

(12) 发明专利

(10) 授权公告号 CN 101043320 B

(45) 授权公告日 2011.07.06

(21) 申请号 200610065507.0

CN 1298229 A, 2001.06.06, 全文.

(22) 申请日 2006.03.20

审查员 李东

(73) 专利权人 明基电通(上海)有限公司

地址 200335 上海市长宁区广顺路33号B栋
6层

(72) 发明人 白伦博

(74) 专利代理机构 北京康信知识产权代理有限公司
责任公司 11240

代理人 章社果 彭焱

(51) Int. Cl.

H04L 9/00 (2006.01)

(56) 对比文件

CN 1351789 A, 2002.05.29, 全文.

CN 1631022 A, 2005.06.22, 第5页第4、5段,
第8页第4、5段, 图2.

JP 特开 2003-141664 A, 2003.05.16, 全文.

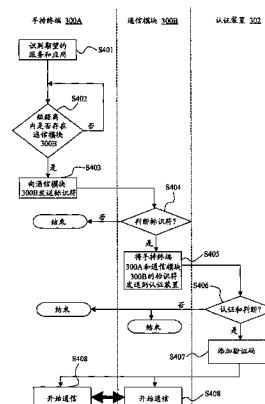
权利要求书 3 页 说明书 7 页 附图 8 页

(54) 发明名称

安全通信系统和方法

(57) 摘要

本发明公开了一种用于自组织网络中的至少两个通信终端之间的安全通信的通信系统,包括:第一通信终端;第二通信终端,通过短距离通信接收来自所述第一通信终端的第一数据,对所述第一数据进行检测,根据检测结果,生成第二数据;以及认证装置,位于网络上,通过所述网络接收来自所述第二通信终端的所述第二数据,对所述第二数据进行验证,以确定所述第一通信终端和所述第二通信终端中至少一个的身份。本发明还公开了一种用于在自组织网络中的两个通信终端之间进行通信的方法,包括:发送步骤;第一检测步骤;第二检测步骤;以及数据交换步骤。



1. 一种通信系统,用于实现自组织网络中的至少两个通信终端之间的安全通信,其特征在于,包括:

第一通信终端;

第二通信终端,通过短距离通信接收来自所述第一通信终端的第一数据,对所述第一数据进行检测,根据检测结果,生成第二数据;以及

认证装置,位于网络上,通过所述网络接收来自所述第二通信终端的所述第二数据,对所述第二数据进行验证,以确定所述第一通信终端和所述第二通信终端中至少一个的身份。

2. 根据权利要求 1 所述的通信系统,其特征在于,所述第一通信终端和所述第二通信终端均至少包括:

短距离收发器,用于短距离发送和接收数据;

处理单元,用于检测由所述短距离收发器所接收的数据,并对所接收的数据进行处理;以及

存储单元,用于存储由所述短距离收发器所接收的数据、所述处理单元执行处理所需要的程序、以及来自所述处理单元的所述检测结果和处理结果。

3. 根据权利要求 2 所述的通信系统,其特征在于,所述第一通信终端还包括:

输入单元,用于供用户选择期望激活的服务和应用以及激活服务和应用所需要的数据。

4. 根据权利要求 2 所述的通信系统,其特征在于,所述第二通信终端和所述认证装置还包括:

网络收发器,用于在所述网络中发送和接收数据,所述认证装置的网络收发器接收来自所述第二通信终端的所述第二数据,通过所述认证装置,对所述第二数据进行验证,以确定所述第一通信终端和所述第二通信终端中至少一个的身份。

5. 根据权利要求 1 所述的通信系统,其特征在于,所述短距离通信通过电缆连接、红外线连接、无线射频以及超声波连接中的至少一种连接方式实现。

6. 根据权利要求 1 所述的通信系统,其特征在于,所述短距离通信通过蓝牙连接、WLAN 连接中的至少一种连接方式实现。

7. 根据权利要求 1 所述的通信系统,其特征在于,所述第二通信终端用于在接收所述第一数据之后检测所述第一数据,并根据检测结果在所述第一数据上生成所述第二数据,并将所得到的第二数据发送给所述认证装置。

8. 根据权利要求 7 所述的通信系统,其特征在于,所述认证装置用于在接收所述第二数据之后,检测所接收的数据,在其检测结果为“否”时,终止所述第一通信终端和所述第二通信终端之间的服务和应用。

9. 根据权利要求 7 所述的通信系统,其特征在于,所述认证装置用于在接收所述第二数据之后,检测所接收的数据,在其检测结果为“是”时,向所述第一通信终端和所述第二通信终端发送肯定应答,所述第一通信终端和所述第二通信终端之间通过短距离收发器和网络收发器中的至少一种来进行数据交换。

10. 根据权利要求 9 所述的通信系统,其特征在于,所述肯定应答通过在所述所接收的数据上添加验证码得到。

11. 根据权利要求 10 所述的通信系统,其特征在于,所述第一数据、所述第二数据、以及所述验证码在被发送之前经过编码器的编码。

12. 根据权利要求 1 所述的通信系统,其特征在于,所述第一数据是装置标识码、用户标识码、服务或应用的标识码、以及随机数中的至少一种。

13. 根据权利要求 3 所述的通信系统,其特征在于,所述的服务和应用包括在 ATM 机上进行的操作、收费站付费、餐厅点菜、向其它通信终端付费、以及传送机密遥测信息中的至少一种。

14. 根据权利要求 1 所述的通信系统,其特征在于,所述第一通信终端和第二通信终端包括车载计费器、移动电话、PDA、ATM 机、寻呼机、以及便携式计算机中的至少一种。

15. 一种通信方法,用于实现自组织网络中的至少两个通信终端之间的安全通信,其特征在于,包括以下步骤:

发送步骤,第一通信终端通过短距离通信向第二通信终端发送第一数据;

第一检测步骤,所述第二通信终端对通过短距离通信接收到的所述第一数据进行检测,其特征在于,

在检测结果为是时,所述第二通信终端将所述第一数据通过网络发送给认证装置;

在检测结果为否时,所述第二通信终端终止服务和应用;

第二检测步骤,所述认证装置对通过所述网络从所述第二通信终端接收的数据进行检测,其特征在于,

在检测结果为是时,所述认证装置通过所述网络向所述第一通信终端和所述第二通信终端发送肯定应答;

在检测结果为否时,所述认证装置通过所述网络终止所述第一通信终端和所述第二通信终端之间的服务和应用;以及

数据交换步骤,在所述第一通信终端和所述第二通信终端中的至少一个接收到由所述认证装置发送的所述肯定应答之后,所述第一通信终端和所述第二通信终端之间通过短距离通信连接和网络通信连接中的至少一种来进行数据交换。

16. 根据权利要求 15 所述的通信方法,其特征在于,所述短距离通信连接包括电缆连接、红外线连接、无线射频以及超声波连接中的至少一种。

17. 根据权利要求 15 所述的通信方法,其特征在于,所述短距离通信连接包括蓝牙连接、WLAN 连接中的至少一种。

18. 根据权利要求 15 所述的通信方法,其特征在于,所述第一检测步骤还包括:在检测结果为是时,在所述第一数据上生成第二数据,并将得到的第二数据发送给所述认证装置。

