

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04Q 7/32 (2006.01)

H04Q 7/30 (2006.01)

H04B 7/26 (2006.01)

H04L 29/06 (2006.01)



# [12] 发明专利说明书

专利号 ZL 01116383.6

[45] 授权公告日 2006年3月15日

[11] 授权公告号 CN 1245846C

[22] 申请日 2001.4.12 [21] 申请号 01116383.6

[30] 优先权

[32] 2000.9.1 [33] US [31] 09/653764

[71] 专利权人 三星电子株式会社

地址 韩国京畿道

[72] 发明人 S·P·赫尔勒

审查员 陈 军

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 栾本生 王忠忠

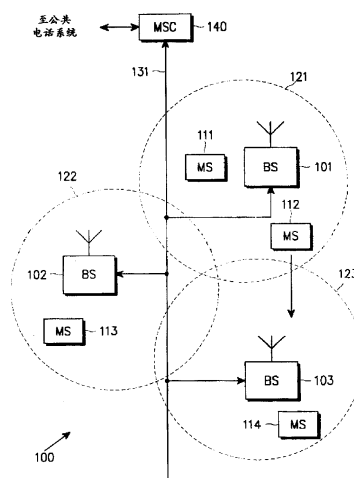
权利要求书 4 页 说明书 14 页 附图 6 页

## [54] 发明名称

安全的通过空间管理无线移动站的系统和方法

## [57] 摘要

公开一种移动站，用于安全地与无线网中的基站通信并从无线网中的服务器接收软件程序，软件校正修补程序和准备数据中至少一种。该移动站包括：RF 发送接收机，加密控制器和数据脉冲串消息协议控制器。也公开了一种通过无线网中的基站安全地利用空间管理无线移动站的系统。它从服务器将软件程序，软件校正修补程序和准备数据中一种或多种发送到无线移动站。该系统包括：数据脉冲串消息协议控制器，加密控制器和 RF 发送接收机。



1. 一种移动站，能够与无线网中的多个基站通信，并从与所述的无线网有关的服务器接收软件程序、软件校正修补程序和准备数据中的至少一种，所述的移动站包括：

RF 发送接收机，能够从所述的多个基站接收软件程序、软件校正修补程序和准备数据的无线消息中的至少一种无线消息并将所述的接收到的无线消息转换成多种互联网协议 IP 分组；

加密控制器，能够将所述的 IP 分组从加密格式转换成解密格式；和

数据脉冲串消息协议控制器，能够将所述的解密 IP 分组转换成至少一种数据脉冲串消息。

2. 如权利要求 1 所述的移动站，其中所述的加密控制器能够按以下至少一种协议将 IP 分组加密和解密：

IP Sec 隧道贯穿协议；

安全壳 SSH 隧道贯穿协议；

安全套接层/传输层安全协议 SSL/TLS；和

点对点隧道贯穿协议 PPTP。

3. 如权利要求 1 所述的移动站，其中每个所述的 IP 分组包括 IP 层和 IP 分组有效载荷。

4. 如权利要求 3 所述的移动站，其中所述的 IP 分组有效载荷包括传输控制协议 TCP 层。

5. 如权利要求 4 所述的移动站，其中所述的 IP 分组有效载荷包括与所述的至少一种数据脉冲串消息有关的通过空间服务准备有效载荷。

6. 如权利要求 1 所述的移动站，其中每个所述的 IP 分组包括 IP 层、传输控制协议 TCP 层和 IP 分组有效载荷。

7. 如权利要求 6 所述的移动站，其中所述的 IP 分组有效载荷包括与所述的至少一种数据脉冲串消息有关的通过空间服务准备有效载荷。

8. 如权利要求 1 所述的移动站，其中所述的数据脉冲串消息协议控制器能够按以下至少一种协议将所述的解密 IP 分组变

换成所述的至少一个数据脉冲串消息：1) IS - 683 - A 协议；2) 短消息服务 SMS 协议；和 3) 可扩展标记语言 XML 协议。

9. 一种用于通过无线网中的基站安全通过空间管理无线移动站的系统，所述的系统能够从与所述的无线网有关的服务器发送软件程序、软件校正修补程序和准备数据中的至少一种到所述的无线移动站，所述的系统包括：

数据脉冲串消息协议控制器，能够接收并将软件程序、软件校正修补程序和准备数据中的至少一种变换成至少一种数据脉冲串消息；

加密控制器，能够将所述的至少一种数据脉冲串消息变换成多种加密的 IP 分组；和

RF 发送接收机，能够将所述的加密的 IP 分组变换成至少一种无线消息，并将所述的至少一种无线消息发送到所述的无线移动站。

10. 如权利要求 9 所述的系统，其中所述的加密控制器能够按以下至少一种协议将 IP 分组加密和解密：

IP Sec 隧道贯穿协议；

安全壳 SSH 隧道贯穿协议；

安全套接层/传输层安全协议 SSL/TLS；和

点对点隧道贯穿协议 PPTP。

11. 如权利要求 9 所述的系统，其中每个所述的 IP 分组包括 IP 层和 IP 分组有效载荷。

12. 如权利要求 11 所述的系统，其中所述的 IP 分组有效载荷包括传输控制协议 TCP 层。

13. 如权利要求 12 所述的系统，其中所述的 IP 分组有效载荷包括与所述的至少一种数据脉冲串消息有关的通过空间服务准备有效载荷。

14. 如权利要求 9 所述的系统，其中每个所述的 IP 分组包括 IP 层、传输控制协议 TCP 层和 IP 分组有效载荷。

15. 如权利要求 14 所述的系统，其中 IP 分组有效载荷包括与所述的至少一种数据脉冲串消息有关的通过空间服务准备

有效载荷。

16. 如权利要求 9 所述的系统，其中所述的数据脉冲串消息协议控制器能够按以下至少一种协议将所述的软件程序、软件校正修补程序和准备数据中的至少一种变换成所述的至少一种数据脉冲串消息：1) IS-683-A 协议；2) 短消息服务 SMS 协议；和 3) 可扩展标记语言 XML 协议。

17. 一种用于无线网的从与无线网有关的服务器安全地发送软件程序、软件校正修补程序和准备数据中的至少一种到无线移动站的方法，该方法包括以下步骤：

接收并将软件程序、软件校正修补程序和准备数据中的至少一种变换成至少一种数据脉冲串消息；

将至少一种数据脉冲串消息变换成多种加密的 IP 分组；

将加密的 IP 分组变换成至少一种无线消息；和

将至少一种无线消息发送到无线移动站。

18. 如权利要求 17 所述的方法，还包括按以下至少一种协议将 IP 分组加密和解密的步骤：

IP Sec 隧道贯穿协议；

安全壳 SSH 隧道贯穿协议；

安全套接层/传输层安全协议 SSL/TLS；和

点对点隧道贯穿协议 PPTP。

19. 如权利要求 17 所述的方法，其中每个 IP 分组包括 IP 层和 IP 分组有效载荷。

20. 如权利要求 19 所述的方法，其中 IP 分组有效载荷包括传输控制协议 TCP 层。

21. 如权利要求 20 所述的方法，其中 IP 分组有效载荷包括与至少一种数据脉冲串消息有关的通过空间服务准备有效载荷。

22. 如权利要求 17 所述的方法，其中每个 IP 分组包括 IP 层、传输控制协议 TCP 层和 IP 分组有效载荷。

23. 如权利要求 22 所述的方法，其中 IP 分组有效载荷包括与至少一种数据脉冲串消息有关的通过空间服务准备有效载

荷。

24. 如权利要求 17 所述的方法，其中接收并将软件程序、软件校正修补程序和准备数据中的至少一种变换成至少一种数据脉冲串消息的步骤包括按以下至少一种协议将软件程序、软件校正修补程序和准备数据中的至少一种变换成至少一种数据脉冲串消息的子步骤：1) IS - 683 - A 协议；2) 短消息服务 SMS 协议；和 3) 可扩展标记语言 XML 协议。

