(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1650302 B
(45)授权公告日 2010.04.28

(21)申请号 03809384.7

(22)申请日 2003.04.24

(30)优先权数据
60/375,449 2002.04.26 US

(85)PCT申请进入国家阶段日
2004.10.26

(86)PCT申请的申请数据
PCT/CA2003/000606 2003.04.24

(87)PCT申请的公布数据
WO2003/091917 EN 2003.11.06

(73)专利权人 捷讯研究有限公司
地址 加拿大安大略省沃特卢市

(72)发明人 伊恩·M·罗伯森

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮

(51)Int.Cl.
G06F 17/00(2006.01)

(56)对比文件
US 5754306 A,1998.05.19, 全文.
US 6157954 A,2000.12.05, 全文.
EP 1026857 A2,2000.08.09, 全文.
EP 0971519 A1,2000.01.12, 全文.

审查员 盖浩

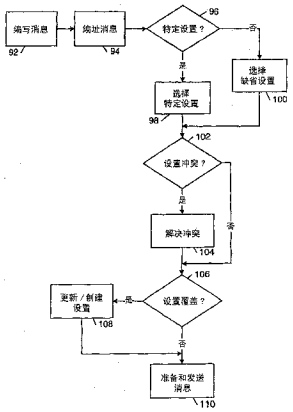
权利要求书 3 页 说明书 13 页 附图 5 页

(54)发明名称

选择消息设置的系统和方法

(57)摘要

提供了一种在一个消息客户机上选择消息设置的方法和系统。当要从消息客户机发送的输出消息被编址到一个消息接收者时，消息客户机访问一个数据存储器，以确定是否已经为消息接收者存储特定的消息设置。如果已经存储该消息接收者的特定消息设置，消息客户机选择用于该消息接收者的特定消息设置以控制所述输出消息的消息特性。



CN 1650302 B

1. 一种在消息客户机上选择消息设置的方法，包括步骤：

对于多个消息接收者的每一个，编写一个输出消息；

将所述输出消息编址到一个消息接收者；

确定是否已经为所述消息接收者建立特定的消息设置；以及

如果已经为所述消息接收者建立特定的消息设置，选择所述特定消息设置以控制所述输出消息的消息特性，所述消息特性包括消息加密，并且所选择的所述特定消息设置包括：当确定所述消息接收者和消息客户机在网络内防火墙后时选择不进行消息加密；

检测为所述多个消息接收者的每一个选择的特定消息设置之间的冲突消息设置；以及

解决任何检测到的冲突消息设置。

2. 如权利要求 1 所述的方法，其中，所述编址步骤包括步骤：选择在一个地址本中的一个地址本项目。

3. 如权利要求 2 所述的方法，其中，所述确定步骤包括步骤：确定所述特定的消息设置是否存储在所述地址本项目中。

4. 如权利要求 2 所述的方法，其中，

所述确定步骤包括步骤：确定所述地址本项目是否标识在由所述消息客户机可访问的数据存储单元中的所述特定消息设置；和

所述选择步骤包括从地址存储单元中选择在所述地址本项目中标识的特定消息设置。

5. 如权利要求 1 所述的方法，其中，

所述编址步骤包括步骤：使用与所述消息客户机相关的一个用户接口，人工输入所述消息接收者的一个地址；以及

所述确定步骤包括步骤：

确定所述地址是否存储在一个地址本的一个地址本项目中；和

如果所述地址存储在所述地址本的一个地址本项目中，确定特定消息设置是否存储在所述地址本项目中。

6. 如权利要求 1 所述的方法，其中，

所述编址步骤包括步骤：使用与所述消息客户机相关的一个用户接口，人工输入所述消息接收者的一个地址，所述地址包括用户名和域名；以及

所述确定步骤包括步骤：确定用于所述域名的特定消息设置是否存储在可由所述消息客户机访问的数据存储器中。

7. 如权利要求 1 所述的方法，其中，

所述输出消息是对在消息客户机处从一个消息发送者接收的消息的答复消息；以及

所述编址步骤包括步骤：从所述接收的消息插入一个地址作为所述消息接收者。

8. 如权利要求 7 所述的方法，其中，

所述确定步骤包括步骤：确定所述插入的地址是否存储在地址本的一个地址本项目中；以及

如果所述插入的地址存储在所述地址本中的一个地址本项目中，确定特定消息设置是否存储在所述地址本项目中。

9. 如权利要求 8 所述的方法，其中，所述插入的地址是所述消息发送者的一个地址。

10. 如权利要求 1 所述的方法，其中，解决检测的冲突消息设置的步骤包括步骤：

警告用户所述检测到的冲突消息设置；

提醒用户选择哪个所述冲突消息设置应该被选择；以及

基于所述用户的选择控制所述输出消息的消息特性。

11. 如权利要求 1 所述的方法，其中，所述解决检测的冲突消息设置的步骤包括步骤：准备多个输出消息，每个输出消息具有由每个所述冲突消息设置控制的消息特性。

12. 如权利要求 1 所述的方法，其中，所述多个消息接收者包括一个分发表。

13. 如权利要求 1 所述的方法，其中：

所述消息接收者是包括多个消息接收者的一个分发表；以及

所述确定步骤包括步骤：确定是否已经为所述分发表建立特定的消息设置。

14. 如权利要求 1 所述的方法，其中，所述消息加密按照安全多用途互联网邮件扩展 (S/MIME) 加密。

15. 如权利要求 1 所述的方法，其中，所述消息加密按照相当好保密 (PGP™) 加密。

16. 如权利要求 1 所述的方法，其中，所述消息客户机运行在一个无线移动通信设备上。

17. 如权利要求 1 所述的方法，其中，所述消息客户机运行在一个个人计算机系统上。

18. 一种选择消息设置的系统，包括：

一个数据存储器，被配置存储多个特定的消息设置；以及

一个消息客户机，被配置为：向所述消息接收者的每一个发送被编址到多个消息接收者的消息，访问所述数据存储器以确定是否已为多个消息接收者的每一个存储特定的消息设置，以及如果已经为所述消息接收者存储特定的消息设置，选择用于每一个所述消息接收者的特定消息设置以控制要发送至每一个所述消息接收者的消息的消息特性，其中，所述消息特性包括消息加密，并且所选择的所述特定消息设置包括：当确定所述消息接收者和消息客户机在网络内防火墙后时选择不进行消息加密；

配置所述消息客户机，以检测为所述多个消息接收者的每一个选择的特定消息设置之间的冲突消息设置和解决任何检测到的冲突消息设置。

19. 如权利要求 18 所述的系统，其中：

进一步配置所述数据存储器，以存储缺省的消息设置；以及

如果在数据存储器中还没有存储用于所述消息接收者的特定消息设置，进一步配置所述消息客户机，以选择缺省的消息设置控制消息的消息特性。

20. 如权利要求 18 所述的系统，其中，所述系统在从下列各项组成的组中选择的一个设备中实现：无线移动通信设备，具有数据通信功能的移动电话，无线语音通信设备，无线数据通信设备和无线双模式通信设备。

21. 如权利要求 18 所述的系统，其中，所述消息客户机是被配置发送安全和非安全消息的一个安全消息客户机。

22. 如权利要求 18 所述的系统，进一步包括：地址本数据存储器，被配置为存储用于多个联系的地址本项目，其中，所述多个地址本项目的每一个包括一个地址字段和用于一个相关联系的消息设置字段；以及配置在每个地址本项目中的消息设置字段，以存储用于所述相关联系的特定消息设置。

23. 如权利要求 18 所述的系统，进一步包括：地址本数据存储器，被配置为存储用于多

个联系的地址本项目，其中，所述多个地址本项目的每一个包括一个地址字段和用于一个相关联系的消息设置字段；以及配置在每个地址本项目中的消息设置字段，以存储用于存储在所述数据存储器中的联系的特定消息设置的标识符。

24. 如权利要求 18 所述的系统，其中：

所述数据存储器包括用于消息接收者的特定消息设置和用于分发表的特定消息设置，每个分发表包括多个消息接收者；以及

进一步配置所述消息客户机，访问所述数据存储器以确定是否已经为一个消息被编址到的分发表存储特定的消息设置，并且如果已经为所述分发表存储特定消息设置，为所述分发表选择所述特定的消息设置以控制所述消息的消息特性。

25. 如权利要求 18 所述的系统，进一步包括：

一个用户接口，被配置从一个用户接收输入，其中响应于来自用户的一个输入，一个消息被编址到多个消息接收者。

选择消息设置的系统和方法

发明领域

[0001] 本发明一般涉及安全电子消息领域，并且特别涉及在一个消息客户机上选择消息配置设置。

背景技术

[0002] 已知的安全消息软件客户机，诸如运行在桌面计算机系统上的电子邮件软件应用，一次只能使用一组消息设置。例如通过使用鼠标、键盘或另一输入设备，配置应该出现在所有输出消息中的格式、字体和普通文本这些消息特性，以及诸如消息签名和加密之类的安全消息特性，可以建立消息设置。尽管一个用户可以建立多于一组的设置，但是只有先前选择为当前或缺省设置的一组，在任何时候控制在一个消息客户机上的消息操作。为了配置与在当前设置中建立的特性不同的一个输出消息的消息特性，必须覆盖当前的设置或必须选择另一组设置。这些操作趋于繁琐，特别当必须频繁地改变消息特性时，诸如当输出消息的收件人具有不同的消息通知能力时。