19. 根据权利要求 15 所述的通信方法,其特征在于,所述肯定应答通过在所述第二通信终端接收的数据上添加验证码得到。

20. 根据权利要求 18 所述的通信方法,其特征在于,还包括编码步骤,以对所述第一数据、所述第二数据在被发送之前经过编码器的编码。

21. 根据权利要求 15 所述的通信方法,其特征在于,所述第一数据是装置标识码、用户标识码、服务或应用的标识码、以及随机数中的至少一种。

22. 根据权利要求 15 所述的通信方法,其特征在于,所述的服务和应用包括在 ATM 机上进行的操作、收费站付费、餐厅点菜、向其它通信终端付费、以及传送机密遥测信息中的至

少一种。

23. 根据权利要求 15 所述的通信方法, 其特征在于, 所述第一通信终端和第二通信终端包括车载计费器、移动电话、PDA、ATM 机、寻呼机、以及便携式计算机中的至少一种。

安全通信系统和方法

技术领域

[0001] 本发明涉及通信领域,更具体地,涉及实现自组织网络中的至少两个通信终端之间的安全通信的通信系统和方法。

背景技术

[0002] 近年来,移动无线通信分布在世界各地,并且在一些国家,几乎每个人都拥有移动电话。移动电话随着时间已经拥有越来越多的功能。除了最基本的电话功能之外,移动电话还具有发送电子邮件、发送信息以及组织等功能,并被用作相机或录像机、浏览器等。

[0003] 现在还有一种趋势,就是许多装置可以具有电话的功能,如:个人数字助理 (PDA, Personal Digital Assistant),并且越来越多的个人数字助理现在具有电话的功能。这是通过使用无线通信模块来实现的,其中无线通信模块可以是卡或芯片,而不必具有类似移动电话的用户界面,例如:在带有无线车载计费器的车载系统中,使用者进入收费站时,可以经由无线车载计费器向收费站发送付费请求,收费站确认后,无线车载计费器直接向收费站进行网络付费。因为具有类似无线通信模块的装置可以彼此间进行交互,或者与使用移动无线通信网络的移动电话进行交互,所以,具有无线通信模块的装置,为新服务和新应用提供了新的机会。

[0004] 在英国专利申请第 0130615.8 号中公开了通过短距离通信信号与其它兼容装置进行通信的数据处理装置。如图 1 所示,在该专利申请中,提出了在 ad-hoc 网络中查找特定数据并将所需数据从一个终端传递到另一终端的方法。但是其并没有涉及在传递数据的过程中,如何能够保证数据交互的安全性,也没有涉及自组织网络中的两个终端的识别和定位,更没有涉及通过无线网络为具有无线通信模块的装置或移动电话提供的移动无线服务和应用,例如,收费站交费、在 ATM 上进行交易、快餐店购买快餐、餐厅点餐、支付帐单、车载计费器以及传输秘密遥测数据等。

[0005] 因此,存在着以下需求,也就是,实现自组织网络中的至少两个通信终端之间的安全通信,解决在两个通信终端之间的安全通信问题,并通过网络提供对两个通信终端的服务。

发明内容

[0006] 本发明旨在解决上述问题中的至少一个,为了实现这一目的,本发明提供了通信系统和方法,该系统和方法可以确保自组织网络中的至少两个通信终端中的第一通信终端在靠近第二通信终端时,可以享受由第二通信终端提供的服务,并解决激活服务或应用时的安全性问题。

[0007] 根据本发明的一个方面,提供了一种通信系统,用于实现自组织网络中的至少两个通信终端之间的安全通信,包括:第一通信终端;第二通信终端,通过短距离通信接收来自第一通信终端的第一数据,对第一数据进行检测,根据检测结果,生成第二数据;以及认证装置,位于网络上,通过网络接收来自第二通信终端的第二数据,对第二数据进行验证,

以确定第一通信终端和第二通信终端中至少一个的身份。

[0008] 第一通信终端和第二通信终端至少包括：短距离收发器，用于短距离发送和接收数据；处理单元，用于检测由短距离收发器所接收的数据，并对所接收的数据进行处理；以及存储单元，用于存储由短距离收发器所接收的数据、处理单元执行处理所需要的程序、以及来自处理单元的检测结果和处理结果。

[0009] 第一通信终端还包括：输入单元，用于供用户选择期望激活的服务和应用以及激活服务和应用所需要的数据。

[0010] 第二通信终端和认证装置还包括：网络收发器，用于在网络中发送和接收数据，认证装置的网络收发器接收来自第二通信终端的第二数据，通过认证装置，对第二数据进行验证，以确定第一通信终端和第二通信终端中至少一个的身份。

[0011] 网络包括移动通信网络、因特网、有线网络中的至少一种。

[0012] 短距离通信连接包括电缆连接、红外线连接、蓝牙连接、WLAN 连接、无线射频以及超声波连接中的至少一种。

[0013] 第一通信终端和第二通信终端包括移动电话、PDA、ATM 机、寻呼机、车载计费器以及便携式计算机中的至少一种。

[0014] 服务和应用包括在 ATM 机上进行的操作、收费站付费、餐厅点菜、向其它通信终端付费、以及传送机密遥测信息中的至少一种。

[0015] 根据本发明的另一方面，还提供了一种通信方法，用于实现自组织网络中的至少两个通信终端之间的安全通信，包括以下步骤：发送步骤，第一通信终端通过短距离通信向第二通信终端发送第一数据；第一检测步骤，第二通信终端对通过短距离通信接收到的第一数据进行检测，其中，在检测结果为是时，第二通信终端将第一数据通过网络发送给认证装置，在检测结果为否时，第二通信终端终止服务和应用；第二检测步骤，认证装置对通过网络从第二通信终端接收的数据进行检测，其中，在检测结果为是时，认证装置通过网络向第一通信终端和第二通信终端中的至少一个发送肯定应答，在检测结果为否时，认证装置通过网络终止第一通信终端和第二通信终端之间的服务和应用；以及数据交换步骤，在第一通信终端和第二通信终端中的至少一个接收到由认证装置发送的肯定应答之后，第一通信终端和第二通信终端之间通过短距离通信连接和网络通信连接中的至少一种来进行数据交换。

[0016] 因此，本发明的优点在于，在没有增加用于防止激活非期望的服务或错收费等错误报警的费用的同时，通过网络上的认证装置保证自组织网络中的至少两个通信装置之间的安全通信。

附图说明

[0017] 图 1 示出了现有技术的在网络中查找数据的方法的示意图；

[0018] 图 2 示出了根据本发明的实施例的通信终端的示意图；

[0019] 图 3 示出了根据本发明的一个实施例的通信系统的示意图；

[0020] 图 4 示出了根据本发明的一个实施例的通信方法的流程图；

[0021] 图 5 示出了根据本发明的另一实施例的通信系统的示意图；

[0022] 图 6 示出了根据本发明的另一实施例的通信方法的流程图；

[0023] 图 7 示出了根据本发明的又一实施例的通信系统的示意图 ; 以及

[0024] 图 8 示出了根据本发明的又一实施例的通信方法的流程图。

具体实施方式

[0025] 下面将参考附图详细描述本发明的实施例。

[0026] 图 2 示出了根据本发明的实施例的通信终端的示意图。如图 2 所示, 通信终端 200 包括 : 天线 202; 网络收发器 204, 用于在移动网络中发送和接收数据; 短距离收发器 206, 用于短距离发送和接收数据; 处理单元 208, 用于检测并判断由网络收发器 204 和短距离收发器 206 中的至少一个所接收的数据, 对所接收的数据进行检测和处理, 以及将检测结果和处理结果发送到网络收发器 204 和短距离收发器 206 中的至少一个; 存储单元 210, 用于存储由网络收发器 204 和短距离收发器 206 中至少一个所接收的数据、处理单元执行处理所需要的程序、以及来自处理单元的检测结果和处理结果; 以及输入单元 212, 用于使用户选择期望激活的服务和应用。其中处理单元 208 还包括 : 检测器 2084, 用于接收网络收发器 204 或短距离收发器 206 的数据信号并进行判断。可选地, 处理单元 208 还可以包括随机值产生器 2086, 用于在每一次激活服务和应用时产生随机值; 以及编码器 2088, 用于在检测器 2084 的检测结果为“是”时, 对数据信号进行编码。可选地, 通信装置 200 还可以包括接口, 用于使用电缆与另一通信装置相连接进行通信。

