选端口设置为开放状态,则可接收消息。

[0012] 该方法还可包括向网络服务器发送用于标识通信设备的数据以及设置为开放状态的所述所选端口的端口号。

[0013] 选择函数可以是一个或若干参数的函数。一种参数可以是通信设备的唯一标识符,其中,所述方法包括在选择端口之前检索通信设备的唯一标识符。作为替代或补充,选择函数是时间参数的函数,其中,所述方法包括在选择端口之前产生时间参数。选择函数还可以是用于随机选择多个端口之一的随机函数。

[0014] 根据本发明的第二方面,此目的还通过适合实现根据本发明的方法的通信设备来实现。该通信设备包括:用于当应用层协议在所述通信设备中与传输协议一起运行时接收电子消息的部件;适合于通过端口选择函数来选择多个端口之一以使它对于接收特定类型的电子消息可访问的端口选择部件;以及适合于把所述所选端口设置为开放状态的控制

器。

[0015] 根据本发明的第三方面,此目的还通过一种计算机程序产品来实现。计算机程序产品包括当计算机程序代码部件由具有计算机功能的电子装置运行时执行根据本发明的方法的计算机程序代码部件。计算机程序代码部件可包含在计算机可读介质中。

[0016] 在从属权利要求中定义了本发明的其它实施例。

[0017] 本发明的一个优点在于,端口根据选择函数而不是缺省端口被选择以及开放以便接收特定类型的消息。因此,安全性得到提高,因为外部实体不知道哪个端口开放以接收特定类型的消息。另一个优点在于,如果选择函数包括一个或若干选择参数,则安全性可进一步提高,这确保在相继端口选择过程中,在一个通信设备中不选择同一个端口。

[0018] 应当强调,在本说明中,术语“包括/包含”用来表示存在所述特征、整数、步骤或组件,但并不排除存在或附加一个或多个其它特征、整数、步骤、组件或上述各项的组合。

附图说明

[0019] 通过以下参照附图对本发明的详细说明,会明白本发明的其它目的、特征和优点,其中:

[0020] 图 1 是连接到通信网络的根据本发明的通信设备的示意图;

[0021] 图 2 是根据本发明的通信设备的某些组件的框图;以及

[0022] 图 3 是根据本发明的方法的一个实施例的流程图。

具体实施方式

[0023] 图 1 说明根据本发明的通信设备 1,它可连接到通信网络 2、如分组交换 IP 网络。共同由终端 B 3 表示的一个或若干附加终端可连接到通信网络 2。适合于存储用于标识通信设备 1 以及可能还有终端 B 3 的数据的网络服务器 4 也连接到通信网络 2。电子消息可通过通信网络 2 在通信设备 1 与终端 B3 之间发送。消息由网络服务器 4 转发。攻击者 5

也可连接到通信网络 2。如上所述,攻击者可试图向通信设备 1 或终端 B3 传送电子消息。

[0024] 通信设备 1 和终端 B3 例如可能是移动电话、移动无线电终端、寻呼机、通信器、电子组织器、智能电话、个人数字助理或者具有通信功能的计算机。为了说明的目的,下面仅参照移动电话 1 和终端 B3。

[0025] 移动电话 1 可包括用于例如通过移动通信网络、诸如 GSM(全球移动通信系统)或 UMTS(通用移动通信系统)网络与通信网络 2 进行无线通信的天线 10。或者,移动电话可例如通过调制解调器经由有线连接、如公共交换电话网连接到通信网络 2。

[0026] 移动电话 1 和终端 B3 可以是 IMS(IP 多媒体子系统)终端,它适合于采用例如 UDP(用户数据报协议)或 TCP(传输控制协议)作为传输协议来运行诸如 SIP(会话发起协议)之类的应用层协议以及诸如 IP(因特网协议)之类的网络协议。

[0027] 在 IMS 中,送往及来自 IMS 终端的所有 SIP 消息将通过 SIP 代理服务器、如网络服务器 4。因此,网络服务器 4 适合于存储用于标识登记为连接到通信网络 2 的 IMS 终端、诸如移动电话 1 和终端 B3 的标识数据。网络服务器 4 还适合于存储与某个电子消息、例如 SIP 消息应当被导向到的每个已登记 IMS 终端的标识数据关联的端口号。标识数据可包括按照以下形式的诸如 SIP URI(统一资源标识符)之类的电子地址和诸如 IP 地址之类的网络地址:

[0028]

SIP URI	IP 地址	端口号
sip:UserA@operator.com	5555::aaa.bbb.ccc.ddd	xxxx
sip:UserB@operator.com	5555::eee.fff.ggg.hhh	yyyy