[0003] 美国专利第 6 157 954 号描述了用于改变电子名片的公钥的方法，其中，可以允许用户覆盖一个传真号码或电子邮件地址的自动选择。

[0004] 美国专利第 5 754 306 描述了一种提供允许信息有效地发送到电子邮件和传真传送的用户的电子地址本的方法和结构。

发明内容

[0005] 按照本发明的一个方面，提供了一种在消息客户机上选择消息设置的方法。该方法包括步骤：编写一个输出消息，将所述输出消息编址到一个消息接收者，确定是否已经为所述消息接收者建立特定的消息设置，以及如果已经建立所述消息接收者的特定消息设置，选择所述特定的消息设置以控制所述输出消息的消息特性。

[0006] 按照本发明的另一方面，还提供了一种选择消息设置的系统。该系统包括：被配置存储多个特定的消息设置的一个数据存储器，和一个消息客户机，被配置发送消息，每个消息具有消息特性和被编址到一个消息接收者，访问所述数据存储器以确定是否已为一个消息被编址到的消息接收者存储特定的消息设置，以及如果已经为所述消息接收者存储特定的消息设置，选择用于所述消息接收者的特定消息设置以控制所述消息的消息特性。

附图说明

[0007] 图 1 是示例消息系统的方框图。

[0008] 图 2 是图示在一个消息系统中安全电子邮件消息交换的方框图。

[0009] 图 3 是实现自动消息设置选择系统的无线移动通信设备的方框图。

[0010] 图 4 是图示支持消息设置选择的示例地址本项目的方框图。

[0011] 图 5 是图示在一个消息客户机上选择消息设置的方法的流程图。

[0012] 图 6 是无线移动通信设备的方框图。

具体实施方式

[0013] 消息设置可以控制用于非安全消息和安全消息的诸如消息格式和字体的一般消息特性。非安全消息例如包括通过互联网在消息客户机之间交换的传统的电子邮件消息。安全消息特性诸如消息签名和加密还可以通过建立消息设置被控制。安全消息可以用一个数字签名进行签名，加密或既签名又加密，并且也能由一个消息发送者或接收安全消息的消息客户机之间的中间系统用其它方法处理。例如，一个安全消息可以由消息发送者按照安全多用途互联网邮件扩展 (S/MIME) 签名、加密然后签名、或签名然后加密。一个安全消息在被签名和 / 或加密之前或之后能够被类似地编码、压缩或另外处理。这样，一组消息设置可以包括一般消息设置、安全消息设置或两者。

[0014] 一个消息客户机允许其运行所基于的系统接收并且还可能发送消息。消息客户机可以运行在一个计算机系统，一个手持设备或带有通信能力的任何其它系统或设备上。很多消息客户机还具有附加的非消息功能。

[0015] 图 1 是一个本发明可以在其中实现的示例消息系统的方框图。系统 10 包括广域网络 (WAN)12，其耦合到计算机系统 14，无线网络网关 16 和公司局域网络 (LAN)18。无线网络网关 16 还连接到配置一无线移动通信设备 22(移动设备) 运行其中的无线通信网络 20。

[0016] 计算机系统 14 可以是被配置与 WAN 12 例如互联网通信的桌上型或膝上型个人计算机 (PC)。PC 诸如计算机系统 14 通常通过互联网服务提供商 (ISP)，应用服务提供商 (ASP) 等访问互联网。

[0017] 公司 LAN 18 是基于互联网的消息客户机的例子。其通常位于安全防火墙 24 的后面。在公司 LAN 30 内，运行于防火墙 24 后面的计算机上的消息服务器 26，其作为主要接口用于公司在 LAN 18 内交换信息和通过 WAN 12 与其它外部消息客户机交换消息。两个所知的最普通的消息服务器 26 是 Microsoft™ Exchange 和 Lotus Domino™。这些服务器 26 通常与互联网邮件路由器一起使用以路由和传递邮件消息。消息服务器 26 还可以提供附加功能，诸如用于如日历、计划表、任务表、电子邮件和电子文档等的动态数据库存储。

[0018] 消息服务器 26 向耦合到 LAN 18 的公司联网的计算机系统 28 提供消息能力。典型的 LAN 18 包括多个计算机系统 28，每个计算机实现一消息客户机诸如 Microsoft Outlook™、Lotus Notes 等。在 LAN 18 内，消息由消息服务器 26 接收，分发给在接收的消息中编址的用户帐户的合适信箱，然后由用户通过与一个计算机系统 28 一起运行的消息客户机访问。

[0019] 无线网关 16 给无线网络 20 提供接口，通过该接口可与移动设备 22 交换消息。这些功能诸如移动设备 22 的编址、用于无线传输的编码或其它转换消息和任何其它需要的接口功能由无线网络网关 16 执行。可以配置无线网关 16 与多于一个无线网络 20 操作，在该情况下，无线网关 16 也可以确定用于定位一个给定的移动设备用户的最可能的网络，并且当用户在国家或网络之间漫游时可跟踪他们。

[0020] 任何访问 WAN 12 的计算机系统 14,28 可以通过无线网络网关 16 与移动设备 22 交换消息。或者，也可以实现专有无线网络网关诸如无线虚拟专有网络 (VPN) 路由器以给无线网络提供一个专有接口。例如，在 LAN 18 中实现的无线 VPN 可以通过无线网络 20 提

供一个从 LAN 18 到一个或多个移动设备 22 的专有接口。这种通过无线网络网关 16 和 / 或无线网络 20 到无线设备的专有接口通过提供与消息服务器 26 操作的消息前送或重定向系统还可以有效地扩展到 LAN 18 外部的实体。这样的一个重定向系统公开在美国专利 6,219,694 中，其通过引用包含在该申请中。在该类型的重定向系统中，由消息服务器 26 接收并且编址到具有移动设备 22 的用户的输入消息通过无线网络接口或者一个无线 VPN 路由器、无线网关 16 或其它接口发送到无线网络 20 及到用户移动设备 22。到在消息服务器 26 上的用户信箱的另一可选接口可以是无线应用协议 (WAP) 网关。在一个这种实现中，通过 WAP 网关，在消息服务器 26 上的用户信箱中的一列消息，和可能每个消息或每个消息的一部分被发送到移动设备 22。

[0021] 无线网络 20 通常通过基站和移动设备 22 之间的 RF 传输，传递消息到移动设备 22 和从移动设备 22 传送信息。无线网络 20 例如可以是 :(1) 数据中心型无线网络，(2) 语音中心型无线网络，或 (3) 能够通过相同的基础设施支持语音和数据通信的双模式网络。最近开发的无线网络包括 :(1) 码分多址 (CDMA) 网络，(2) 移动特别小组 (Groupe Special Mobile) 或全球移动通信系统 (GSM) 和通用分组无线业务 (GPRS) 网络，两者由 CEPT 标准委员会开发，和 (3) 当前在开发中的第三代 (3G) 网络，诸如全球演进的增强型数据比率 (EDGE) 和通用移动电信系统 (UMTS)。GPRS 是在现有 GSM 无线网络顶部上的数据覆盖，其在世界上的很多地方使用。

[0022] 数据中心网络的例子，包括 :(1)Mobitex™ 无线网络 (“Mobitex”)，和 (2)DataTAC™ 无线网络 (“DataTAC”)。已知的语音中心型数据网络的例子包括已经在北美和世界范围内使用近 10 年的个人通信系统 (PCS) 网络象 CDMA，GSM 和时分多址 (TDMA) 系统。

[0023] 移动设备 22 可以是数据通信设备，语音通信设备诸如带有数据通信功能的移动电话或能够进行语音、数据和其它类型通信的多模式设备。下面进一步详细描述一个示例的移动设备 22。

[0024] 也许当前使用的最普通类型的消息是电子邮件。在标准的电子邮件系统中，电子邮件消息由电子邮件发送者很可能通过消息服务器和 / 或服务提供者系统发送、然后经互联网路由到一个或多个消息接收者。电子邮件消息通常用明文发送，并且典型地使用简单邮件传输协议 (SMTP) 首标 (header) 和多用途互联网邮件扩展 (MIME) 主体部分定义电子邮件消息的格式。

[0025] 在近些年，安全消息技术已经得到发展以保护消息诸如电子邮件消息的内容和完整性。S/MIME 和 Pretty Good Privacy™(PGP™) 是两个公钥安全电子邮件消息协议，提供保护数据内容的加密，和保护消息的完整性和提供由消息接收者进行的发送者验证的签名。除了利用数字签名和可能的加密，安全消息还可以或者替换为被编码、压缩或其它处理。本领域技术人员将理解在此描述的技术决不限于上述安全消息方案，甚至安全消息。安全消息设置代表本发明的选择技术可应用到的一种类型的消息设置的示例。还应理解，这些技术可应用到不是电子邮件的其它类型的消息，例如包括即时消息和短消息服务 (SMS)。

[0026] 图 2 是图示在一个消息系统中安全电子邮件消息交换的方框图。该系统包括耦合到 WAN 32 的电子邮件发送者 30，和无线网关 34，该无线网关提供 WAN 32 和无线网络 36 之间的接口。调整移动设备 38 运行于无线网络 36 内。