[0027] 根据本发明的通信系统有着很多应用, 下面结合具体的应用进行说明。

[0028] 在 ATM 机上的应用

[0029] 图 3 示出了根据本发明的一个实施例的通信系统的示意图。在该实施例中, 本发明用于在 ATM 机上进行操作。如图 3 所示, 该通信系统 30 包括 : 手持终端 (第一通信终端) 300A, 具有图 2 所示结构; 通信模块 300B, 设置在 ATM 机内, 具有图 2 所示结构 (在此应该理解, 该通信模块中的处理单元、存储单元和输入单元也可以与 ATM 机共用), 用于通过短距离收发器 306B 接收来自手持终端 300A 的数据, 并通过网络收发器 304B 或短距离收发器 306B 与手持终端 300A 进行数据交换来实现服务和应用; 以及认证装置 302, 位于网络上 (本实施例中可以为因特网), 用于验证和确认手持终端 300A 和通信模块 300B。其中, 认证装置 302 具有与手持终端 300A 和通信模块 300B 相似的结构。

[0030] 图 4 示出了根据本发明的一个实施例的通信系统的操作流程图。如图 4 所示, 在该系统中, 手持终端 300A 在启动时加载在 ATM 机上进行相关操作 (例如, 存款、取款、转帐或支付帐单等) 的应用程序。这些应用程序可以预先存储在存储单元 310A 中, 也可以后来通过下载或安装添加到存储单元 310A 中。用户通过手持终端 300A 的输入单元 312A 选择其期望激活的服务和应用。在此假设用户选择支付帐单, 手持终端 300A 的处理单元 308A 对用户的输入进行识别 (S401), 并检测在短距离范围内是否存在对应所选择的服务和应用的通信终端 (在该实施例中为安装在 ATM 机上的通信模块 300B) (S402)。如果不存在所需的通信模块 300B (S402, 否), 则返回到 S402。如果存在所需的通信模块 300B (S402, 是), 则通过短距离收发器 306A 向该通信模块 300B 发送手持终端 300A 的标识符, 可选地, 也可以发送用户标识符、所选择的服务和应用标识符以及随机数等。通信模块 300B 通过短距离收发器 306B 接收手持终端 300A 发送的标识符, 并将该标识符传送到处理单元 308B, 处理单元将处理后的数据信号传送到检测器。检测器对该数据信号进行判断 (S404), 例如, 判断其是

否为该 ATM 机认可的用户。如果判断结果为“否”(S404, 否), 即通信模块 300B 不能识别手持终端 300A, 则通信模块 300B 的处理单元 308B 通过短距离收发器 306B 向手持终端 300A 发送终止信号, 该应用终止。如果判断结果为“是”(S404, 是), 即通信模块 300B 可以识别手持终端 300A 并愿意执行被请求的服务, 则通信模块 300B 的处理单元 308B 在接收到的手持终端 300A 的标识符上添加通信模块 300B 的标识符, 并由编码器对其进行编码, 然后通过网络收发器 304B 将得到的数据发送到位于一网络上的认证装置 302(S405)。可选地, 在通信模块 300B 可以识别手持终端 300A 之后, 向手持终端 300A 发出输入密码的请求, 或向其发送由通信模块 300B 的随机值产生器产生的随机数, 要求用户通过手持终端 300A 的输入单元 312A 正确输入该随机数, 以进一步确认用户的身份。在此应当理解, 如果仅将手持终端 300A 的标识符发送到认证装置 302, 本发明仍然可以实现。

[0031] 认证装置 302 通过其网络收发器 3024 接收来自通信模块 300B 的数据, 认证装置 302 的处理单元 3026 对该数据进行认证和判断 (S406), 例如, 手持终端 300A 是否为注册的用户, 其是否具有良好的信用, 以及其是否具有足够的权限使用期望的服务和应用等。

[0032] 如果判断的结果为“否”(S406, 否), 则认证装置 302 通过网络收发器 3024 向手持终端 300A 和通信模块 300B 发送终止服务和应用的信号, 手持终端 300A 和通信模块 300B 分别通过网络收发器 304A 和 304B 接收终止信号并分别通过处理单元 308A 和 308B 终止通信。

[0033] 如果判断的结果为“是”(S406, 是), 则认证装置 302 的处理单元 3026 在接收到的数据上添加验证码 (S407), 然后将添加验证码之后得到的数据作为肯定应答通过网络收发器 3022 发送给手持终端 300A 和通信模块 300B。在手持终端 300A 和通信模块 300B 分别通过网络收发器 304A 和 304B 接收到肯定应答之后, 两者开始通过短距离收发器 306A 和 306B 进行通信并执行服务和应用 (S408)。在此应当理解, 如果认证装置 302 仅向手持终端 300A 和通信模块 300B 发送肯定应答, 而不添加验证码, 本发明仍然可以实现。可选地, 在手持终端 300A 和通信模块 300B 开始进行通信之后, 可以分别通过网络收发器 304A 和 304B 发送确认信号, 以通知认证装置 302, 本次通信成功。

[0034] 在收费站的应用

[0035] 图 5 示出了根据本发明的另一个实施例的通信系统的示意图。在该实施例中, 本发明用于在收费站缴费。如图 5 所示, 该通信系统 50 包括: 缴费卡 500A, 具有图 2 所示结构; 收费模块 500B, 设置在收费站内, 具有图 2 所示结构, 用于通过短距离收发器 506B 接收来自缴费卡 500A 的数据, 并通过网络收发器 504B 或短距离收发器 506B 与缴费卡 500A 进行数据交换来实现服务和应用; 以及认证装置 502, 位于网络上 (本实施例中可以为移动通信网络), 用于验证和确认缴费卡 500A 和收费模块 500B。其中, 认证装置 502 具有与缴费卡 500A 和收费模块 500B 相似的结构, 在此省略对其的详细描述。

[0036] 图 6 示出了根据本发明的另一个实施例的通信系统的操作流程图。如图 6 所示, 在该系统中, 缴费卡 500A 在启动时加载在收费站进行交费操作的应用程序。这些应用程序可以预先存储在存储单元 510A 中, 也可以后来通过下载或安装添加到存储单元 510A 中。用户通过缴费卡 500A 的输入单元 512A 选择付费, 缴费卡 500A 的处理单元 508A 对用户的输入进行识别 (S601), 并检测在短距离范围内是否存在对应所选择的服务和应用的通信终端 (在该实施例中为安装在收费站上的收费模块 500B) (S602)。如果不存在所需的收费模块