## 安全的通过空间管理无线移动站的系统和方法

### 技术领域

- 5 本发明一般涉及无线网络，并且更具体而言，涉及一种用于安全通过空间（over-the-air）(OTA)规定、更新和管理蜂窝电话手机和其他移动设备的系统。

### 背景技术

- 可靠的预测表明，到2000年全球的蜂窝电话消费者将超过3亿。  
10 在美国，蜂窝服务是由蜂窝服务提供商，由地区性的Bell公司，和由国家的长途经营者提供。增强的竞争已经驱使蜂窝服务的价格下降到这样的点上，以致可提供给很大部分的人口。

- 当代的蜂窝电话主要用于在用户手机（或移动站）和另一方之间通过无线网的话音交谈。较少数量的移动站是数据设备，例如装有蜂窝/  
15 无线调制解调器的个人计算机（PC）。因为当代的移动站的带宽，典型情况下限于每秒几十千位（kbps），使当代移动站的应用是相当有限的。然而，这种情况预期在下一（或第三）代的蜂窝/无线技术，有时被称为“3G”无线/蜂窝中将得以改变，在其中对于每个移动站将可用较大的带宽（也就是，125 kbps或更大）。较高的数据速率将使互联网  
20 应用对于移动站更加普遍。例如，3G小区电话（或带有3G蜂窝调制解调器的PC）可用于浏览互联网上的网址，发送和接收图片，执行流式传输音频和流式传输视频的应用，等。简言之，更高百分数的由3G蜂窝系统处理的无线通信业务将是互联网协议（IP）通信业务，较少的百分数将是传统的话音通信业务。

- 25 为了使无线服务尽可能方便和尽可能易于提供，无线服务提供商常常直接从超级市场和百货商店的展摊上将无线电话手机（或其他类型的移动站）销售给潜在的用户。提供简单的子令，引导购买者通过激活蜂窝手机和立约购买无线服务成为一个用户。在通常的蜂窝系统中，手机购买者通过按照手机子令，在手机键板上拨打“\*228××”  
30 激活新的手机并立约购买服务。“××”的值按照销售的手机的无线服务提供商的身份改变。在手机键板上拨打“\*228××”启动服务提供商过程，使手机能够正常地与无线网通信。

虽然一开始未被提供，新的手机仍必须具有某些最低限度的射频（RF）通信能力，使手机可被提供使用。在手机键板上拨打“\*228××”自动启动将手机购买者与经营者连接的专用的呼叫。经营者从购买者要求某些帐户信息，例如个人信息，信用卡号码，家庭账单地址，等。当帐户信息被收集到时，帐户被建立，经营者指示手机购买者输入通行字，编码号码，菜单选择命令，等几个序列，使手机中的某些功能能够工作。

这个过程通常称为“服务准备（service provisioning）”。服务准备在无线手机中激活号码分配模块（NAM），给手机一个唯一的电话号码，用于打入电话和通过识别被准许的无线载波提供漫游能力。服务准备也在手机中激活最佳的漫激目录（PRL），这是一份在每个地理区域中每个载波拥有的频率/频带的目录，同样可以识别每个区域中最佳的和/或被禁止的频率。最后，服务准备在蜂窝手机中激活一个证明码，有时称为“A-键”。当用户试图接入无线网时，手机利用A-键证实该手机。

无线网利用归属位置寄存器（HLR）存储A-键，电话号码，漫游能力信息，和已经或正在被无线网证实和准备的与每个手机有关的其他数据。HLR是一种由无线服务提供者使用的永久性的数据库，用以识别或检验用户并存储与特征和服务有关的各个用户的数据。当用户正在接入用户归属覆盖区内无线网时，用户的无线服务提供者利用HLR数据。当用户漫游在用户的归属覆盖区外时，其他的无线服务提供者也利用HLR数据（典型情况下通过有线电话网接入）。

已经建立了大量的服务准备标准，允许新的无线服务用户激活无线服务，包括IS-683-A协议。IS-683-A协议是一种TIA/EIA标准，通过空间准备和管理手机。IS-683-A协议利用在移动站手机和基站之间通信业务信道中的数据脉冲串消息来发送管理数据。数据脉冲串消息也用于传递SMS消息。数据脉冲串消息也用于传送其他类型的信息，例如Java字节码，显示在无线手机上的商业广告，用于校正手机错误的软件修补程序，等。

遗憾的是，像IS-683-A和SMS那样的协议有许多缺点。这些协议并不允许漫游（也就是被准备或管理的移动站必须在用户的归属网内）。IS-683-A协议也需要无线网中专门的设备和软件用于在IS

- 683 - A 协议下通信的特殊目的。IS - 683 - A 协议并不提供下载应用程序的能力，也不允许无线服务提供者自动地对移动站提供升级。例如，如果无线服务提供者将它的网络基站从无线电链路协议 3 (RLP3) 升级到无线电链路协议 4 (RLP4) 以便支持较高的数据速率，IS - 683 - A 协议并不允许无线服务提供者通过空间下载软件，将移动站升级到 RLP4。

最好是，使对手机的服务准备过程，升级和管理最大可能程度的自动化，以便降低劳动成本，消除差错，并通过减少或消除用户的交互作用使过程更加为用户喜欢。特别是，通过经互联网连接接入准备服务器通过空间 (OTA) 实施蜂窝服务准备，手机升级和手机管理将是极其方便的。在这样一种情景下，手机并不放置话音呼叫给经营者，而是放置“数据呼叫”，发送互联网协议 (IP) 分组到无线网的基站，和从无线网的基站接收 IP 分组。

因此，在技术上有需要改进的系统和方法，用以实施对无线手机(和其他类型的移动站)的自动服务准备，升级和管理。尤其是，在技术上需要用于实施对无线设备安全的，通过空间的准备和升级。更具体而言，需要这样的系统和方法，即使当用户在用户的归属网外漫游时，也能够实施安全的通过空间准备和升级无线设备。

#### 发明内容

为解决以上讨论的现有技术的不足，本发明的一个主要目的提供一种移动站，能够安全地与无线网中的多个基站通信，并且从与无线网有关的一个服务器接收软件程序、软件校正修补程序和准备数据的至少一个。依据本发明的一种有利的实施方案，该移动站包括：1) RF 发送接收机 (transceiver)，能够从多个基站接收无线消息并将接收到的无线消息变换成多个互联网协议 (IP) 分组；2) 加密控制器，能够将 IP 分组从加密格式变换成解密格式；和 3) 数据脉冲串消息协议控制器，能够将解密的 IP 分组变换成至少一个数据脉冲串消息。

具体地，本发明提供一种移动站，能够与无线网中的多个基站通信，并从与所述的无线网有关的服务器接收软件程序、软件校正修补程序和准备数据中的至少一种，所述的移动站包括：RF 发送接收机，能够从所述的多个基站接收软件程序、软件校正修补程序和准备数据的无线消息之中的至少一个无线消息并将所述的接收到的无线消息变



换成多种互联网协议 IP 分组；加密控制器，能够将所述的 IP 分组从加密格式变换成解密格式；和数据脉冲串消息协议控制器，能够将所述的解密 IP 分组变换成至少一种数据脉冲串消息。

5 本发明还提供一种用于通过无线网中的基站安全通过空间管理无线移动站的系统，所述的系统能够从与所述的无线网有关的服务器发送软件程序、软件校正修补程序和准备数据中的至少一种到所述的无线移动站，所述的系统包括：数据脉冲串消息协议控制器，能够接收并将软件程序、软件校正修补程序和准备数据中的至少一种变换成至少一种数据脉冲串消息；加密控制器，能够将所述的至少一种数据脉冲串消息变换成多种加密的 IP 分组；和 RF 发送接收机，能够将所述的加密的 IP 分组变换成至少一种无线消息，并将所述的至少一种无线消息发送到所述的无线移动站。