[0027] 电子邮件发送者 30 可以是一个 PC 诸如图 1 中的系统 14 或 28，或一个移动设备，

消息客户机操作其上使得电子邮件消息被编辑和发送。WAN 32、无线网关 34、无线网络 36 和移动设备 38 实际上与图 1 中类似标记的组件相同。

[0028] 按照一个公钥签名方案，安全电子邮件消息发送者 30 典型地通过使用发送者的签名私钥对一个消息或一个消息摘要执行加密或某些其它转换操作，以按照签名算法产生一个数字签名，来签名一个消息。本领域技术人员将理解，尽管数字签名算法的完成需要只对消息发送者已知的密钥，某些签名算法的部分，诸如使用象安全散列算法 1(SHA-1) 或消息摘要算法 5(MD5) 产生消息部分的摘要，不涉及私钥。

[0029] 然后数字签名附加到输出消息上。此外，包括发送者签名公钥和用一个或多个数字签名捆绑到公钥的发送者标识信息的发送者数字证书，和可能的任何链式证书或与证书和任何链式证书相关的证书注销表 (CRL)，也可以包括在输出消息中。

[0030] 由电子邮件发送者 30 发送的示例安全电子邮件消息 40 包括包含发送者证书、证书链、CRL 和数字签名的组件 42 和签名的消息体 44。在 S/MIME 安全消息技术中，证书、CRL 和数字签名通常放在消息的开始如图 2 所示，并且消息体包括在文件附件中。由其它安全消息方案产生的消息可以以与所示的顺序不同的顺序放置消息组件或者包括附加的和 / 或不同的组件。例如，签名的消息 40 可以包括编址信息，诸如“To(到) :”和“From(来自) :”电子邮件地址，和其它首标信息。当从电子邮件发送者 30 发送安全电子邮件消息 40 时，它通过 WAN 32 路由到无线网关 34。尽管电子邮件发送者 30 直接发送消息 40 到无线网络网关 34，在一个可选的实现方案中，改为该消息传递到与移动设备 38 相关的计算机系统，然后通过相关计算机系统发送到移动设备 38。如上所述，在一个进一步可选的实施例中，消息可以经无线 VPN 路由器或其它接口通过无线网关 36 路由或重定向到移动设备 38。

[0031] 签名消息 40 的接收者，移动设备 38，使用发送者签名公钥 (在公钥签名方案中) 和对应于由消息发送者 30 使用的签名算法的签名验证算法，检验数字签名 42。如果安全消息 40 在被签名之后由发送者 30 加密或另外处理，那么在执行签名验证之前，移动设备 38 首先解密或对消息执行其它逆向处理操作。然而，如果在签名之前执行加密或处理，在签名验证之后执行逆向处理诸如解密。

[0032] 为了验证摘要签名，一般通过从附加到消息 40 的发送者证书 42 提取公钥，检索到发送者 30 的签名公钥，然后是使用检索到的公钥执行签名验证算法。图 2 所示的安全消息 40 包括发送者证书 42，从该证书能够提取发送者公钥。例如，当从来自发送者 30 的较早消息中提取公钥并且存储在接收者的密钥存储单元中的情况下，也可以从本地存储单元检索到发送者公钥。或者，可以从存储在本地存储单元中的发送者证书或从公钥服务器 (PKS) 检索到公钥。PKS 是通常与证书权威机关 (CA) 相关的服务器，从证书权威机关得到一个实体的证书包括实体的公钥。PKS 可以驻留在公司 LAN 诸如 18(图 1) 内，或 WAN 32 上、互联网或其它网络或系统上的任何地方，通过它消息接收者可以建立与 PKS 的通信。

[0033] 证书、证书链和 CRL 42 由一个接收者使用以保证发送者的证书是有效的，即，证书还没有被注销或过期并且是信任的。一个证书通常是一个证书链的一部分，包括用户的证书及验证用户的证书是可信的其它证书。例如，用于任何特定实体的证书典型地包括实体的公钥和用一个数字签名捆绑到公钥的标识信息。当前使用的几个类型的证书例如包括典型地用在 S/MIME 中的 X.509 证书，和具有略微不同的格式的 PGP 证书。在一个证书中的数字签名由该证书的发行者产生，并且能够如上所述由消息接收者检验。一个证书可以包

括一个过期时间或有效期，从该过期时间或有效期一个消息客户机可以确定是否该证书是否已经过期。还可以对每个证书检验其 CRL 以保证证书还没有被注销。

[0034] 如果在消息发送者的证书中的数字签名被验证，该证书还没有过期或没有被注销并且证书的发行者被消息接收者信任，那么消息的数字签名被该消息的接收者信任。如果证书的发行者不被信任，那么该消息接收者可以通过证书链跟踪一个证书路径，以验证在该链中的每个证书由其发行者签名，其证书是在该证书链中的下一个，直到从由接收者信任的源诸如从一个大 PKS 发现由一个根证书签名的证书。一旦发现一个根证书，然后能够信任一个签名，因为发送者和接收者信任根证书的源。例如在 S/MIME 中使用该信任机制。尽管其它消息方案例如包括 PGP，可以使用不同的信任机制，本发明决不依赖于特定的签名方案或信任机制。

[0035] 在电子邮件发送者 30 处，安全消息特性，在消息 40 中的消息签名，可以通过消息设置（或者缺省的消息设置或者当前选择的由用户建立的消息设置组），或者通过覆盖 (over-ride) 缺省或当前的消息设置，得到控制。在已知的系统中，无论何时具有与在消息设置的当前组中指定的那些不同的消息特性的消息从一个消息客户机发送，必须选择不同组的消息设置或必须覆盖当前设置。

[0036] 频繁的消息设置改变不仅繁琐和耗时，而且易于出错。例如，可以配置某些安全消息客户机以与其它消息客户机交换安全或非安全消息。然而，如上所述，已知的消息客户机只允许在任何时候仅单个消息设置组是激活的。因此，当一个安全消息客户机与非安全消息客户机相对经常地交换消息时，安全消息客户机的用户可以通常只选择一般消息设置作为缺省设置，以保证发送的消息可以由非安全消息客户机处理。然后，当一个安全消息要发送到安全消息客户机时，选择不同组的设置，或覆盖当前一般消息设置，以便发送一个安全消息。当用户忘记选择安全消息设置或覆盖一般消息设置时，打算安全发送的消息以明文发送。当这样一个消息包含保密或其它敏感信息时，这种情况是特别不希望的。同样，当安全消息设置用作缺省设置，并且当消息要发送到一个非安全消息客户机时不被覆盖，非安全消息客户机将不能够处理安全消息，并且消息发送者必须以非安全格式重发送该消息。然而，在大多数情况下，在接收者告诉发送者消息不能被处理之前，发送者不知道接收者不能处理一个接收的消息。这样，通常不能及时地执行重发送，当消息包括时间关键的信息时这是一个严重的问题。

[0037] 图 3 是实现自动消息设置选择系统的无线移动通信设备的方框图。

[0038] 移动设备 38 包括存储器 52，消息客户机 60，用户接口 (UI)62 和无线收发机 64。

[0039] 存储器 52 是一个其它设备组件和系统可以写入数据的可写存储器诸如 RAM，并且最好包括 :用于证书存储单元 54 的存储区域，存储消息联系信息的地址本 56，存储与移动设备 38 上的软件应用相关的数据的应用数据存储区 58，和存储消息设置的设置存储单元 59。数据存储单元 54，56，58 和 59 是可以在移动设备 38 上的存储器 52 中实现的存储单元的示例。存储器 52 还可以由除了图 3 中示出的那些之外的其它设备系统使用，并且用于存储其它类型的数据。

[0040] 消息系统 60 连接到无线收发机 66，并且由此能够通过一个无线网络通信。

[0041] UI 64 可以包括这样一些 UI 组件，如键盘或小键盘，显示器，或从移动设备 38 的用户接收输入或提供输出给移动设备 38 的用户的其它组件，移动设备 38 典型地包括多于一

个 UI，并且 UI 64 由此代表一个或多个用户接口。

[0042] 消息客户机 60 存储接收的证书到证书存储单元 54，并且还从证书存储单元 54 检索所存储的证书。证书通常以它们被接收的格式存储在证书存储器 54 中，但可选地可以在写到存储单元 54 之前被解析或另外翻译成一种存储格式。证书可以用安全消息接收，通过无线收发机 64 从证书源诸如 PKS 请求，或通过一个通信接口诸如串行口、通用串行总线 (USB) 口、红外数据协会 (IrDA) 口、802.11 模块或 Bluetooth™ 模块，从一个类似装备的外部系统例如 PC，加载到移动设备 38 上。本领域技术人员将理解“802.11”和“Bluetooth(蓝牙)”指从电气电子工程师协会得到的、分别涉及无线 LAN 和无线个人局域网络的规范组。从进一步的源的证书装载可以通过这些其它接口诸如智能读取器或安全数字 (SD) 口得到支持。如上所述，可需要证书中的公钥用于发送或接收安全消息。