[0029] 实际端口号和网络地址只有移动电话 1 和网络服务器 4 才知道。端口号标识可访问端口,在该端口,在移动电话 1 内将接收特定类型的电子消息、如 SIP 消息。

[0030] 网络服务器 4 可以是 S-CSCF(在服务呼叫会话控制功能)服务器或者适合于向特定端口转发特定类型的电子消息的任何服务器。

[0031] 终端 B3 可通过用移动电话 1 的电子地址为消息定址,向移动电话 1 发送特定类型的消息。消息通过通信网络 2 传送到网络服务器 4。网络服务器 4 适合于检索与消息的电子地址关联的网络地址和端口号,并把消息转发给具有关联网络地址的移动电话的所述端口。

[0032] 图 2 说明移动电话 1 的某些组件。通信单元 20 包括诸如发射机之类的发送部件 21 和诸如接收机之类的接收部件 22。通信单元连接到天线 10 以及连接到处理部件或控制器 23、如处理器或中央处理器(CPU)。控制器 23 适合于运行不同的协议,例如以上所述的应用和传输协议。控制器 23 还适合于提供作为用于传递电子消息的进程或程序与通信单元 20 之间的逻辑接口的某种端口。

[0033] 移动电话 1 可包括各种存储器,例如 ROM(只读存储器)、RAM(随机存取存储器)和/或 SIM(用户标识模块),它们共同由存储器 24 表示。存储器 24 连接到控制器 23。

[0034] 选择部件或端口选择器 25 适合于通过端口选择函数来选择多个端口之一,以使用它对于接收特定类型的电子消息、如 SIP 消息是可访问的。各端口具有其自己的端口号。用于特定类型的消息的端口可从多个可能的端口中选取。一旦选择了端口,所选端口的编号被转发给控制器 23,它可把所选端口设置为开放状态。当端口设置为开放状态时,则可在所述端口接收特定类型的消息。端口选择器 25 可能是例如由控制器 23 运行的独立应

用所实现的软件。但是,端口选择器 25 也可作为诸如 CPU 之类的独立硬件单元或者诸如 ASIC(专用集成电路)或 FPGA(现场可编程门阵列)之类的集成电路来提供。

[0035] 端口选择器 25 可适合于选择当移动电话 1 开启时将设置为开放状态的端口。或者,端口选择器 25 适合于当移动电话 1 进入其中可接收特定类型的消息的特定模式、如 IMS 模式时选择所述端口。

[0036] 控制器 23 可适合于在预定时间段把所选端口设置为开放状态,或者只要移动电话开启或保持在特定模式时把所选端口设置为恒定开放状态。只要移动电话开启或在特定模式,移动终端 1 可始终具有活动 PDP(分组数据协议)上下文和有效 IP 地址。因此,当所选端口开放时,移动电话可始终接收特定类型的消息、如 IMS 消息。把端口设置为恒定开放状态的优点在于,移动电话 1 只要被开启就可接收特定类型的消息。

[0037] 选择函数将确定选取多个端口之一。要选择的多个端口可能是 IANA(因特网编号分配机构)众所周知端口范围和 IANA 登记端口范围之外的 16384 个可能的端口。16384 个端口的所述集合中可能没有端口被登记,因而端口选择器可无条件地从端口的这个集合中选择。如果端口号按照 IANA 标准来提供,则它们可能是 49152-65535 的范围中的任何端口号。但是,如果本发明连同另一个标准来实现,则端口可能具有一个或若干范围中提供的其它端口号。

[0038] 选择函数可能是一个或若干选择参数的函数。选择函数确定按照外部未知的方案选择端口。这是一个优点,因为潜在的攻击者将不知道向哪一个端口发送消息。每当所述所选端口是任何外部、如攻击者 5 未知的时,同一个端口可被选择为专用于接收特定类型的消息。各移动电话 1 可选择例如由制造商预设的不同端口。选择函数还可确定每次选择不同的端口。这提高了防止潜在攻击的安全性,因为一旦移动电话 1 已经关机并再次开启,不同的端口将被设置为开放状态。此外,选择函数可确定,不同的移动电话 1 通过按照不同方案或者随机将不同的端口设置为开放状态,将它们设置为开放状态以接收特定类型的消息。其优点在于,与选择同一个端口相比,防止攻击的安全性进一步提高。如上所述,攻击者不知道移动终端 1 的网络地址。因此,要确保攻击一个终端,攻击者必须把消息导向通信网络 2 的所有网络地址的全部可能的端口,与端口已经是已知的情况相比,这是一个巨大的数量。