15 本发明又提供一种用于无线网的从与无线网有关的服务器安全地发送软件程序、软件校正修补程序和准备数据中的至少一种到无线移动站的方法，该方法包括以下步骤：接收并将软件程序、软件校正修补程序和准备数据中的至少一种变换成至少一种数据脉冲串消息；将至少一种数据脉冲串消息变换成多种加密的 IP 分组；将加密的 IP 分组变换成至少一种无线消息；和将至少一种无线消息发送到无线移动站。

20 依据本发明的一种实施方案，该加密控制器能够按以下至少一种对 IP 分组加密和解密：1) IP Sec 隧道贯穿 (tunneling) 协议；2) 安全壳 (Secure Shell) (SSH) 隧道贯穿协议；3) 安全套接层 (Secure Sockets Layer) / 传输层安全协议 (Transport Layer Security) (SSL/TLS)；和 4) 点对点隧道贯穿协议 (PPTP)。

25 依据本发明的另一种实施方案，每个 IP 分组包括 IP 层和 IP 分组有效载荷 (payload)。

依据本发明又一个实施方案，IP 分组有效载荷包括传输控制协议 (TCP) 层。

30 依据本发明的另一个实施方案，IP 分组有效载荷包括与至少一个数据脉冲串消息有关的通过空间服务准备有效载荷。

依据本发明的另一实施方案，每个 IP 分组包括 IP 层、传输控制协议 (TCP) 层和 IP 分组有效载荷。

依据本发明的又一个实施方案，IP 分组有效载荷包括与至少一个数据脉冲串消息有关的通过空间服务准备有效载荷。

依据本发明又一个实施方案，该数据脉冲串消息协议控制器能够按照以下的至少一种将解密的 IP 分组转换成至少一个数据脉冲串消息：

- 5 1) IS-683-A 协议；2) 短消息服务 (short messaging service) (SMS) 协议；和 3) 可扩展标记语言 (extensible mark-up language) (XML) 协议。

提供一种用于经由无线网中的基站安全的通过空间管理无线移动站的系统也是本发明的一个主要目的。该系统能够将软件程序、软件校正修补程序和来自与无线网有关的服务器的准备数据的至少一种发送到该无线移动站。在本发明的一种有利的实施方案中，该系统包括：

10 1) 数据脉冲串消息协议控制器，能够接收软件程序、软件校正修补程序和准备数据的至少一种，并将其变换为至少一个数据脉冲串消息；

2) 加密控制器，能够将至少一个数据脉冲串消息转换成多个加密的 IP

15 分组；和 3) RF 发送接收机，能够将加密的 IP 分组转换成至少一个无线消息并将至少一个无线消息发送到无线移动站。

在本发明的一种实施方案中，加密控制器能够按照以下的至少一种将 IP 分组加密和解密：1) IP Sec 隧道贯穿协议；2) 安全壳 (SSH) 隧道贯穿协议；3) 安全套接层/传输层安全协议 (SSL/TLS)；和 4) 点对点隧道贯穿协议 (PPTP)。

20

在本发明的另一种实施方案中，每个 IP 分组包括一个 IP 层和一个 IP 分组有效载荷。

在还是本发明的另一种实施方案中，IP 分组有效载荷包括传输控制协议 (TCP) 层。

25 在本发明的又一个实施方案中，IP 分组有效载荷包括一个与至少一个数据脉冲串消息有关的通过空间服务准备有效载荷。

在本发明的另一种实施方案中，每个 IP 分组包括一个 IP 层，传输控制协议 (TCP) 层和一个 IP 分组有效载荷。

30 在本发明的又一种实施方案中，IP 分组有效载荷包括与至少一个数据脉冲串消息有关的通过空间服务准备有效载荷。

在本发明再一个实施方案中，数据脉冲串消息协议控制器能够按照以下的至少一种协议将软件程序，软件校正修补程序和准备数据的至

少一种变换为至少一个数据脉冲串消息：1) IS-683-A 协议；2) 短消息服务 (SMS) 协议；和 3) 可扩展标记语言 (XML) 协议。

5 以上已经相当广泛地概述了本发明的特征和技术优点，以使本领域的技术人员可以较好地理解以下的本发明详述。以下将描述本发明另外的特征和优点，这些组成了本发明权利要求的主题。本领域的技术人员应该理解，他可很容易利用所公开的构思和具体的实施方案作为修改或设计其他结构的基础，用于实现本发明的相同目的。本领域的技术人员也应该意识到这样一些等同的结构并不偏离本发明的精神和范围。

10 在开始本发明详述前，陈述在本专利文件通篇中所用的某些词和短语的定义可能是有利的：术语“包含”和“包括”及其派生词，意味着无限制地包括；术语“或”是范围广泛的，意思是和/或；短语“与...有关”和“与其中...有关”及其派生词，可以意味着包括，包括在内，与...有联系，包含，在...内包含，连接到或与...相连，耦合到或  
15 与...相耦合，与...可联系的，与...合作，插入，把...并列，近似于，结合到或与...结合，具有，具有...特性，等；术语“控制器”意思是控制至少一种操作的任何设备，系统或部件，这样一种设备可以用硬件，固件或软件，或至少两种同样的某种组合。与任何控制器有关的功能可以是集中的或者分布式的，或者就地或者远距离进行。对于某些词或短语的定义被提供在本专利文件的整篇中，本领域的技术人员  
20 应该理解，在许多情况下，如果不是大多数情况的话，这些定义适用于这些被定义的词和短语现在，以及将来的使用。

#### 附图说明

25 为了更全面地理解本发明及其优点，现在参考以下结合附图的描述，其中同样的数字标记同样的物件，其中：

图 1 示出依据本发明的一种实施方案的一种示范性无线网概貌；

图 2 示出图 1 中示范性无线网所选部分的备用图，依据本发明的一种实施方案实现通过空间 (OTA) 服务准备；

30 图 3 示出依据本发明的一种实施方案，在示范性无线网的所选部分之间的逻辑连接的备用图；

图 4 示出依据本发明的一种实施方案的一种示范性移动站；

图 5A 示出一种示范性 IP 分组，其中 IS-683-A 通过空间服务准

备 (OTASP) 的有效载荷已经被按照本发明的一种实施方案, 利用安全壳隧道贯穿协议加密;

图 5B 示出一种示范性 IP 分组, 其中 TCP 层和 IS - 683 - A 通过空间服务准备 (OTASP) 的有效载荷已经被按照本发明的一种实施方案, 利用 IP Sec 隧道贯穿协议加密; 和

图 6 描述流程图 600, 示出依据本发明的一种实施方案, 在无线网 100 中一种示范性安全的数据下载操作。

#### 具体实施方式

以下讨论的图 1 到图 6, 和在本专利文件中用于描述本发明原理的各种实施方案只是用作说明的方法, 无论如何不应该被解释为对本发明范围的限制。本领域的技术人员将理解, 本发明的原理可在任何被适当安排的无线网中得到实施。

图 1 示出依据本发明的一种实施方案的一种示范性无线网 100 的概貌。无线电话网 100 包括多个小区场地 (cell site) 121 - 123, 每个包含基站 BS101, BS102, 或 BS103 中的一个。基站 101 - 103 能够与多个移动站 (MS) 111 - 114 通信。移动站 111 - 114 可以是任何合适的无线通信设备, 包括通常的蜂窝电话、PCS 手机设备、便携式计算机、遥测设备等。

虚线示出小区场地 121 - 123 的近似边界, 基站 101 - 103 位于其中, 将蜂窝场地表示成近似圆形只是为了图示说明和解释。应该清楚地理解, 小区场地也可以有不规则的形状, 这取决于所选的小区配置和自然的及人为的障碍物。