[0043] 地址本 56 存储联系信息，至少某些信息由消息客户机 60 在消息操作中使用。在地址本 56 中的项目典型地最常用于编址要从消息客户机发送的消息。当从地址本项目存在于地址本 56 中的发送者接收的一个消息显示给移动设备 38 的用户时，地址本项目还用于用个人或熟悉的名字替换编址信息诸如电子邮件地址。当从没有在地址本 56 中存在项目的发送者接收一个消息时，或者人工地例如通过使用 UI 62 输入个人信息或从一个接收的消息选择一个地址，或自动地诸如通过配置消息客户机 60 以存储联系信息，能够典型地创建一个地址本项目。当一个新证书存储到证书存储器 54 时，联系信息还能够被提取和存储在地址本 56 中，正如在标题为“证书信息存储系统和方法”、转让给本申请的受让人并且通过引用包含在此的共同待审的国际专利申请 PCT/CA03/00406 中描述的。

[0044] 设置存储单元 59 存储控制从移动设备 38 发送的输出消息的特性的消息设置。尽管在已知的系统中，在任何时候，仅有一个先前选择的设置组是激活的，设置存储单元 59 可存储多于一组的消息设置。一个典型的消息客户机确定哪一组消息设置被先前选择，并且使用该设置控制一个输出消息的特性。

[0045] 然而，消息客户机 60 被配置为每个输出消息提供消息设置选择。例如对于每个地址本项目可以启动该特性。图 4 是展示支持消息设置选择的示例地址本项目的方框图。

[0046] 地址本项目 70 包括多个联系信息字段用于：名 72，姓 74，电子邮件地址 76，邮件地址 78，其它联系信息 80，和消息设置 82。一个实际地址本项目可包括比图 4 示出的那些字段更多、更少或不同的字段，并且在地址本项目中的某些字段可能是空白的。例如，如果其它字段是空白的，消息客户机 60 可只需要一个电子邮件地址 76 以便使用一个地址本项目 70 以编址一个输出消息并且由此可以使用一个地址本项目 70。消息客户机 60 或可选的其它设备组件，可以被配置使用在项目 70 中的其它字段（当它们被填充时）。在一个未完成的地址本项目中的一个或多个字段的信息的缺少最好不排除使用在地址本项目中其它填充的字段的使用。

[0047] 从图 4 中的标志将明显知道字段 72 到 78 的内容。字段 80 可包括一个相关联系的诸如电话号码、传真号等的这些其它联系信息。消息设置字段 82 最好包括要用于控制发送到项目 70 对应的联系的任何消息特性的一组消息设置。消息设置最好可由移动设备 38 的用户，例如使用诸如键盘和消息客户机 60 的设置功能之类的 UI 62 进行人工配置。可替换为配置地址本项目允许对其进行编辑以建立或改变消息设置。一旦为一个联系建立消息设置，消息设置存储在消息设置字段 82 中。或者，如下面进一步详细描述的，消息设置可存

储在其它数据存储单元或存储器中，并且在设置字段 82 中存储用于访问所存储的消息设置的一个存储指针或其它标识符。

[0048] 当地址本 56 包括具有消息设置字段 82 的项目时，为基于消息收件人要由消息客户机 60 发送的每个消息，选择消息设置。

[0049] 在操作中，使用 UI 62 诸如键盘和一个显示器在移动设备 38 上编写一个消息。通常配置消息客户机 60 发送新消息和答复消息，并且也前送接收的消息。当从地址本 56 选择一个输出消息的接收者时，在编写消息之前或之后或可能在编写消息的同时，消息客户机 60 访问在地址本项目 70 中的消息设置字段 82，以确定应该用于控制输出消息的消息特性的消息设置。

[0050] 消息设置字段 82 可包含用于要编址到地址本项目 70 所对应的特定联系的消息的实际消息设置，或可能指向已经建立并且存储在存储器 52 中例如在设置存储单元 59 中的一组消息设置的标识符或指针。如果消息设置字段 82 包括一个标识符或指针，那么消息客户机 60 访问设置存储器 59 以选择相应的设置控制消息特性。这样一个标识符或指针的使用减少了当一组消息设置用于地址本 56 中的几个联系时需要的整个存储器存储空间。在该情况下，实际设置只在设置存储器 59 中存储一次，然后每次在地址本项目中发现一个相应的标识符或指针时访问和使用。例如，对于具有与一个特定域相关的电子邮件地址的每个联系，用户可能希望建立要使用的共同消息设置。用户可能例如在设置存储器 59 中建立共同消息设置，并且在具有与该域相关的电子邮件地址的每个地址本项目中包括一个指针或消息设置名。例如在该特定例子中，替换为，可配置消息客户机 60 以确定输出消息的接收者电子邮件地址的域名，然后访问设置存储器 59 以确定是否为该域名已经建立共同消息设置。

[0051] 如上所述，消息设置可以控制一般消息特性诸如格式和字体，以及安全消息特性诸如签名和加密。当所选择的消息设置指示要发送一个安全消息时，消息客户机 60 检索到任何需要的密钥并且按照在选择的消息设置中指定的，处理输出消息。例如，当在消息设置字段 82 中包含的或标识的所选择的消息设置指定要发送一个签名然后加密的 S/MIME 消息时，那么消息客户机 60 可以使用其自己的私钥为该消息产生一个数字签名，产生一个会话密钥，并且使用该会话密钥加密消息和数字签名，从证书存储器 54 检索到消息接收者的公钥或证书，并且用该公钥加密会话密钥。

[0052] 该用于消息设置的选择的技术允许消息客户机 60 的用户为一个项目已经创建并且存储在地址本 56 中的每个联系，建立优选的消息设置。每次一个消息发送到这样的一个联系，选择和使用优选的消息设置，以便用户不需要人工覆盖缺省的或当前激活的消息设置。一旦选择一个消息的消息设置，消息客户机最好显示一个设置指示符，以便消息客户机的用户能够快速确定消息将如何发送。一个设置指示符可以是一个消息设置名，消息类型诸如“签名的 S/MIME”，或某些其它指示符，从这些其它指示符所选择的消息设置对用户是明显的。对于一个联系，基于消息客户机 60 的用户和该联系之间的关系，通过例如使用 UI 62 人工配置，可以建立消息设置。例如，如果对于与个人联系消息交换消息安全不重要，用户可以为个人联系仅建立一般消息特性的消息设置。同一个用户可以建立用于业务联系的一般和安全二种消息特性的消息设置。例如，当与在同一公司内的内部业务联系的消息交换已经是安全的时，当一个加密方案用于公司用户之间的所有通信时，或当所有用户工作

站例如操作在防火墙后面的网络内时，用户可以建立消息设置指定输出消息应该只使用 S/MIME 签名。用户还可以建立另一组消息设置用于外部业务联系指定到任何这些联系的消息应该使用例如 PGP 被加密和签名。还可以使用其它准则，确定为在地址本 56 中的任何联系建立特定的消息设置。

[0053] 很多消息客户机允许用户创建包括多联系的分发表。最好为这些分发表建立与在表中的每个联系的消息设置分开的消息设置。当在一个输出消息中直接编址一个单联系时，与该联系相关的消息设置被选择和用于控制输出消息的消息特性。如果相同的联系出现在用于编址另一输出消息的分发表中时，那么选择用于该分发表的消息设置。这种分发表消息设置的使用避免了表中联系的冲突消息设置之间的争用。当建立分发表消息设置时，由用户有效地解决这些设置冲突。在基本分发表设置实现的另一增强方案中，配置消息客户机 60 以识别任何联系和该联系添加到的分发表之间的冲突消息设置，以警告用户该冲突。然后，用户能够建立合适的分发表消息设置，从分发表中丢掉该联系，编辑该联系的消息设置，或采取某些行动解决冲突。

[0054] 当一个输出消息被单独编址到多个接收者时，通过配置消息客户机 60 警告用户这些接收者的任何冲突的消息设置，是否这些接收者是具有各消息设置的多重联系，具有分发表消息设置的多分发表，或联系和分发表的某些组合，也可以实现类似的消息设置冲突解决方案。然后用户选择应该应用到该输出消息的消息设置。消息客户机 60 最好允许用户指定与每个接收者相关的消息设置应该应用到该输出消息，在该情况下，消息客户机 60 按照接收者消息设置产生具有不同消息特性的输出消息的不同版本。当分发表消息设置不被启动或建立时，那么该特性还提供了当一个编写的消息被编址到表中，而不是当创建该表时的分发表中的联系之间的消息设置冲突的解决。

[0055] 如上所述的特定联系消息设置、特定小组消息设置和 / 或特定分发表消息设置的使用最好不排除缺省消息设置的使用。例如，当没有消息设置已经建立用于一个或多个输出消息的接收者时，诸如当人工输入一个新接收者电子邮件地址时，或一个用户答复从一个没有地址本项目存在的联系所接收的消息时，用户可以建立某些消息设置，以控制消息特性。

[0056] 即使当已经建立特定的消息设置时，当缺省和特定的消息设置涉及不同的消息特性时，也可以用于缺省的消息设置。由此，一个用户可以用缺省的设置控制某些消息特性和用特定的设置控制其它特性。在用于任何消息特性的缺省和特定消息设置之间的冲突的情况下，特定设置最好优先，尽管如上所述消息设置冲突矛盾解决方案可以被替换使用。