500B(S602,否),则返回到S602。如果存在所需的收费模块500B(S602,是),则通过缴费卡500A上的短距离收发器506A向该收费模块500B发送缴费卡500A的标识符(S603),可选地,也可以发送用户标识符、所选择的服务和应用标识符以及随机数等。交费模块500B通过短距离收发器506B接收缴费卡500A发送的标识符,并将该标识符传送到处理单元508B,处理单元将处理后的数据信号传送到检测器。检测器对该数字信号进行判断(S604),例如,判断其是否为该收费站认可的用户。如果判断结果为“否”(S604,否),即收费模块500B不能识别缴费卡500A,则收费模块500B的处理单元508B通过短距离收发器506B向缴费卡500A发送终止信号,该应用终止。如果判断结果为“是”(S604,是),即收费模块500B可以识别缴费卡500A并愿意执行被请求的服务,则收费模块500B的处理单元508B在接收到的收费卡500A的标识符上添加收费模块500B的标识符,并由编码器对其进行编码,然后通过网络收发器504B将得到的数据发送到位于网络上的认证装置502。可选地,在收费模块500B可以识别缴费卡500A之后,向缴费卡500A发出输入密码的请求,并向其发送由收费模块500B的随机值产生器产生的随机数,要求用户通过缴费卡500A的输入单元512A正确输入密码和该随机数,以进一步确认用户的身份。在此应当理解,如果仅将缴费卡500A的标识符发送到认证装置502,本发明仍然可以实现。

[0037] 认证装置502通过其网络收发器5024接收来自收费模块500B的数据,认证装置502的处理单元5026对该数据进行认证和判断(S606),例如,缴费卡500A是否为注册的用户,其是否具有良好的信用,以及其是否具有足够的权限使用期望的服务和应用等。

[0038] 如果判断的结果为“否”(S606,否),则认证装置502通过网络收发器5024向缴费卡500A和收费模块500B发送终止服务和应用的信号,缴费卡500A和收费模块500B分别通过网络收发器504A和504B接收终止信号并分别通过处理单元508A和508B终止通信。

[0039] 如果判断的结果为“是”(S606,是),则认证装置502的处理单元5026在接收到的数据上添加验证码(S607),然后将添加验证码之后得到的数据作为肯定应答通过网络收发器5024发送给缴费卡500A和收费模块500B。在缴费卡500A和收费模块500B分别通过网络收发器504A和504B接收到肯定应答之后,两者开始通过短距离收发器506A和506B进行通信并执行服务和应用(S608)。在此应当理解,如果认证装置502仅向缴费卡500A和收费模块500B发送肯定应答,而不添加验证码,本发明仍然可以实现。可选地,在缴费卡500A和收费模块500B开始进行通信之后,可以分别通过网络收发器504A和504B发送确认信号,以通知认证装置502,本次通信成功。

[0040] 在传输机密数据时的应用

[0041] 图7示出了根据本发明的又一实施例的通信系统的示意图。在该实施例中,本发明用于在维护或维修装置时传输机密数据。如图7所示,该通信系统70包括:手持终端700A,具有图1所示结构;机密数据通信模块700B,设置在任何需要其数据被保密的装置内,具有图1所示结构,用于通过机密数据模块的短距离收发器706B接收来自手持终端700A的数据,并通过移动网络收发器704B或短距离收发器706B与手持终端700A进行数据交换来实现服务和应用;以及认证装置702,位于网络上,用于验证和确认手持终端700A和机密数据通信模块700B。其中,认证装置702具有与手持终端700A和机密数据通信模块700B相似的结构,在此省略对其的详细描述。

[0042] 图8示出了根据本发明的又一实施例的通信系统的操作流程图。如图8所示,在

该系统中，手持终端 700A 在启动时加载与传输机密数据相关的应用程序。这些应用程序可以预先存储在存储单元 710A 中，也可以后来通过下载或安装添加到存储单元 710A 中。用户通过手持终端 700A 的输入单元 712A 选择其期望激活的服务和应用。手持终端 700A 的处理单元 708A 对用户的输入进行识别 (S801)，并检测在短距离范围内是否存在对应所选择的服务和应用的通信终端（在该实施例中为机密数据通信模块 700B）(S802)。如果不存在所需的机密数据通信模块 700B(S802, 否)，则返回到 S802。如果存在所需的机密数据通信模块 700B(S802, 是)，则通过短距离收发器 706A 向该机密数据通信模块 700B 发送手持终端 700A 的标识符 (S803)，可选地，也可以发送用户标识符、所选择的服务和应用标识符以及随机数等。机密数据通信模块 700B 通过短距离收发器 706B 接收手持终端 700A 发送的标识符，并将该标识符传送到处理单元 708B，处理单元将处理后的数据信号传送到检测器。检测器对该数字信号进行判断 (S804)，例如，判断其是否为该装置认可的用户。如果判断结果为“否”(S804, 否)，即机密数据通信模块 700B 不能识别手持终端 700A，则机密数据通信模块 700B 的处理单元 708B 通过短距离收发器 706B 向手持终端 700A 发送终止信号，该应用终止。如果判断结果为“是”(S804, 是)，即机密数据通信模块 700B 可以识别手持终端 700A 并愿意执行被请求的服务，则机密数据通信模块 700B 的处理单元 708B 在接收到的手持终端 700A 的标识符上添加机密数据通信模块 700B 的标识符，并由编码器对其进行编码，然后通过移动网络收发器 704B 将得到的数据发送到位于网络上的认证装置 702。可选地，在机密数据通信模块 700B 可以识别手持终端 700A 之后，向手持终端 700A 发出输入密码的请求，或向其发送由机密数据通信模块 700B 的随机值产生器产生的随机数，要求用户通过手持终端 700A 的输入单元 712A 正确输入该随机数，以进一步确认用户的身份。在此应当理解，如果仅将手持终端 700A 的标识符发送到认证装置 702，本发明仍然可以实现。

[0043] 认证装置 702 通过其移动网络收发器 7024 接收来自通信模块 700B 的数据，认证装置 702 的处理单元 7026 对该数据进行认证和判断 (S806)，例如，手持终端 700A 是否为注册的用户，以及其是否具有足够的权限使用期望的服务和应用等。

[0044] 如果判断的结果为“否”(S806, 否)，则认证装置 702 通过网络收发器 7024 向手持终端 700A 和机密数据通信模块 700B 发送终止服务和应用的信号，手持终端 700A 和通信模块 700B 分别通过网络收发器 704A 和 704B 接收终止信号并分别通过处理单元 708A 和 708B 终止通信。

[0045] 如果判断的结果为“是”(S806, 是)，则认证装置 702 的处理单元 7026 在接收到的数据上添加验证码 (S807)，然后将添加验证码之后得到的数据作为肯定应答通过网络收发器 7024 发送给手持终端 700A 和机密数据通信模块 700B。在手持终端 700A 和机密数据通信模块 700B 分别通过网络收发器 704A 和 704B 接收到肯定应答之后，两者开始通过短距离收发器 706A 和 706B 进行通信并执行服务和应用 (S808)。在此应当理解，如果认证装置 702 仅向手持终端 700A 和机密数据通信模块 700B 发送肯定应答，而不添加验证码，本发明仍然可以实现。可选地，在手持终端 700A 和机密数据通信模块 700B 开始进行通信之后，可以分别通过移动网络收发器 704A 和 704B 发送确认信号，以通知认证装置 702，本次通信成功。

[0046] 在根据本发明的实施例中，所有的数据在被发送之前都经过编码器的编码。通过上述结合实施例对本发明进行的描述可以了解，在根据本发明的系统和方法中，第一通信