在本发明的一种实施方案中, BS101, BS102, 和 BS103 中的一个或多个可以包括一个基站控制器 (BSC) 和至少一个与每个 BSC 有关的基本发送接收机站 (BTS)。基站控制器和基本发送接收机站对于本领域的技术人员是众所周知的。基站控制器是一种管理无线通信资源的设备, 包括在无线通信网中特定小区的基本发送接收机站。基本发送接收机站包括 RF 发送接收机, 天线, 和位于每个小区场地中的其他电气设备。该设备可包括空中调整单元, 加热单元, 电源, 电话线接口, RF 发射机和 RF 接收机, 以及呼叫处理电路。为了解释本发明的操作简单和清楚起见。将在每个小区 121, 122 和 123 中的基本发送接收机站, 和与每个基本发送接收机站有关的基站控制器合起来分别用 BS101,

BD102 和 BS103 表示。

BS101, BS102 和 BS103 通过通信线 131 和移动交换中心 (MSC) 140 在相互以及公共电话系统 (未示出) 之间传送语音和数据信号。移动交换中心 140 对于本领域的技术人员是熟知的。移动交换中心 140 是一种交换设备, 在无线网中的用户和外部网, 如公共电话系统或互联网之间提供服务和协调。通信线 131 可以是任何合适的连接装置, 包括 T1 线, T3 线, 光纤链路, 网络骨干连接, 等。在本发明的某些实施方案中, 通信线 131 可以是几种不同的数据链路, 其中每种数据链路将 BS101, BS102, 或 BS103 中的一个连到 MSC140。

10 在示范性的无线网 100 中, MS111 位于小区场地 121 中, 与 BS101 通信, MS113 位于小区场地 122 中, 与 BS102 通信, 和 MS114 位于小区场地 123 中, 与 BS103 通信。MS112 也位于小区场地 121 中, 靠近小区场地 123 的边缘。最贴近 MS112 的方向箭头指明 MS112 朝小区场地 123 移动。在某个点上, 当 MS112 移入小区场地 123 和移出小区场地 121 时, 将发生“转交 (handoff)”。

正如众所周知的那样, “转交”步骤将呼叫的控制从第一小区传递到第二小区。例如, MS112 在与 BS101 通信, 感觉到来自 BS101 的信号成为不可接受的微弱, 那末 MS112 可以切换到具有较强信号的 BS, 例如由 BS103 发送的信号, MS112 和 BS103 建立了新的通信链路, 信号被发送到 BS101 和公共交换电话网以便通过 BS103 传送进行中的语音, 数据, 或控制信号。从而该呼叫被无缝地从 BS101 传递到 BS103。

“空闲的”转交是正在控制或导呼信道中通信的移动设备的小区之间的转交, 而不是在常规通信业务信道中发送语音和/或数据信号。

一个或多个移动站 111 - 114 一开始可以是未被准备的设备。也就是, 必要的配置数据, 例如号码分配模块 (NAM) 数据, 最佳的漫游目录 (PRL) 数据, 或证明码 (或“A-键”) 数据可能未存在于, 例如 MS112 中, 或者, 如果存在, 可能未被正确地配置或起动, 以致 MS112 不能够通过 BS101 正确地接入无线网 100。而且, 无线网 100 的经营者可能希望发送 (也就是下载) 软件修补程序以校正 MS112 中存在的差错, 或者软件升级以增加新的服务能力 (例如, 新的 RLP 版本) 给 MS112。为了使这样的未被准备的设备能够在无线网 100 中操作, 在无线网 100 中提供一种通过空间 (OTA) 能力来实现服务准备、升级

和移动站管理。

图 2 示出示范性无线网 100 所选部件的一种备用图，依据本发明的一种实施方案实现通过空间 (OTA) 服务准备。如图 1 中那样，仍然存在 MS112, BS101, 和 MSC140。在图 2 中，无线网 100 还包括相互  
5 工作功能 (IWF) 单元 150, 归属位置寄存器 (HLR) 155, 开帐单和维护服务器 158, 准备服务器 160, 和手机数据库 170。准备服务器 160 是一种全系统的中央服务器，可位于远离无线网 100 的其他部件，也就是，BS101, MSC140, IWF 单元 150, 和 HLR155。为了接入准备服务器 160 中的数据，MSC140 通过内部网/互联网 165 (在此以后称“互联网  
10 网 165”) 与准备服务器 160 通信。因为在无线网 100 内的数据可按照无线服务提供者所做的选择与一种或多种各种各样的通信协议通信，需要 IWF 单元 150 将传送无线网 100 中应用数据的“本来的”通信传输协议翻译成为基于适于在互联网 165 中传输的数据分组的互联网协议 (IP)。

15 应该指出，本发明的范围并不限于利用互联网链接基站和准备服务器的无线网。在本发明的替换的实施方案中，互联网 165 实际上可以是一种具有相对最少量安全性的大的内部网，将一组基站链接到一个或多个准备服务器。

正如以下将要更详细地解释的那样，当一个未被准备的移动站，如  
20 MS112, 接入无线网 100 (通过 BS101) 时，BS101 和/或 MSC 140, 利用在 HLR 155 中的手机数据，将 MS 112 识别为一个未被准备的手机，并通过互联网 165 与准备服务器 160 建立会话，以便实现对 MS 112 的服务准备。然而，因为互联网 165 是一种并不由经营无线网 100 的无线服务提供者拥有或控制的网络，本发明提供安全保护，防止未授权  
25 的人干扰敏感的操作，如准备，参数管理，软件下载等。

而且，如果升级软件或软件校正修补程序可得到，无线网 100 能够发送通知消息到 MS 112, 通知 MS 112 升级和/或修补。然后操作 MS 112 的用户可以通过 BS101 和 MSC 140 选择下载升级或校正修补。在示范性的实施方案中，假定，除了准备数据外，准备服务器 160 也负责  
30 存储和下载软件升级和软件校正修补程序。在本发明的一种实施方案中，准备服务器 160 可以通过互联网 165 从手机数据库 170 回放准备数据，软件升级和校正修补程序。

如图 2 中通过逻辑数据路径 205 所指明的那样, 以上操作是通过建立 MS 112 和无线网 100 之间的数据呼叫实现的。逻辑数据路径 205 表示, 例如, 连接 MS 112 和 IWF 单元 150 的点对点协议 (PPP) 链路, 这适合于在 MS 112 和 IWF 单元 150 之间传送 IP 分组。无线网 100 也在 MS 112 和准备服务器 160 之间建立安全连接。如图 2 中由逻辑数据链路 210 所示。逻辑数据链路 210 表示在 MS 112 和准备服务器 160 之间的一种虚拟的安全的 (也就是加密的) 传输控制协议/互联网协议 (TCP/IP) 的连接。实际的物理路径是通过 MS 112, BS 101, MSC 140, IWF 单元 150, 和处理服务器 160 建立的。

在本发明的一种实施方案中, 安全性由隧道贯穿协议提供, 在 MS 112 和准备服务器 160 之间的两个方向中, 将包括 TCP 层信息的 TCP/IP 分组有效载荷加密。在本发明的另一种实施方案中, 安全性由例如 IP Sec 隧道提供, 在 MS112 和准备服务器 160 之间的两个方向中, 将包括 TCP 层的整个 IP 分组有效载荷加密。

SSH 对于熟悉本领域的技术人员是众所周知的。例如, 见 “Secure Shell Protects Network Communications”, George Lavender, <http://istpub/berkeley.edu:4201/bcc//Winter98/gen.ssh.html>; “SSH Basics”, <http://www.uni-karlsruhe.de/~ig25/ssh-faq/ssh-faq-2.html>; 和 “Getting started with SSH”, Kimmo Suominen, <http://www.tac.nyc.ny.us/~kim/ssh/>。

在本申请的整个本发明详述部分, 本发明的示范性实施方案所描述的是利用 SSH 隧道贯穿协议或 IP Sec 隧道贯穿协议提供移动站和准备服务器通信的加密数据路径。然而, 应该理解, 这只是利用举例的方法, 无论如何不应该被解释成对本发明范围的限制。本领域的技术人员将意识到, 本发明可利用其他的隧道贯穿协议容易得以实现。特别是, 在本发明的其他实施方案中, 利用一种或多种 IP Sec、SSH、安全套接层/传输层安全协议 (SSL/TLS) 可以提供一种安全的、加密的数据路径, 这是由 Netscape 浏览器推广的一种互联网标准, 或者利用 PPTP, 这是点对点隧道贯穿协议 (大部分是基于 PPP) 的 Microsoft 的版本。通常, 本发明可以利用任何的虚拟私人网 (VPN) 技术来实现。