[0057] 很多消息客户机 60 允许用户以不同的方法在输出消息中设置接收者地址。当一个输出消息例如是一个答复消息时，如上所述可以从地址本 56 中选择接收者地址，但是还可以通过用户使用 UI 62 诸如一个键盘或小键盘输入地址，或由消息客户机 60 插入地址。当从一个地址本 56 选择一个接收者地址时的消息设置选择已经如上描述。然而，当一个地址由消息客户机 60 人工输入或插入时，消息客户机 60 最好访问地址本 56 和可能的设置存储单元 59 以确定是否已经建立用于该地址或类似地址的消息设置。如果发现包括该地址的一个地址本项目，那么对于该输出消息选择在地址本项目中指定或标识的消息设置。当对于在电子邮件地址中的域名、公司或分部名或与地址相关的某些其它标识符，消息设置已经存储到设置存储器 56 时，然后选择那些设置。这样，消息设置选择不需要依赖于通过

来自地址本 56 的接收者地址选择编址一个输出消息。

[0058] 消息设置选择很可能不防止用户覆盖当前选择的消息设置。在某些情况下，用户可能希望覆盖缺省或选择的消息设置。例如，如果个人消息要发送到一个外部业务联系，对于该外部业务联系已经建立消息设置指定对该联系的输出消息应该被签名和加密，那么用户可能希望覆盖该消息设置发送一个非安全的消息。类似地，当对于输出消息的接收者，没有已经建立特定的消息设置，用户可能覆盖缺省的消息设置以控制输出消息的消息特性。

[0059] 可配置消息客户机 60 以检测何时缺省或特定的消息设置被覆盖，并且提醒用户决定是否存储的消息设置应该被更新以反映产生的新消息设置。如果特定的消息设置被覆盖，那么可更新特定的消息设置。当缺省的消息设置被覆盖时，然后如果特定的消息设置存在，可以使用产生的消息设置更新特定的消息设置，或如果特定的消息设置不存在，建立新的特定的消息设置，用于消息设置被覆盖的输出消息接收者。

[0060] 图 5 是图示在消息客户机上选择消息设置的方法的流程图。

[0061] 当编写一个消息时在步骤 92 开始该方法。当在步骤 94，消息被编址到一个或多个接收者时，消息客户机确定是否对于接收者已经建立特定的设置。如果这样，那么在步骤 98 选择特定的设置，并且可选地显示。否则，在步骤 100 选择缺省的设置（如果有）。任何上述的方案可以在步骤 96 使用以确定是否已经建立特定的设置，包括当从地址本选择一个接收者地址时检验地址本项目，或当人工输入或由消息客户机插入一个接收者地址时搜索一个地址本和设置存储单元。

[0062] 当在输出消息中编址多于一个接收者时，对于每个接收者重复步骤 96 到 100，并且在步骤 102 检测消息设置冲突。然后通过例如警告用户所述冲突，和提示用户选择应该应用哪个消息设置，在步骤 104 解决检测的设置冲突。

[0063] 如果由用户覆盖任何特定的设置，正如在步骤 106 确定的，对于输出消息无论解决一个设置冲突还是改变消息设置，可以在步骤 108 更新现有缺省或特定的消息设置，或可以创建新的特定的消息设置。如果没有设置已经被覆盖或消息设置被创建或如果需要被更新，方法进行到步骤 110，在此在消息设置的控制下准备一个消息并且发送到任何编址的接收者。当输出消息被编址到多于一个接收者，并且不同的消息设置用于控制输出消息的消息特性时，在步骤 110，准备和发送多于一个消息，每个消息具有不同的消息特性。

[0064] 图 6 是无线移动通信设备的方框图。移动设备 600 最好是至少具有语音和数据通信能力的双向通信设备。移动设备最好具有与互联网上的其它计算机系统通信的能力。根据移动设备提供的功能，移动设备可称为数据消息设备、双向寻呼机、带有数据消息能力的蜂窝电话、无线互联网设备或数据通信设备（带有或不带有电话功能）。

[0065] 双模式设备 600 包括收发器 611、微处理器 638、显示器 622、非易失存储器 624、RAM 626、辅助输入 / 输出 (I/O) 设备 628、串行口 630、键盘 632、扬声器 634、麦克风 636 和短距离无线通信子系统 640，并且还可以包括其它设备子系统 642。收发器 611 最好包括发送和接收天线 616、618，接收器 (Rx)612，发送器 (Tx)614，一个或多个本地振荡器 (LO)613 和数字信号处理器 (DSP)620。在非易失存储器 624 内，移动设备 600 包括多个可由微处理器 638（和 / 或 DSP 620）执行的软件模块 624A-624N，包括语音通信模块 624A、数据通信模块 624B 和多个用于执行多个其它功能的其它操作模块 624N。

[0066] 如上所述，移动设备 600 最好是具有语音和数据通信能力的双向通信设备。于是，

例如移动设备 600 可以在语音网络诸如任何模拟或数字蜂窝网络上通信，也可以在数据网络上通信。语音和数据网络在图 6 中由通信塔 619 表示。这些语音和数据网络可以是使用分离的基础设施诸如基站、网络控制器等的分离的通信网络，或它们可以集成为一个单个的无线网络。

[0067] 通信子系统 611 用于与网络 619 的通信。DSP 620 用于发送信号给发送器 614 和从接收器 612 接收通信信号，并且也可以与发送器 614 和接收器 612 交换控制信息。如果语音和数据通信发生在单个频率上，或近间隔的频率组上，那么单个 LO 613 可以与发送器 614 和接收器 612 一起使用。或者，如果不同频率用于语音和数据通信，那么能够使用多个 LO 产生对应于网络 619 的多个频率。尽管在图 6 中示出了两个天线 616、618，移动设备 600 能够使用单天线结构。包括语音和数据信息二者的信息经 DSP 620 和微处理器 638 之间的链路与通信模块 611 交互通信。

[0068] 通信子系统 611 的详细设计诸如频带、分量选择和功率电平等取决于移动设备 600 将运行其中的通信网络 619。例如，打算运行于北美市场的移动设备 600 可包括通信子系统 611，该子系统设计运行于 Mobitex 或 DataTAC 移动数据通信网络，并且也设计运行于各种语音通信网络诸如 AMPS，TDMA，CDMA，PCS 等，而打算用在欧洲的移动设备 600 可被配置运行于 GPRS 数据通信网络和 GSM 语音通信网络。其它类型的数据和语音网络，分离的和集成的，也可以用于移动设备 600。

[0069] 取决于网络 619 的类型，对于双模式移动设备 600 的访问需要也可改变。例如，在 Mobitex 和 DataTAC 数据网络中，移动设备使用与每个设备相关的唯一标识号注册在网络上。然而在 GPRS 数据网络中，网络访问与移动设备 600 的订户或用户相关。GPRS 设备典型地需要用户标识模块（“SIM”），需要它以便移动设备 500 运行于 GPRS 网络上。没有 SIM，本地或非网络通信功能（如果有）可能是可运行的，但是移动设备 600 将不能执行涉及在网络 619 上通信的任何功能，除了任何合法需要的操作诸如‘911’紧急呼叫之外。

[0070] 在已经完成任何需要的网络注册或激活程序之后，移动设备 600 可经网络 619 发送和接收通信信号，最好包括语音和数据两种信号。由天线 616 从通信网络 619 接收的信号被路由到接收器 612，该接收器设有信号放大、频率下转换、滤波、信道选择和模拟到数字转换的操作。接收信号的模拟到数字转换允许更复杂的通信功能，包括例如使用 DSP 620 执行的数字解调和解码。以类似方式，由 DSP 620 处理将发送到网络 619 的信号，例如调制和编码信号，然后所处理的信号提供给发送器 614 用于数字模拟转换、频率上变换、滤波、放大和经天线 618 发送给通信网络 619。尽管图 6 中所示的单个接收器 611 用于语音和数据二种通信，移动设备 611 能够包括两个不同的收发器，诸如用于发送和接收语音信号的第一收发器和用于发送和接收数据信号的第二收发器，或用于在不同的操作频段操作的多个收发器。

[0071] 除了处理通信信号之外，DSP 620 还可设有接收器和发送器控制。例如，应用到接收器 612 和发送器 614 中的通信信号的增益电平也可以通过在 DSP 620 中实现的自动增益控制算法得到自适应控制。其它收发器控制算法也能够在 DSP 620 中实现以便提供更复杂的收发器 611 的控制。

[0072] 微处理器 638 最好管理和控制移动设备 600 的整个操作。这里可以使用很多类型的微处理器或微控制器，或者，可选地，能够使用单个 DSP 620 执行微处理器 638 的功能。

低级通信功能包括至少数据和语音通信通过收发器 611 中的 DSP 620 执行。其它高级通信功能诸如语音通信应用 624A 和数据通信应用 624B 也可以存储在快闪存储器 624 中用于由微处理器 638 执行。例如，语音通信模块 624A 可提供高级用户接口，该接口可操作经网络 619 在移动设备 600 和多个其它语音设备之间发送和接收语音呼叫。类似地，数据通信模块 624B 可提供高级用户接口，可操作用于经网络 619 在移动设备 600 和多个其它数据设备之间发送和接收数据诸如电子邮件消息、文件、组织者信息、短文本消息等。在移动设备 600 上，消息客户机可以与数据通信模块 624B 一起运行，以实现上述的技术。