终端通过短距离通信连接来查找第二通信终端,以确保仅在短距离内的通信装置被找到,而不会产生错误报警。并且在该系统中,在通信过程中采用了各种编码,可以保证通信中的安全性。此外,认证装置通过网络连接来验证和确认两个通信终端,这与两通信终端通过短距离通信连接来发送识别码的方式不同,这使得整个系统中的通信更加安全。

[0047] 在根据本发明的实施例中,第一通信终端通过短距离通信连接来查找第二通信终端,在此,短距离通信连接包括电缆连接、红外线连接、蓝牙连接、WLAN 连接、无线射频以及超声波连接等,短距离连接的距离可以在 0m 到 1600m 的范围内,优选地,在 0m 到 100m 的范围内,在该范围内,第一通信终端和第二通信终端之间的通信效果更好,更适于本发明的应用。

[0048] 应当理解,本发明除了在上述实施例中描述的可以对 ATM 机进行操作、在收费站缴费、以及传送机密信息之外,还可以用于在餐厅点菜、向其它通信终端缴费(例如,缴纳乘车费)等。

[0049] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

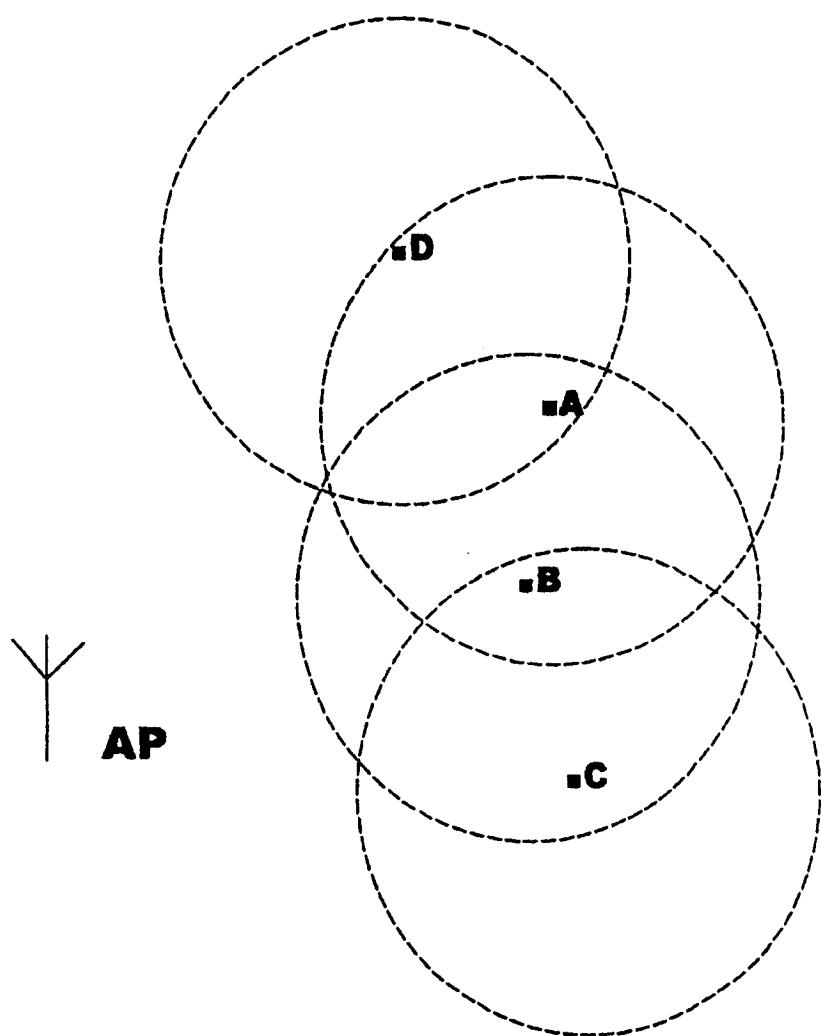


图 1

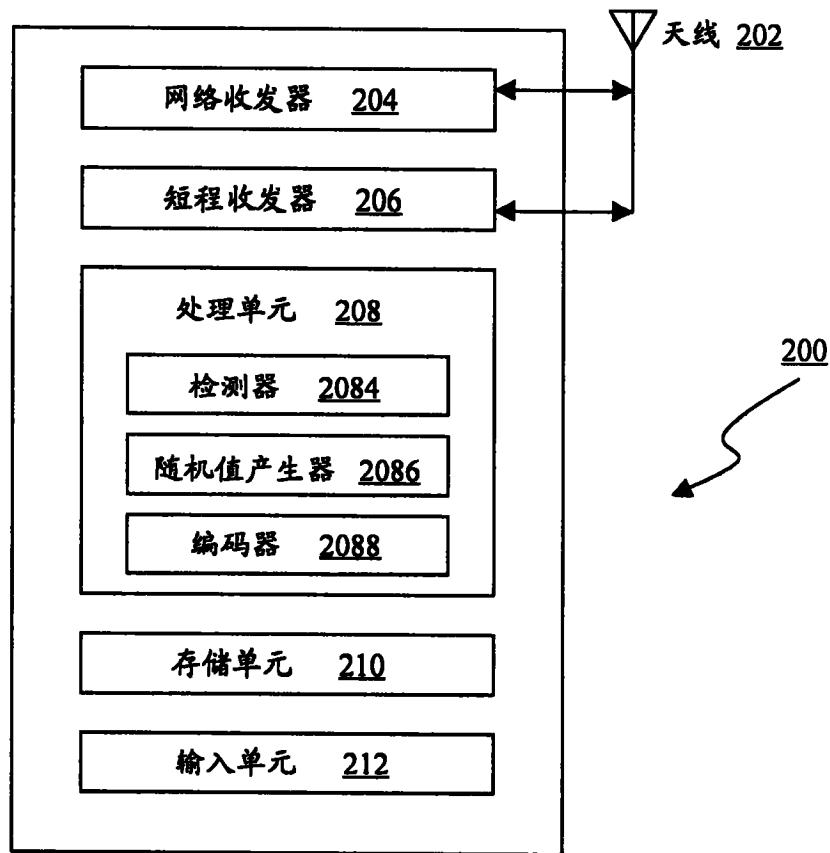


图 2

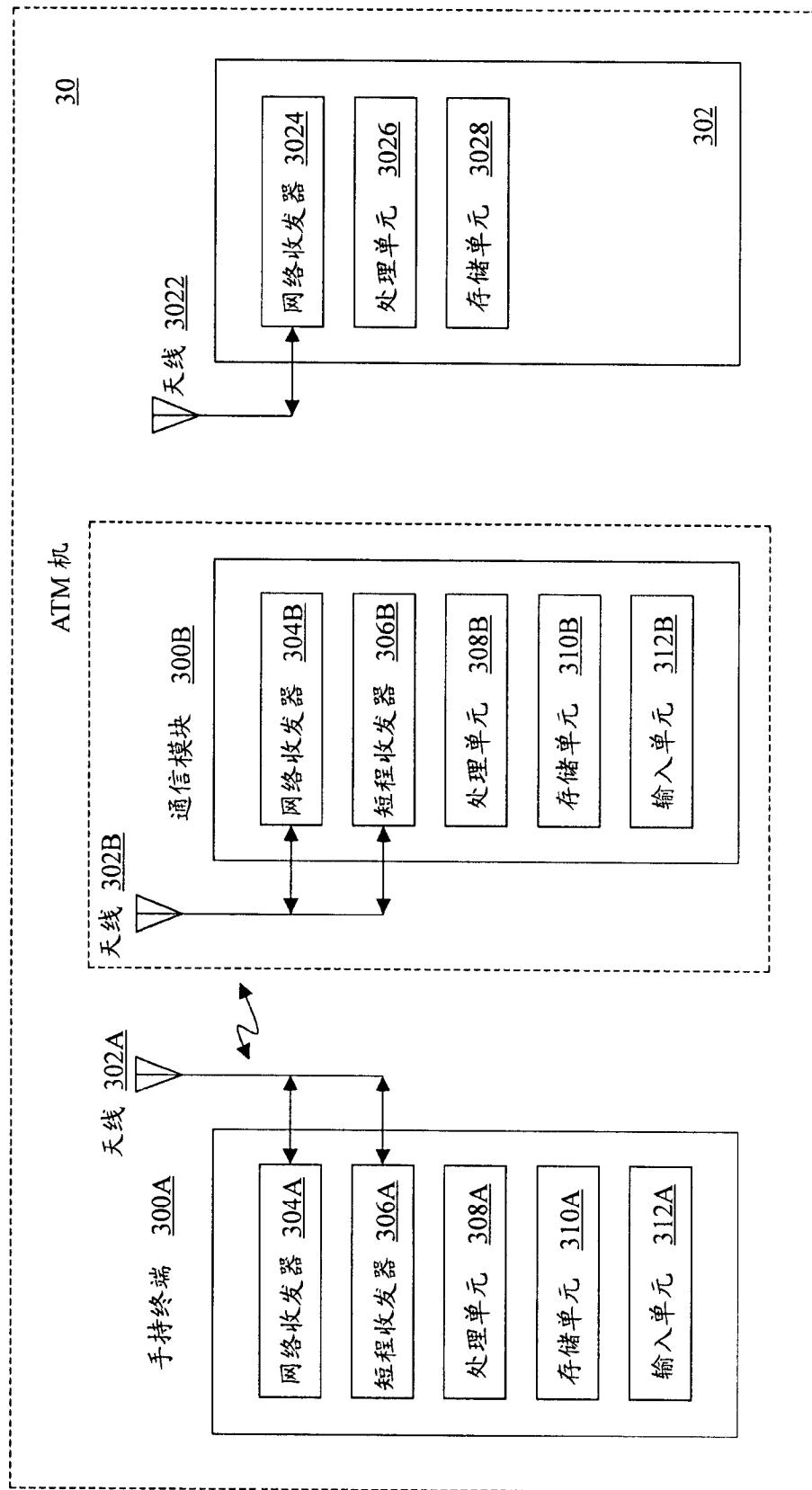


图 3