同样, 本公开内容描述本发明的示范性实施方案, 利用 IS-683-A 协议在移动站和准备服务器之间发送数据脉冲串消息。这再一次只

是利用举例的方法，不应该被解释成对本发明范围的限制。本领域的技术人员将认识到，本发明可以利用其他协议在移动站和准备服务器之间发送在数据脉冲串消息中准备的内容来实现。特别是，在本发明的其他实施方案中，提供的内容可在移动站和准备服务器之间，通过数据脉冲串消息发送，利用的是一种或多种以下的协议：IS - 683 - A 协议，短消息服务（SMS）协议，和可扩展标记语言（XML）衍生品，包括（但并不限于）HTML 和 XHTML。

图 3 示出依据本发明的一种实施方案，表示示范性无线网 100 所选部分之间的逻辑连接的备用图。如图 2 中一样，BS101，MS112，MSC 140，IWF 单元 150，HLR 155，开帐单和维护服务器 158，准备服务器 160，互联网 165，手机数据库 170，和逻辑数据路径 205 仍然存在。准备处理器 160 执行软件应用程序 161，能够在 IS - 683 - A 和 SSH 协议之下通信。逻辑数据路径 305 表示在 MS 112 和准备服务器 160 之间 TCP/IP 连接上的一个虚拟的安全（也就是加密的）的 SSH 隧道。逻辑数据路径 310 表示一个 IS - 683A，在 MS 112 和准备服务器 160 之间的一种虚拟的安全的（也就是加密的）SSH 隧道，通过空间服务准备（over-the-air-service）（OTASP）有效载荷。

图 3 也示出连接的顺序，标记为 1 - 5，指明在 MS 112，MSC 140，IWF 单元 150，和准备处理器 160 之间的信息流。当用户，例如，按压手机上的一个专门的互联网键，或在键板上拨打“228 × ×”时，MS 112 启动准备数据呼叫。准备数据呼叫将 MS 112 通过 BS 101 连到 MSC 140。接着，MSC 140 利用 IWF 单元 150 启动快速 - 网络 - 连接（QNC）。当完成时，在 MS 112 和 IWF 单元 150 之间建立点对点（PPP）连接。MSC 140 也与 HLR 155 以及开帐单和维护服务器 158 交换需要的准备数据。

IWF 150 与软件应用程序 161 通信建立逻辑数据路径 305，这就是在准备服务器 160 和 MS 112 之间 TCP/IP 连接上的一个 SSH 隧道。在 SSH 隧道内，逻辑数据路径 310 在 MS 112 和软件应用程序 161 之间传递 IS - 683 AOTASP 有效载荷数据。一旦准备完成，逻辑数据路径 305 也可以在 MS 112 的准备服务器 160 之间提供安全的信息传递，例如软件修补程序或软件升级数据。

图 4 更详细地示出依据本发明的一种实施方案的移动站 112。MS 112 包括 RF 发送接收机 415，天线阵列 416，发射机（TX）处理电路



420, 接收机 (RX) 处理电路 425, TCP/IP 控制器 430, 存储器 435, IS-683-A 协议控制器 445, 和 SSH 密码控制器 450。存储器 435 还包括准备数据文件 441, 升级软件文件 442, 软件校正修补程序 443, 和应用程序 444。

5 RF 发送接收机 415 通过天线阵列 416 发送和接收前向信道和反向信道消息, 并将它们变换成数字电平信号和从数字电平信号变换回来。天线阵列 416 在无线网 100 和 RF 发送接收机 415 之间传送前向和反向信道消息。发射机 (TX) 处理电路 420 从 MS 112 的其他部分, 例如来自话筒的话音数据或者传真/调制解调器/互联网协议 (IP) 数据, 10 如果 MS 112 是个人计算机, 传真机, 等的话。接收机 (RX) 处理电路 425 处理前向信道数据, 例如输入的话音数据, 传真/调制解调器/IP 数据, 控制信道数据, 和通信联络信道数据。RX 处理电路 425 将被处理的前向信道数据传送到 MS 112 的其他部分或被连接的设备, 如显示监视器或扬声器。

15 TCP/IP 控制器 430 在 TX 处理电路 420 或 RX 处理电路 425 和存储器 435 或 IS-683-A 协议控制器 445 之间传递数据。TCP/IP 控制器 430 将来自 RX 处理电路 425 的前向信道数据从 TCP/IP 格式变换成适合于在一个或多个准备数据 441 文件, 升级软件文件 442, 或软件校正修补程序 443 中存储的格式。同样地, TCP/IP 控制器 430 将 IS-683 20 -A 数据变换成 TCP/IP 格式, 并将 TCP/IP 数据传送到 TX 处理电路 420 供在反向通信业务信道中发送。

存储器 435 存储为 MS 112 的系统操作所需的软件和数据。准备数据文件 441 存储准备数据, 如 NAM 数据, PRL 数据, A-键数据, 等。升级软件文件 442 包含可被从 BS 101 下载的软件升级数据。同样地, 25 软件校正修补程序 443 存储可被从 BS 101 下载的软件修补程序。应用程序 444 包括操作 MS 112 的软件。

IS-683-A 协议控制器 445 将发送到或从 TCP/IP 控制器 430 接收到的数据变换到和来自 IS-683-A OTASP 有效载荷。SSH 密码控制器 450 将发送到或在 OTASP 有效载荷中接收到的数据加密和解密。SSH 30 密码控制器 450 对要发送到 TCP/IP 控制器 430 的反向信道数据加密并在存储到存储器 435 中以前将从 TCP/IP 控制器 430 接收到的前向信道数据解密。这样, SSH 加密控制器 450 利用公共键/私人键密码技术在

非安全信道上提供安全的通信。

为了与 MS 112 安全地通信,准备服务器 160 包含许多相同的 MS 112 中找得到的非 RF 部件。也就是,由准备服务器 160 执行的软件应用程序 161 可包括与 MS 112 中对应部件类似的 TCP/IP 控制器, IS - 683 - A 协议控制器和 SSH 加密控制器。而且,准备服务器 160 也包括与存储器 435 类似的存储器,可用于保存被下载到 MS 112 的准备数据,升级软件和软件校正修补程序。

图 5A 示出示范性 IP 包 500,在其中 IS - 683 - A 通过空间服务准备 (OTASP) 的有效载荷已被按本发明的一个实施方案,利用安全壳 (SSH) 隧道贯穿协议加密。示范性的 IP 包 500 包括 IP 层 505, TCP 层 510, 和加密层 515, 该层包含在安全壳隧道中的 IS - 683 - A OTASP 有效载荷。加密层 515 只是被加密的示范性 IP 包 500 的部分。

图 5B 示出示范性 IP 包 550,其中 TCP 层和 IS - 683 - A 通过空间服务准备 (OTASP) 的有效载荷已被按本发明的一个实施方案,利用 IP Sec 隧道贯穿协议加密。示范性的 IP 分组 550 包括 IP 层 555 和加密层 560, 该层包含在 IP Sec 隧道中被加密的 TCP 层数据和 IS - 683 - A OTASP 有效载荷。只有 IP 层 555 未被加密。

图 6 描述流程图 600,依据本发明的一个实施方案,示出一种在无线网 100 中的示范性安全的软件下载操作。起先,MS 112 的操作者建立对 BS 101 的数据呼叫,以便传送一种或多种服务准备数据,更新数据,和软件校正(修补)数据(处理步骤 605)。连同 BS 101,MS112 和 IWF 单元 150 一起工作建立一种虚拟的 PPP 连接,用于在 MS112 和 IWF 单元 150 之间传送 IP 数据分组(处理步骤 610)。依次,IWF 单元 150 通过互联网 165 建立与准备服务器 160 的 IP 会话。