[0039] 选择函数可能是随机函数,在其中,端口选择器 25 适合于在多个端口号中选择随机编号。

[0040] 或者,选择函数是移动电话 1 的唯一标识符的函数。例如,如果标识符为 123,则多个可能的端口包括 10 个第一小组,以及各第一小组包括 10 个第二小组,端口可按照以下选择函数来选取:第一位(1)确定第一小组,第二位(2)确定已确定第一小组中的第二小组,以及第三位(3)确定已确定第二小组中的端口号。或者,第三位(3)确定已确定第二小组内的第三小组,其中端口号随机选取。

[0041] 或者,选择函数是诸如唯一标识符、可能端口的数量以及变为可访问的第一可能端口、即具有可能端口的最低端口号的端口的编号的组合之类的多个参数的函数。这种选择函数例如可实现为:

[0042] 要变为可访问的端口的端口号 = (“唯一标识符”模“可能端口的数量”)+“第一可能端口号”。

[0043] 唯一标识符例如可能是移动电话 1 的 IMSI (国际移动用户标识符)。IMSI 例如用于 GSM 和 UMTS 电信系统。IMSI 可从它存储于的存储器 24 中检索。或者,单独的唯一标识符被分配给每个移动电话 1。但是,有利的是采用 IMSI,因为不必分配附加标识符。也可采用移动电话 1 的其它任何标识符。选择函数基于唯一标识符是一个优点,因为各移动电话 1 将以不同方式选择要设置为开放状态的端口。

[0044] 又一个备选选择函数是时间参数的函数。时间参数可能是某个时间点或者计时器值。时间点例如可能是移动电话 1 开启时或者进入某种模式、如 IMS 模式时的时间点。计时器值可能是例如在移动电话 1 开启时的时间点直到它进入某种模式、如 IMS 模式之间所计算的时间周期。端口选择器 25 可适合于登记移动电话 1 开启和 / 或进入特定模式时的时间点。端口选择器 25 还可适合开始和停止计时器。如果采用时间参数、例如 hh.mm.ss, 则可能的多个端口被分为 25 个第一小组、各第一小组中的 61 个第二小组以及各第二小组中的 61 个第三小组,端口例如可按照以下选择函数来选取:选择第一小组作为时间参数的小时值(hh);选择所选第一小组中的第二小组作为时间参数的分钟(mm)值;以及选择所选第二小组中的端口号作为时间参数的秒值(ss)。或者,在所选第二小组中,第二值(ss)确定第二小组中的第三小组,其中端口号随机选取。在又一个备选选择函数中,第三小组通过时间参数来确定,以及唯一标识符确定在其中要选择哪一个端口号。如果第三小组包括 100 个端口号(1...99),并且唯一标识符包括五位数、例如 12345,则两位、例如第二与第五位的值的任何组合(25 或 52)可确定要选择的端口号。

[0045] 在选择函数的一个备选实施例中,它是诸如时间点或者计时器值之类的时间参数、日期、变为可访问的可能端口的数量、变为可访问的第一可能端口、即具有可能端口的最低端口号的端口的编号的函数。这种选择函数例如可实现为:要变为可访问的端口的端口号 = (“时间参数”模“可能端口的数量”) + “第一可能端口号”。

[0046] 图 3 说明根据本发明的方法的一个实施例。在第一步骤 100,产生时间参数。如上所述,时间参数可能是某个时间点或者计时器值。在步骤 110,移动电话 1 的唯一标识符从存储器 24、例如从 SIM 卡中检索。在步骤 120,要设置为开放状态以便接收特定类型的消息的端口通过选择函数来选取。如上所述,选择函数可能是诸如时间参数、唯一标识符和 / 或随机数之类的一个或若干参数的函数。如果选择函数只是随机数的函数,则不需要执行步骤 100 和 110。在步骤 130,所选端口被设置为开放状态。如上所述,端口可能设置成恒定开放状态,或者在预定时间周期设置为开放状态。一旦端口设置为开放状态,则随时可接收特定类型的消息。在步骤 140,用于标识移动终端 1 的数据以及所选端口的端口号被传送给网络服务器 4。

[0047] 根据本发明的方法可通过软件来实现。可提供一种包括执行该方法的计算机程序代码部件的计算机程序产品。所述代码部件在由具有计算机功能的电子装置(1)运行时可实现该方法。计算机程序代码部件可包含在计算机可读介质、如存储器 24 中。