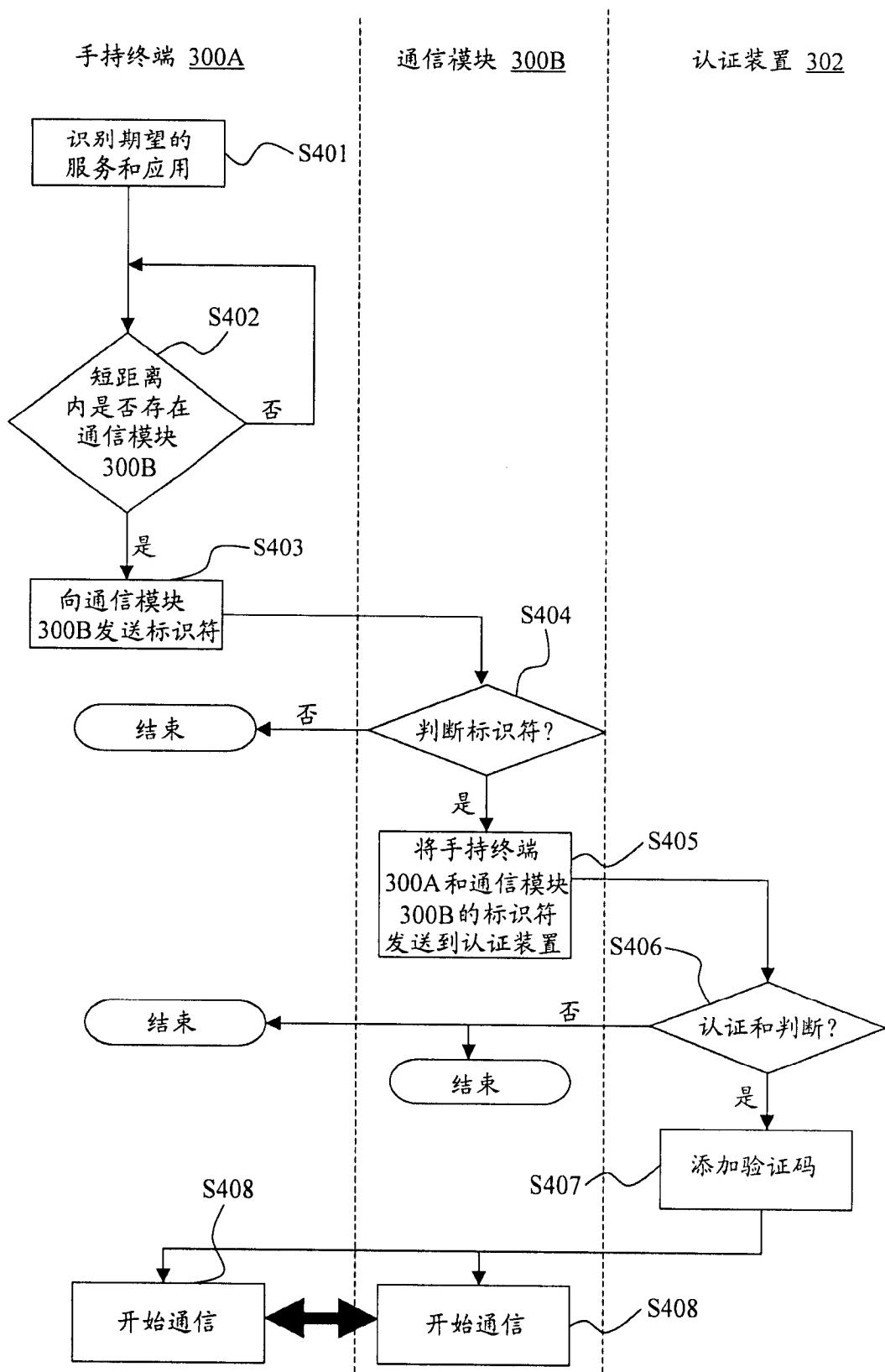


图 4

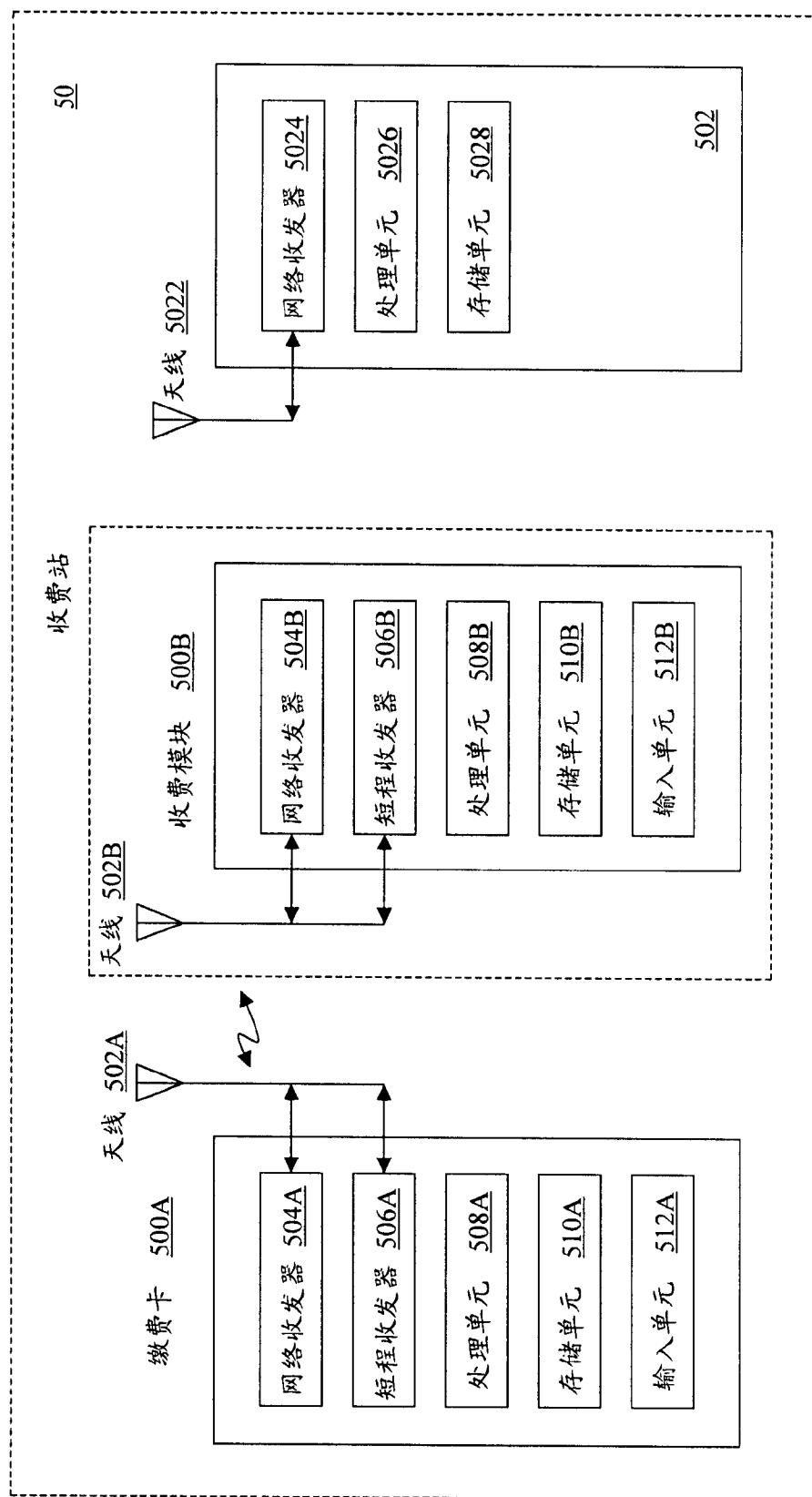


图 5

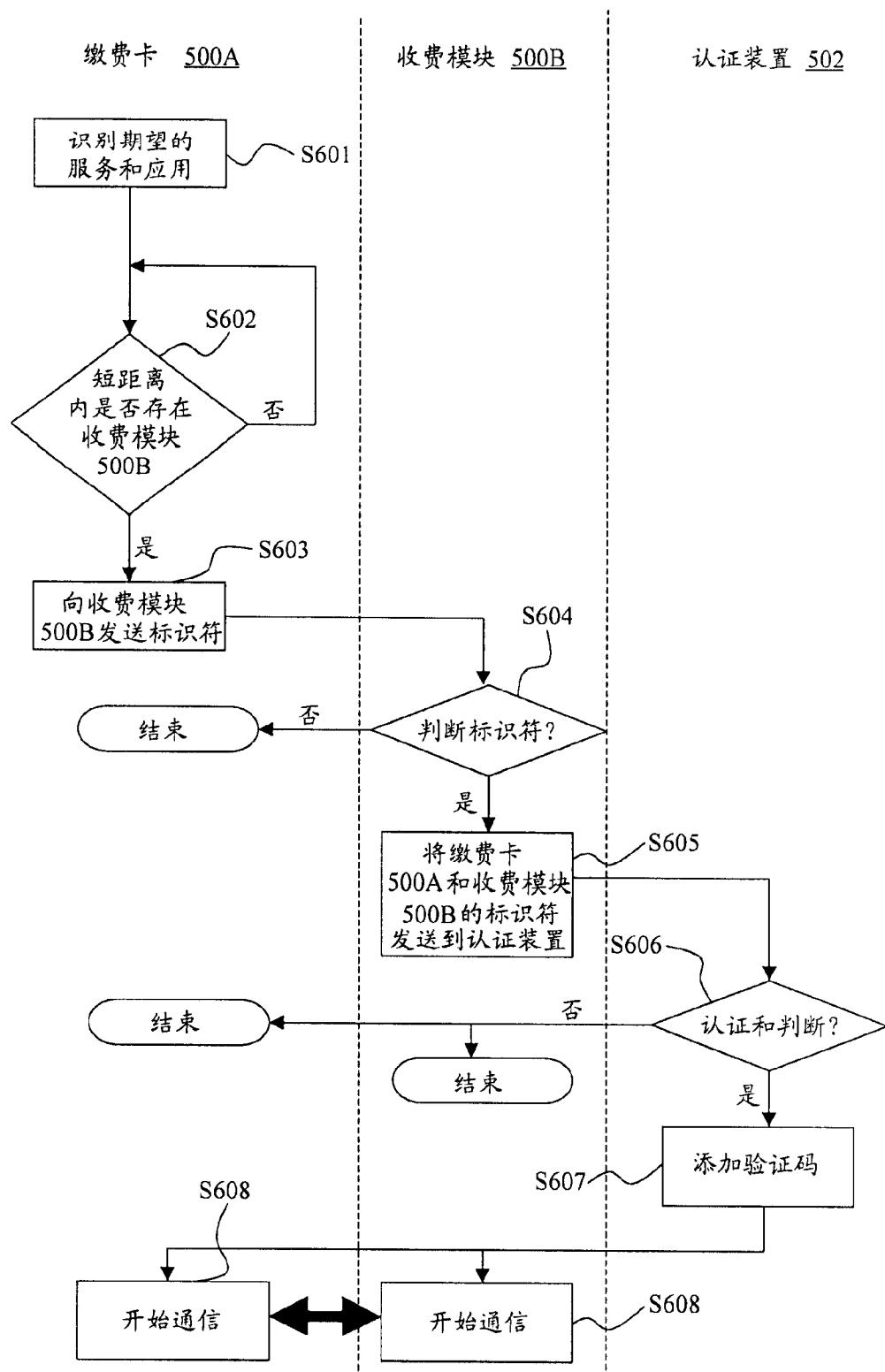


图 6

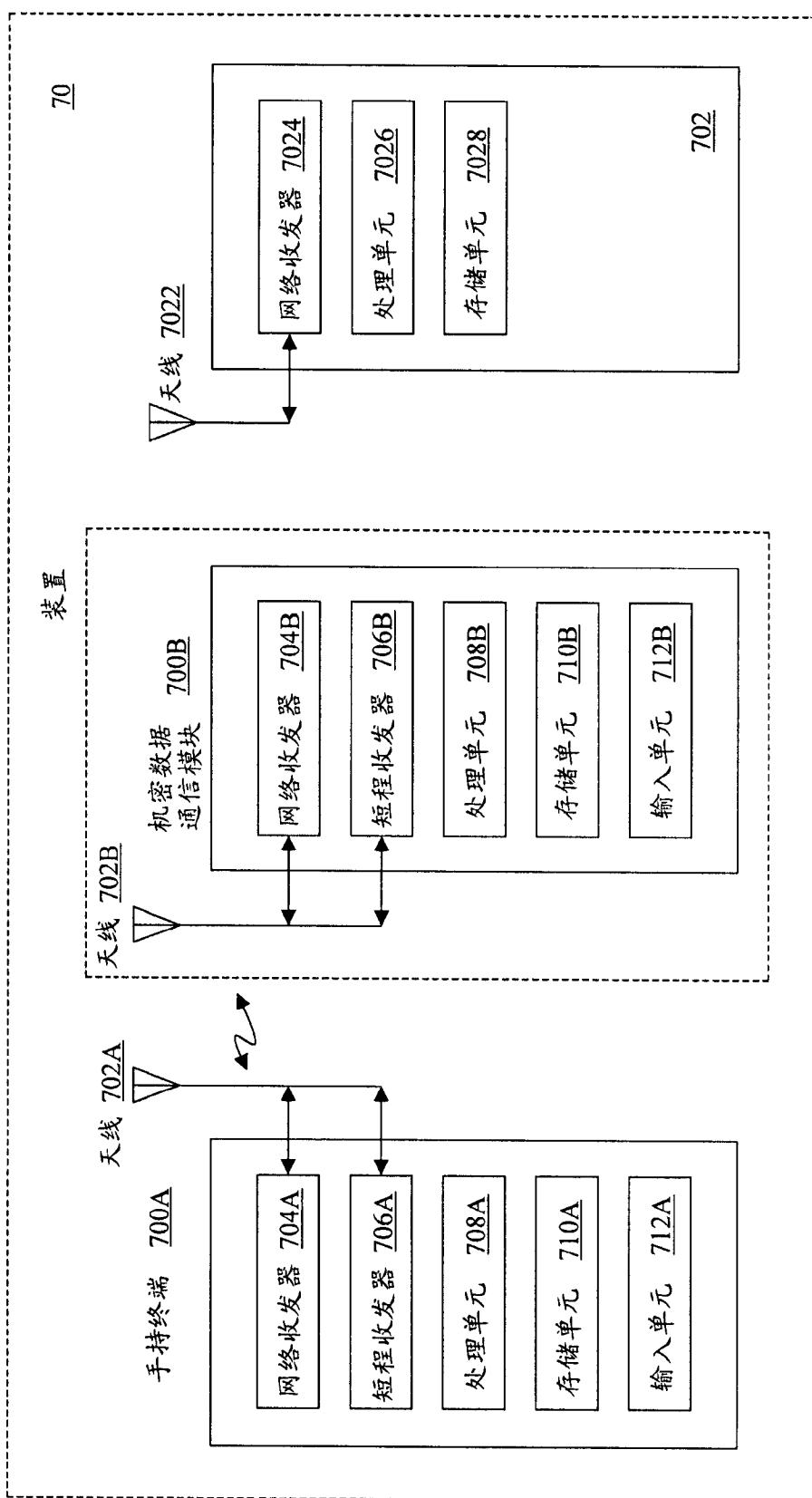


图 7

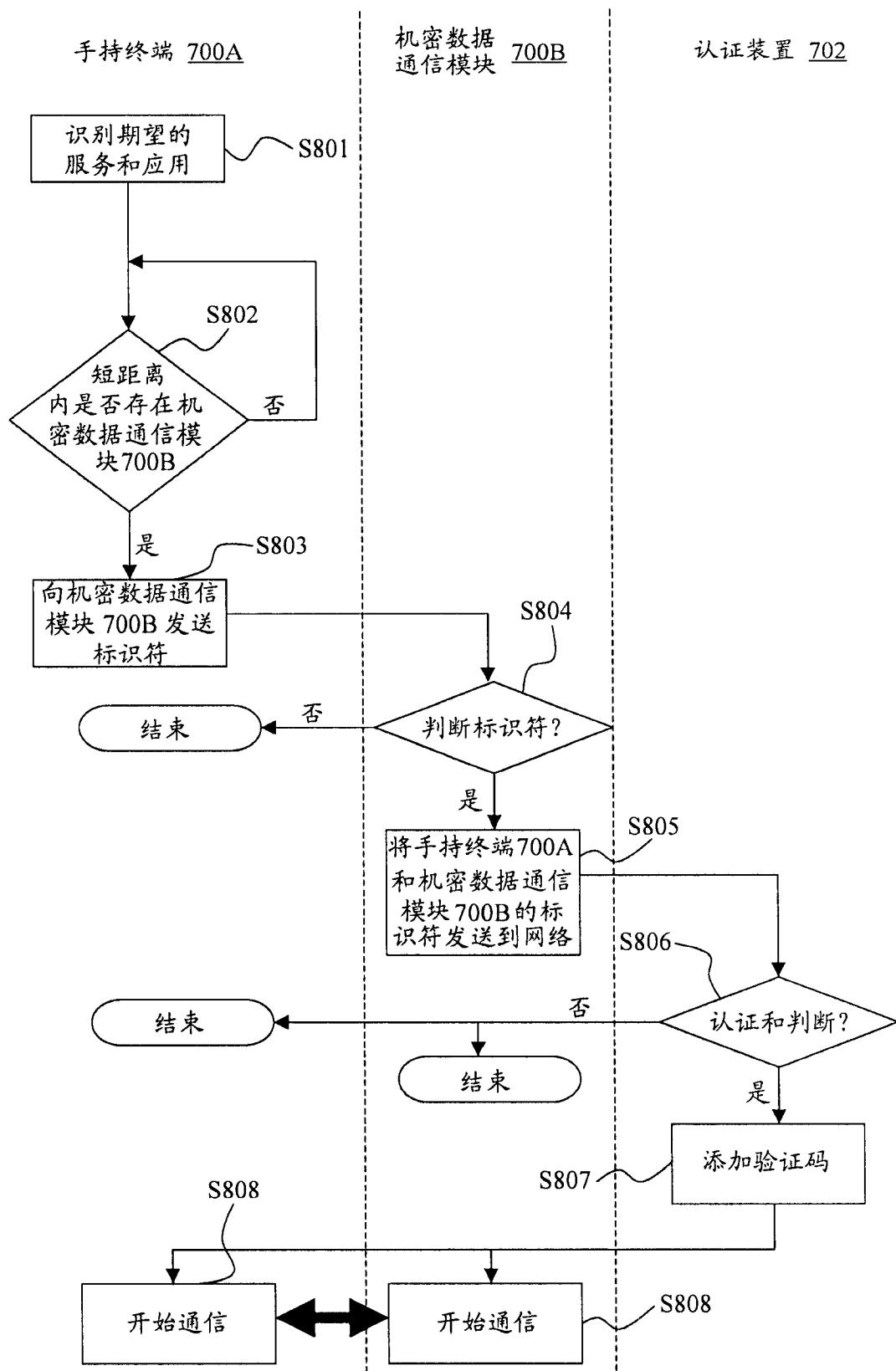


图 8