接着,MS 112 和准备服务器 160 通过互联网 165 和无线网 100 建立一个虚拟的安全的隧道(处理步骤 615)。MS 112 将 IS - 683 - A 协议命令和数据文件作为 IP 有效载荷重新编排格式,并利用 SSH, IPSEC, 或其他的加密算法对 IP 分组加密。然后,MS 112 将加密的 IP 分组在反向数据信道中传送到准备服务器 160。MS 112 也在前向信道中从准备服务器 160 接收作为加密的 IP 有效载荷的 IS - 683 - A 协议命令和数据文件,并利用 SSH、IP Sec 或其他的解密算法对 IP 分组解密(处理步骤 620)。

同样地，准备服务器 160 将 IS - 683 - A 协议命令和数据文件作为 IP 有效载荷重新编排格式，并利用 SSH, IP Sec, 或其他的加密算法对 IP 分组加密。然后准备服务器 160 将加密的 IP 分组在前向数据信道中传送到 MS 112。准备服务器 160 也在反向数据信道中从 MS 112 接收加密的 IP 有效载荷，包含 IS - 683 - A 协议命令和数据文件。准备服务器 160 利用 SSH, IP Sec, 或其他的解密算法对 IP 分组解密(处理步骤 625)。MS 112 和准备服务器 160 连续交换和处理加密数据直到被启动的事务完成为止。