[0073] 微处理器 638 还与其它设备子系统交互，这些子系统诸如是显示器 622、快闪存储器 624、RAM 526、辅助输入 / 输出 (I/O) 子系统 628、串行口 630、键盘 632、扬声器 634、麦克风 636、短距离通信子系统 640 和总的表示为 642 的任何其它设备子系统。组件 628，632，634 和 636 是能够作为 UI 62(图 3) 提供的子系统类型的例子。模块 624A-N 由微处理器 638 执行，并且可提供用户和移动设备 600 之间的高级接口。该接口典型包括通过显示器 622 提供的图形组件和通过辅助 I/O 628、键盘 632、扬声器 634 或麦克风 636 提供的输入 / 输出组件。

[0074] 图 6 中所示的某些子系统执行与通信相关的功能，而其它子系统可提供“驻留”或设备内置功能。明显的是，某些子系统诸如键盘 632 和显示器 622 可以用于通信相关功能诸如输入文本消息用于经数据通信网络传送，以及设备驻留功能诸如计算器或任务列表或其它 PDA 型功能。

[0075] 微处理器 638 使用的操作系统软件最好存储在永久存储器诸如非易失存储器 624 中。正如本领域技术人员将理解的，非易失存储器 624 例如可以实现为快闪存储器设备，电池备用 RAM 或非易失存储器芯片和相关控制器。当没电时提供数据记忆能力的其它合适的组件或配置，对于本领域技术人员来说是显而易见的。除了操作系统和通信模块 624A-N，非易失存储器 624 还能包括用于存储数据的文件系统。最好还在非易失存储器 624 中提供存储区域以存储公钥，私钥，和安全消息需要的其它信息。操作系统、特定的设备应用或模块或其部分，可以临时装进易失存储器诸如 RAM 626 用于较快操作。此外，接收的通信信号在永久将它们写到位于非易失存储器 624 中的文件系统之前也可以临时存储到 RAM 626。

[0076] 可以装到双模式设备 600 的示例应用模块 624N 是个人信息管理器 (PIM) 应用，其提供 PDA 功能诸如日历事件、约会和任务项。该模块 624N 还能与语音通信模块 624A 交互用于管理电话呼叫，语音信件等，也可以与数据通信模块 624B 交互，用于管理电子邮件通信和其它数据传输。或者，语音通信模块 624A 和数据通信模块 624B 的所有功能可以集成到 PIM 模块中。

[0077] 非易失存储器 624 最好提供文件系统以方便在该设备上 PIM 数据项的存储。PIM 应用最好包括经无线网络 619 或者通过其自身或者结合语音和数据通信模块 624A 和 624B 发送和接收数据项的能力。PIM 数据项通过无线网络 619 最好与所存储的或与主机算机系统相关的一组相应的数据项无缝集成、同步和更新，由此为与特定的用户相关的数据项建立镜像系统。

[0078] 通过将移动设备 600 放置在连接移动设备 600 的串行口 630 到主系统的串行口的一个接口底座中，移动设备 600 还能与计算机系统人工同步。串行口 630 还能用于使用户能够通过外部设备或软件应用程序建立消息设置，以下载其它应用模块 624N 用于安装，并

且加载证书、密钥和其它信息到设备上。可以使用该有线下载路径，以将加密密钥加载到设备上，这个是比通过无线网络 619 交换加密信息更安全的方法。

[0079] 附加的应用模块 624N 可通过网络 619、通过辅助 I/O 子系统 628、通过串行口 630、通过短距离通信子系统 640 或通过任何其它合适的子系统 642 被加载到移动设备 600 上，并且由用户安装在快闪存储器 624 或 RAM 626 中。这种在应用安装方面的灵活性增加了移动设备 600 的功能，并且能够提供增强的设备内置功能、通信相关功能或二者。例如，安全通信应用可以使得电子商务功能和其它财务交易能够使用移动设备 600 执行。

[0080] 当移动设备 600 运行于数据通信模式时，接收的信号诸如文本消息或网页下载由收发器 611 处理并且提供给微处理器 638，其最好进一步处理接收的信号用于输出到显示器 622，或可选地输出到辅助 I/O 设备 628。移动设备 600 的用户也可以使用键盘 632 编辑数据项诸如电子邮件信息，键盘 632 最好是 QWERTY 型的完整字母数字键盘布局，尽管也能使用其它类型的完整字母数字键盘诸如已知的 DVORAK 型。对移动设备 600 的用户输入用多个辅助 I/O 设备 628 得到进一步增强，该辅助设备可包括指轮输入设备、触板、各种开关、摇杆输入开关等。然后用户输入的编辑的数据项可经收发器 611 在通信网络 619 上被发送。

[0081] 当移动设备 600 操作在语音通信模式中时，移动设备 600 的整个操作基本上类似于数据模式，除了接收的信号最好输出到扬声器 634 和用于发送的语音信号由麦克风 636 产生之外。可选的语音或音频 I/O 子系统诸如语音消息记录子系统也可以在移动设备 600 上实现。尽管语音或音频信号输出最好基本通过扬声器 634 完成，也能使用显示器 622 提供呼叫方标识的指示、语音呼叫的持续时间或其它语音呼叫相关的功能。例如，微处理器 638 结合语音通信模块 624A 和操作系统软件可以检测接收的语音呼叫的呼叫方标识信息并且将其显示在显示器 622 上。

[0082] 短距离通信子系统 640 可以包括上述的任何证书加载接口，例如包括红外设备，802.11 模块，蓝牙模块，USB 口，SD 口和智能卡读取器。尽管上述描述为证书加载接口，这些接口还普遍用于传送其它类型的数据。

[0083] 上述描述涉及本发明的一个例子。对于本领域技术人员很多变体将是明显的，并且无论是否被明显地描述，这些变体是在所描述的和权利要求所要求的本发明的范围内。

[0084] 例如，还可以配置消息设置选择系统或方法存储和访问不是消息设置的信息。当一个消息客户机被启动用于发送和接收消息时，接收的消息的特性提供发送者使用的消息客户能力的指示。如果从一个特定的发送者接收到一个签名和加密的 S/MIME 消息，那么很可能发送者的消息客户机支持所有的 S/MIME 变体。这样，除了消息设置，在一个地址本项目中、设置存储单元或分离的消息能力存储单元中存储消息能力可能是有用的。然后，所存储的消息能力可以被访问和显示给用户，例如当识别一个设置冲突时。当一个消息接收者的特定消息设置不同于同一消息的另一消息接收者的特定消息设置时，存储的消息能力提供关于该接收者是否可能支持其它接收者的消息设置的指示。能力信息允许用户针对具有设置冲突的这些消息如何能够或应该被发送，进行明智的决定。消息能力的另一可能的应用是确定是否所建立的用于一个联系的特定消息设置和似乎由该联系支持的消息设置的类型之间存在任何矛盾。当从没有消息设置已经被建立或只建立一般的消息设置的一个联系，接收到一个安全消息时，能够提示用户在地址本项目中设置该联系的安全消息设置。