[0048] 以上已经参照具体实施例描述了本发明。但是,在本发明的范围之内,不同于以上所述的其它实施例是可行的。在本发明的范围内,可提供通过硬件或软件执行该方法、与以上所述的那些不同的方法步骤。本发明的不同特征和步骤可结合在不同于以上所述的其它组合中。本发明仅受所附权利要求的限制。

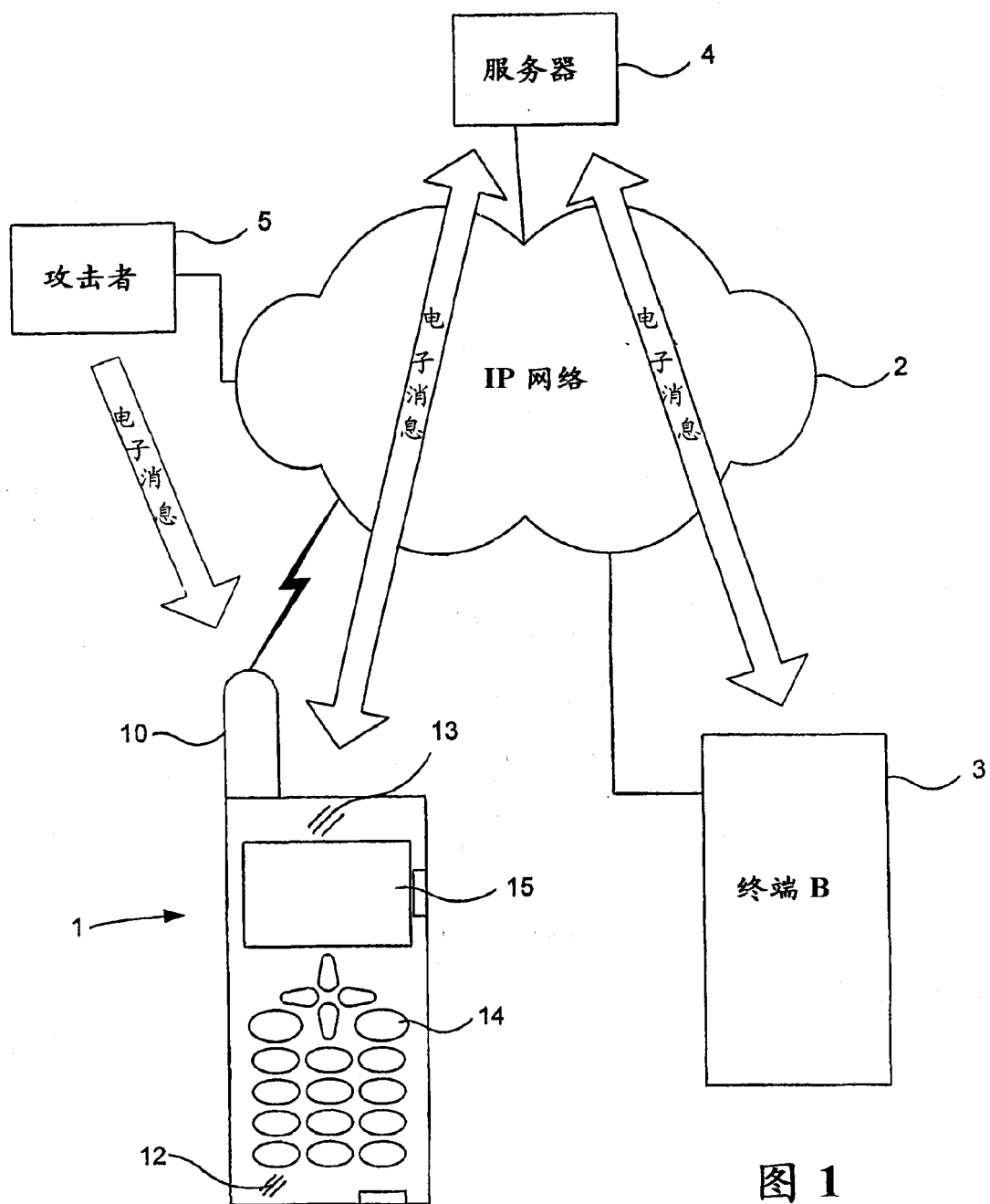


图 1

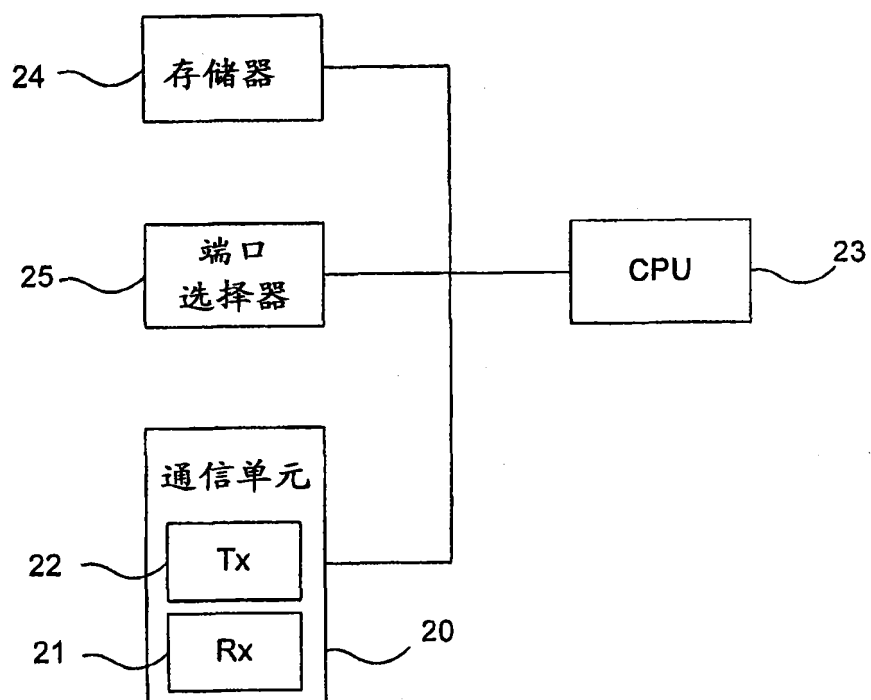


图 2

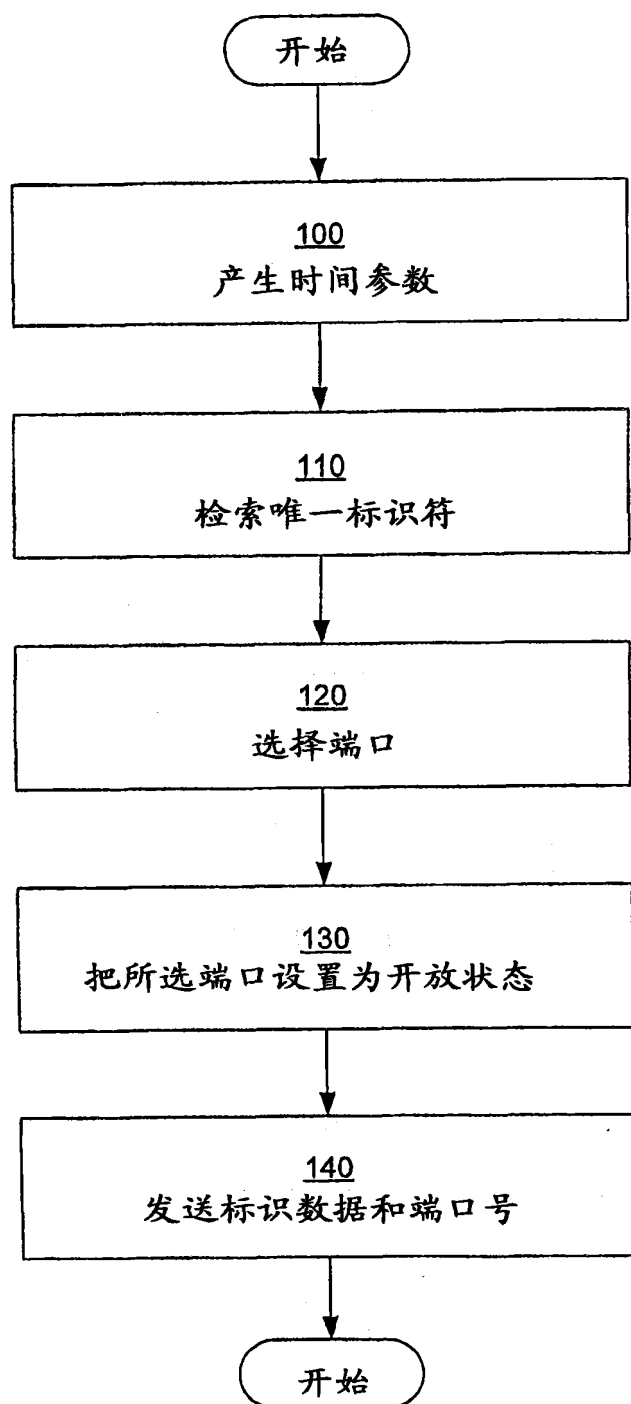


图 3