虽然对本发明已经详细作了描述，本领域的技术人员应该理解，它们可在其中做各种改变、替换和变更而不偏离本发明的精神和范围。

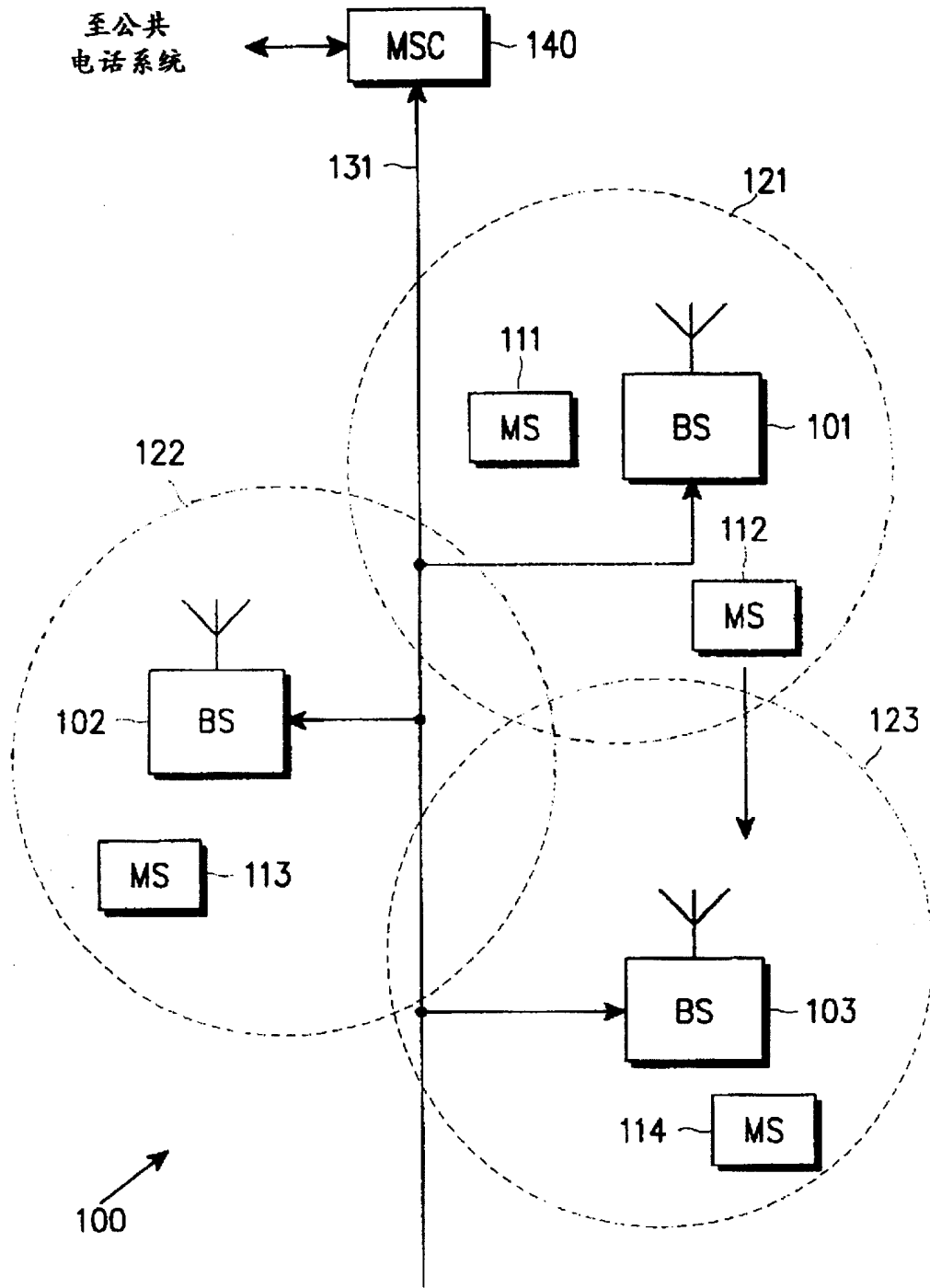


图 1

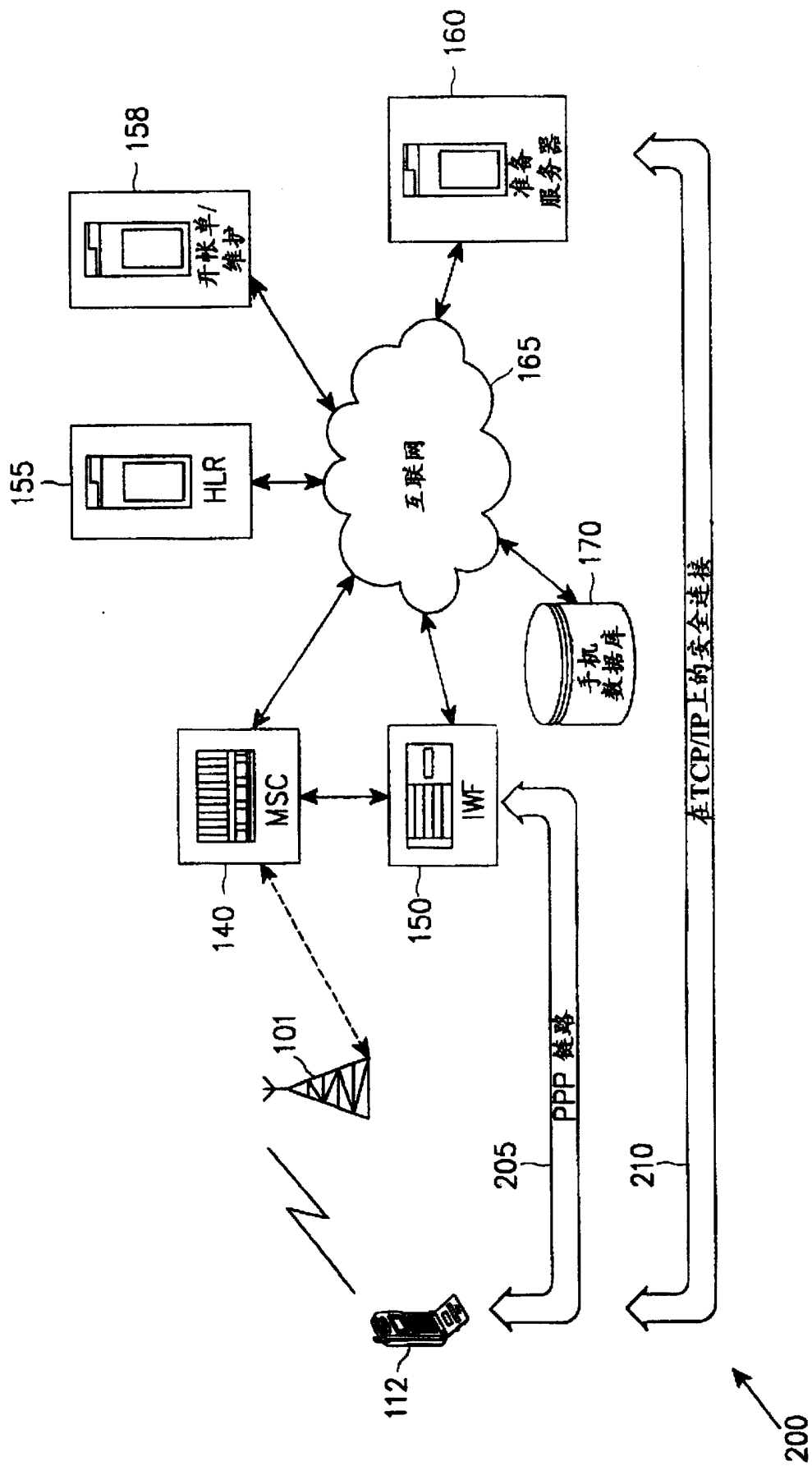
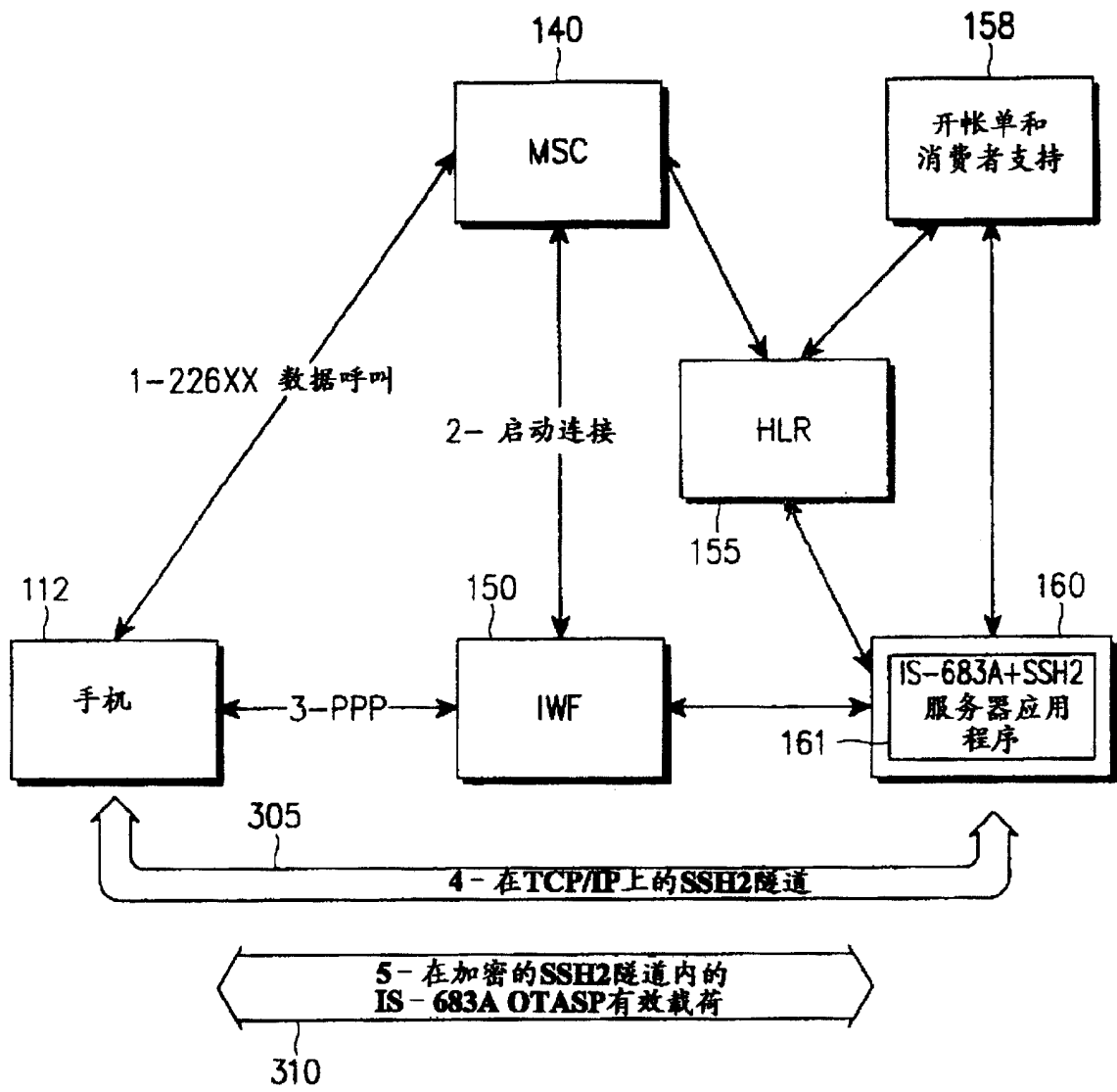