[0085] 此外，尽管一个无线移动通信设备在图 6 中示出，并且被描述为一个可能的消息

客户机，本发明还可以在其它消息客户机中实现，包括操作于桌面、膝上和联网的计算机系统或结合它们操作的那些。

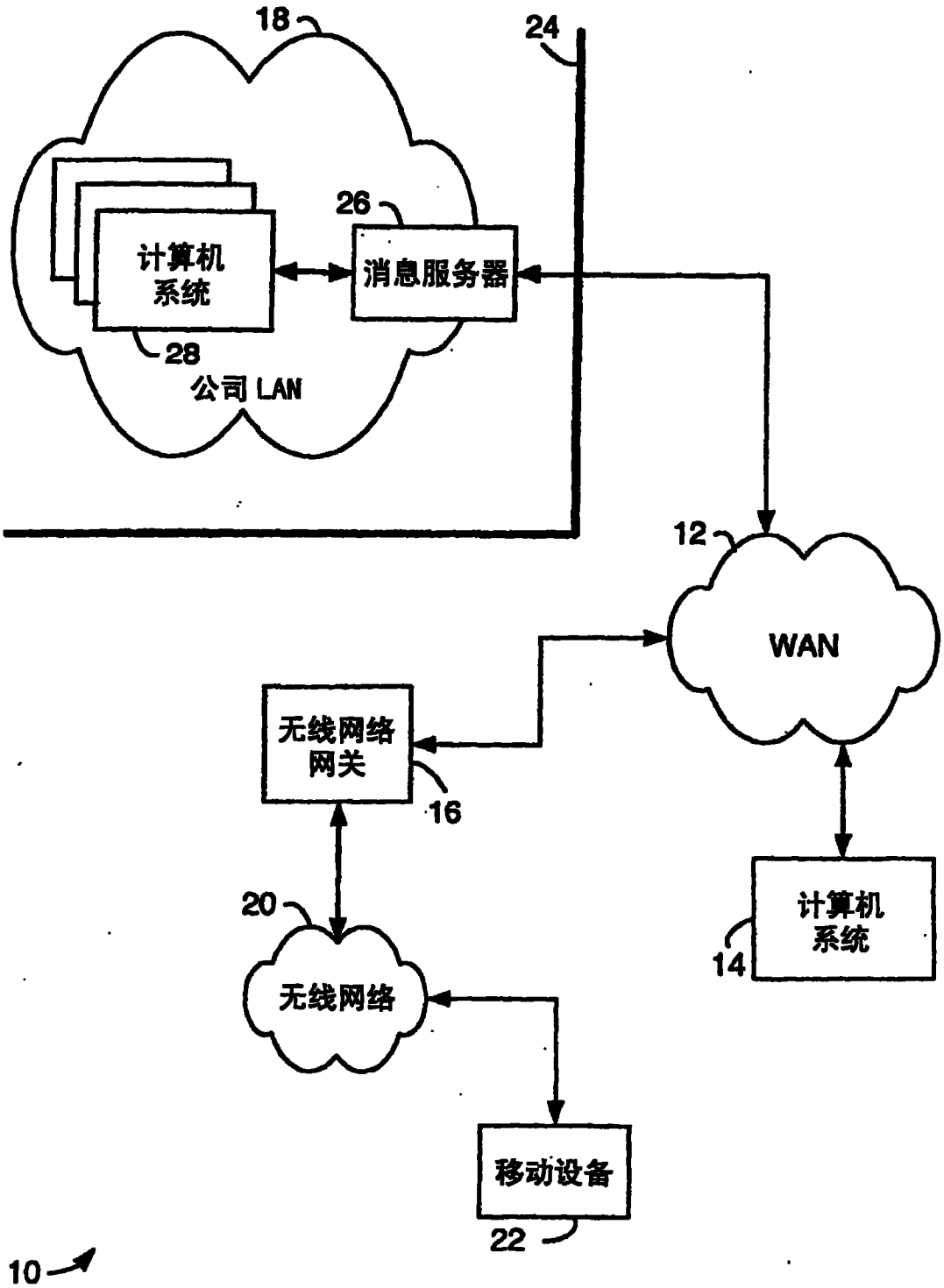

18
24
26
计算机系统
消息服务器
28
公司 LAN
12
WAN
无线网络网关
16
20
无线网络
计算机系统
14
移动设备
22
10

图 1

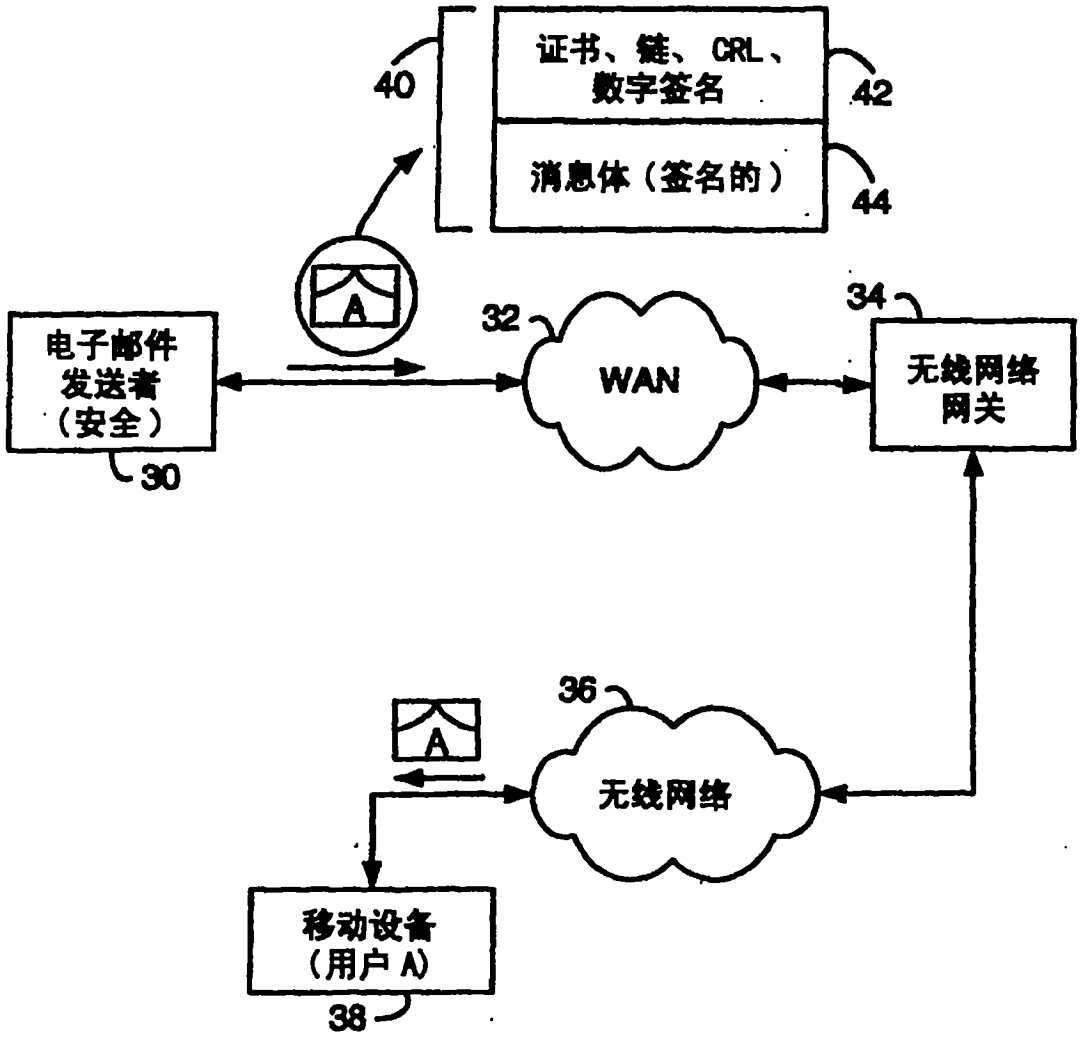

证书、链、CRL、
数字签名
42
40
消息体（签名的）
44
A
32
WAN
34
无线网络
网关
电子邮件
发送者
（安全）
30
36
A
无线网络
移动设备
（用户 A）
38

图 2

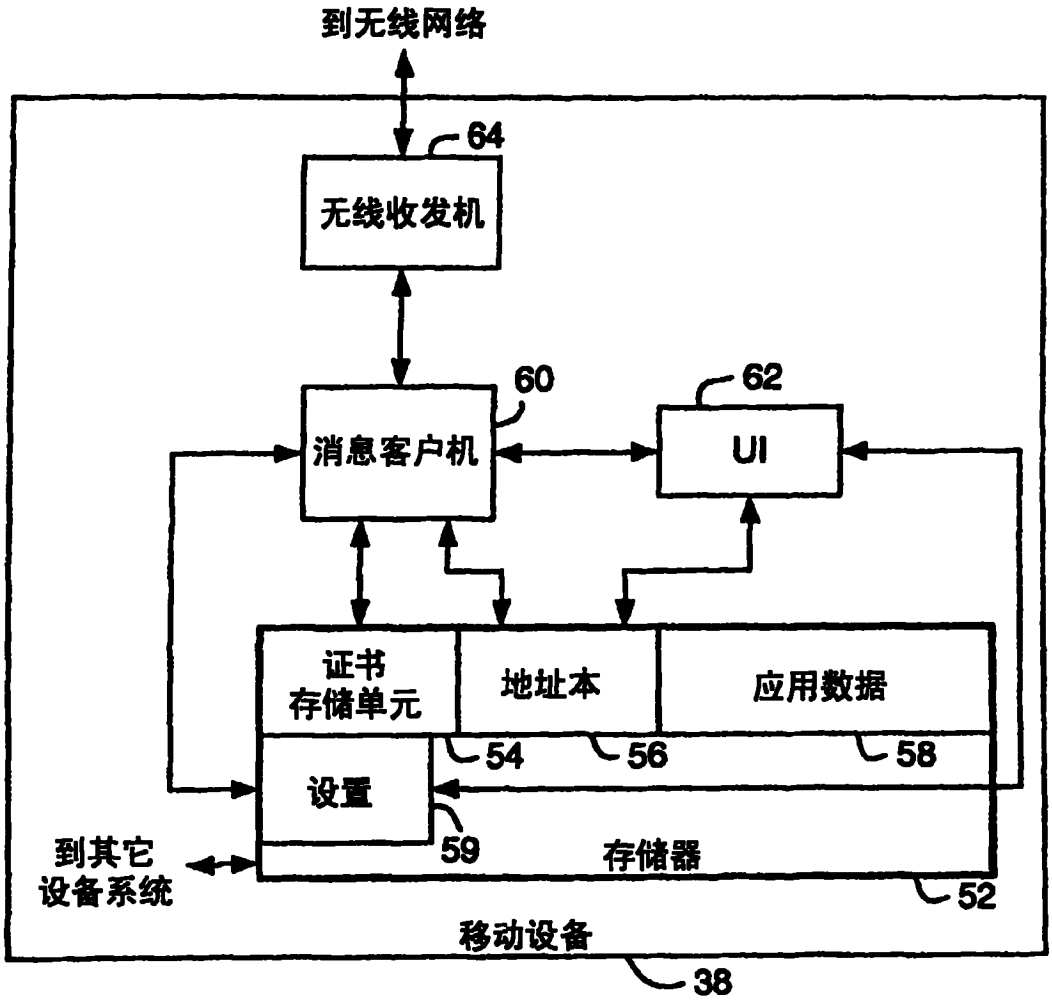

到无线网络
64
无线收发机
60
消息客户机
62
UI
证书
存储单元
地址本
应用数据
54
56
58
设置
59
存储器
52
到其它
设备系统
移动设备
38

图 3

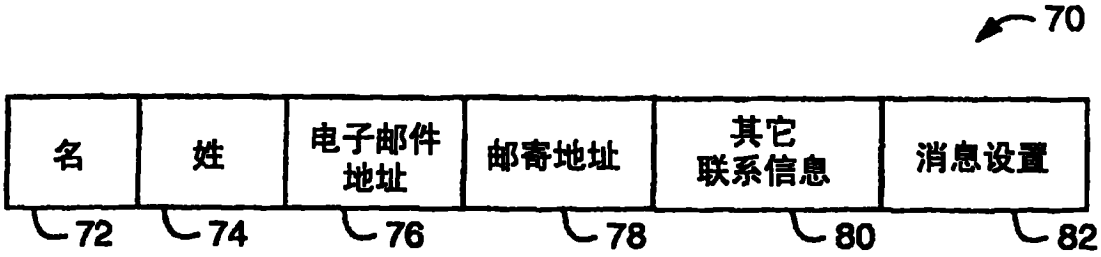

70
名
姓
电子邮件
地址
邮寄地址
其它
联系信息
消息设置
72
74
76
78
80
82

图 4

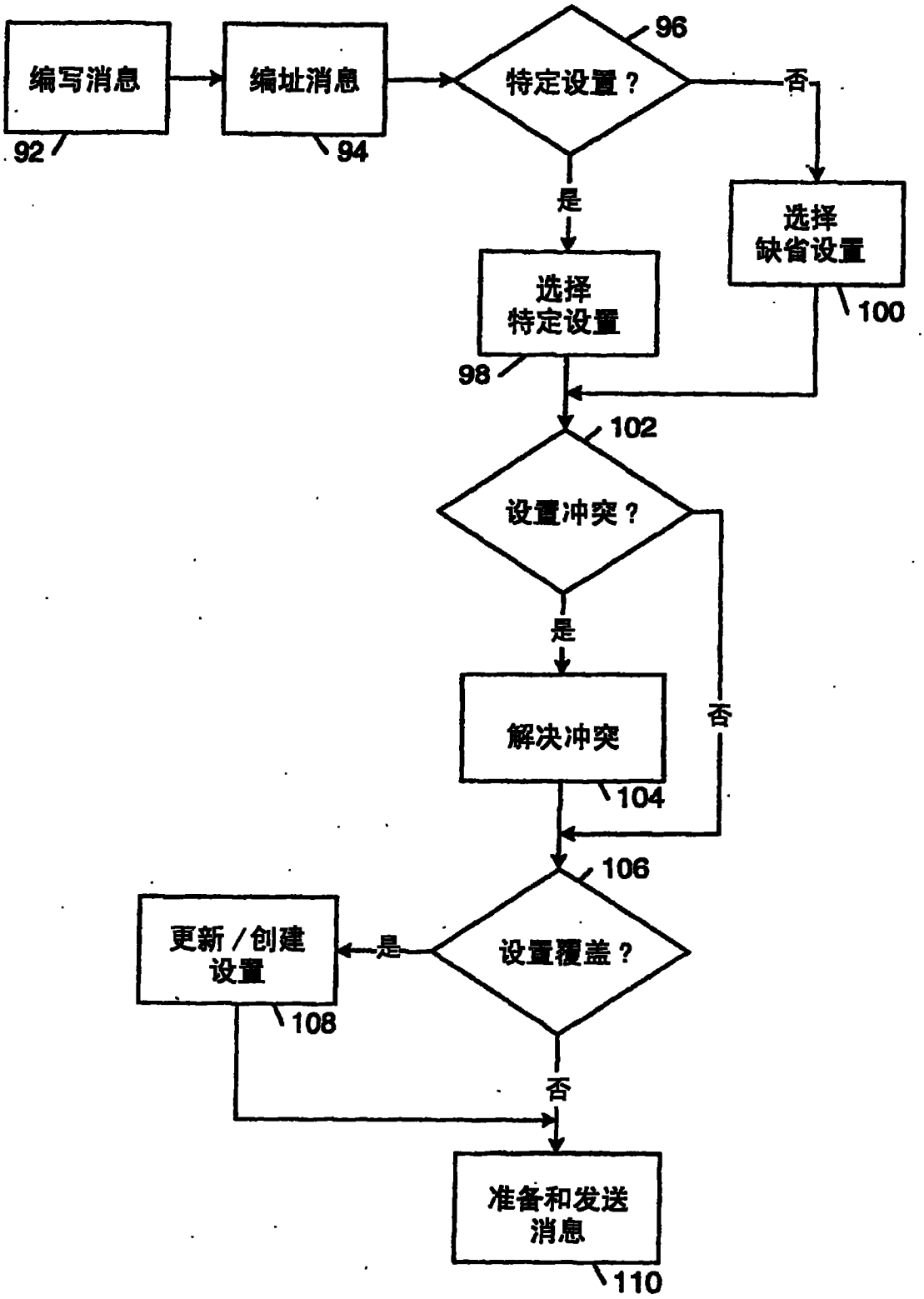

编写消息
92
编址消息
94
特定设置？
96
否
是
选择
缺省设置
100
选择
特定设置
98
102
设置冲突？
是
否
解决冲突
104
106
设置覆盖？
是
更新/创建
设置
108
否
准备和发送
消息
110

图 5

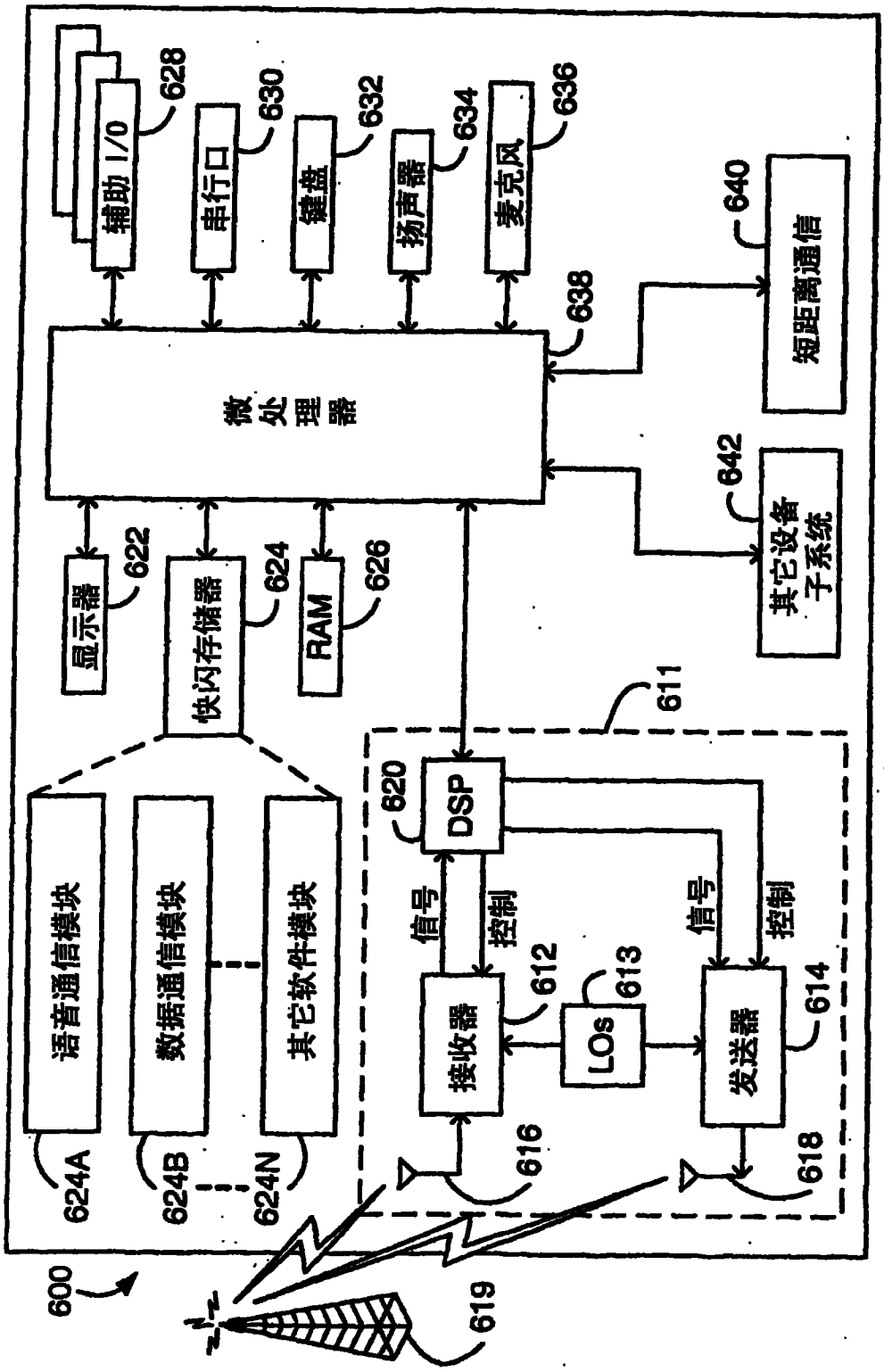

600
619
辅助 I/O
628
串行口
630
键盘
632
扬声器
634
麦克风
636
638
640
短距离通信
微处理器
显示器
622
快闪存储器
624
RAM
626
842
其它设备子系统
611
620
DSP
信号
控制
612
613
LOs
614
接收器
发送器
616
618
语音通信模块
数据通信模块
其它软件模块
624A
624B
624N

图 6