图 2



300 ↗

图 3

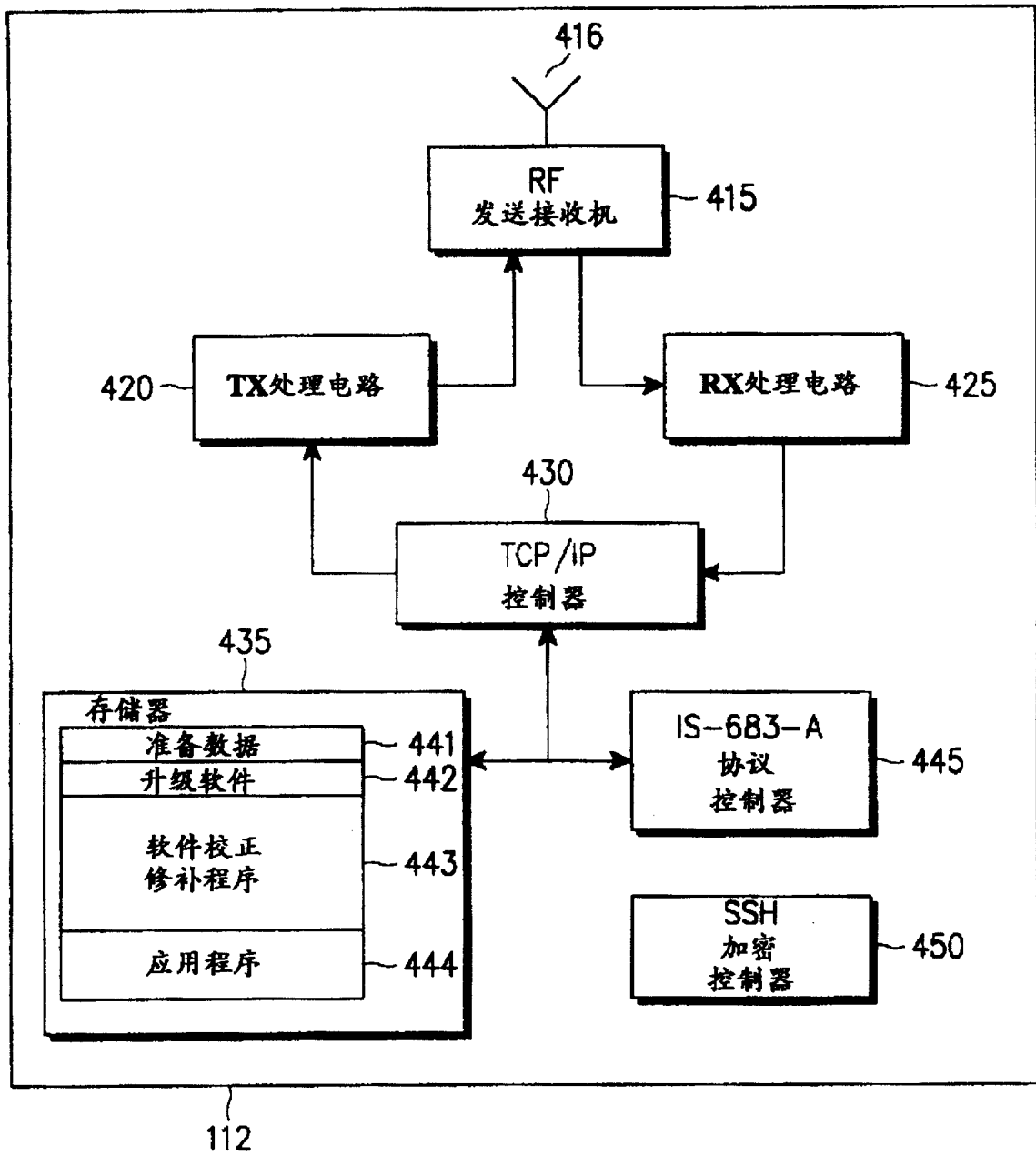


图 4

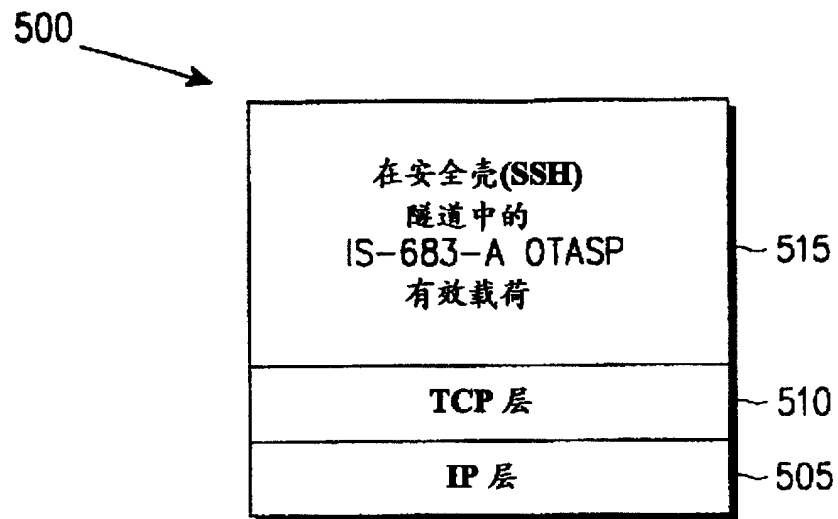


图 5A

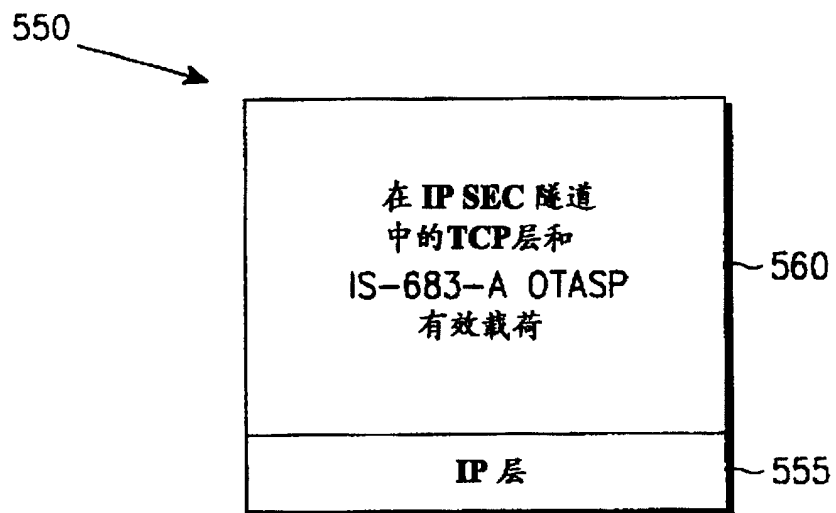


图 5B



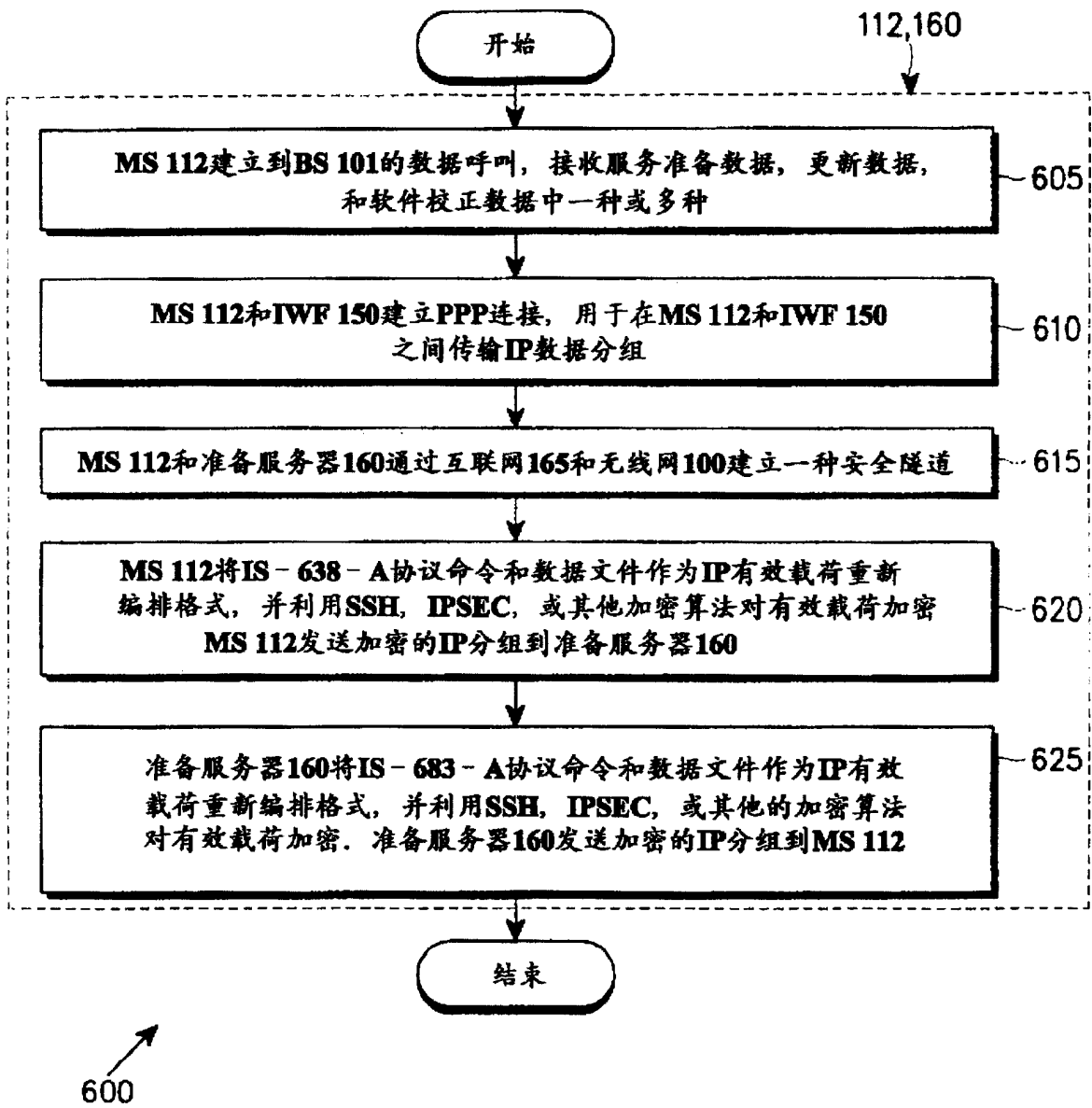


图 6