



(12) 发明专利申请

(10) 申请公布号 CN 104980901 A

(43) 申请公布日 2015. 10. 14

(21) 申请号 201510154421. 4

(22) 申请日 2015. 04. 02

(30) 优先权数据

14/244525 2014. 04. 03 US

(71) 申请人 通用汽车有限责任公司

地址 美国密执安州

(72) 发明人 Y. H. 雷 R. 海涅斯 K. L. 皮尔斯
D. 帕尔

(74) 专利代理机构 中国专利代理(香港)有限公
司 72001

代理人 周春梅 肖日松

(51) Int. Cl.

H04W 4/14(2009. 01)

H04W 12/00(2009. 01)

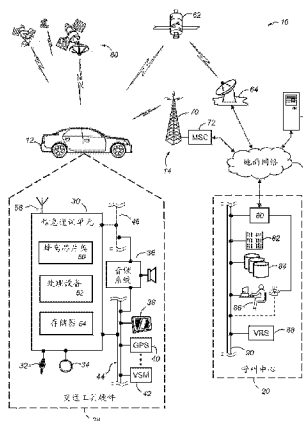
权利要求书2页 说明书13页 附图5页

(54) 发明名称

安全 SMS 消息发送

(57) 摘要

本发明公开了安全 SMS 消息发送。一种移动交通工具通信系统和使用所述系统发送一个或多个安全短消息服务(SMS)消息的方法。所述方法包括以下步骤:a)在发送者处确定与零个或更多个专用数据包(PDP)相关联的数据数量,以在一个或多个 SMS 消息中发送;b)配置一个或多个被配置的 SMS 消息中的每一个的经加密的有效载荷,以携带所述 PDP 的总数量,其中当有效载荷的大小将会导致 SMS 消息超过 140 字节时,所述配置步骤包括配置多个 SMS 消息以携带所述有效载荷;以及 c)从移动发起设备发射一个或多个被配置的 SMS 消息。



1. 一种发送一个或多个安全短消息服务(SMS)消息的方法,包括以下步骤:
 - a) 在发送者处确定与零个或更多个专用数据包(PDP)相关联的数据数量,以在一个或多个 SMS 消息中发送;
 - b) 配置所述一个或多个 SMS 消息中的每一个的经加密的有效载荷,以携带所述 PDP 的总数量,其中当所述有效载荷的大小将会导致 SMS 消息超过 140 字节时,配置步骤包括配置多个 SMS 消息以携带所述有效载荷;以及
 - c) 从移动发起设备发射一个或多个被配置的 SMS 消息。
2. 一种发送一个或多个安全短消息服务(SMS)消息的方法,包括以下步骤:
 - a) 在发送者处确定与零个或更多个专用数据包(PDP)相关联的数据数量,以在至少一个 SMS 消息中发送;以及
 - b) 当一个或多个 PDP 的所确定的数据数量大于单个 SMS 消息的预定最大值时,
 - b1) 配置多个 SMS 消息,以携带所述一个或多个 PDP 的数据,
其中多个 SMS 消息中的每一个的 SMS 报头携带:与 SMS 消息的级联序列相关联的消息索引(MI),所述 SMS 消息的级联序列指示所述序列中的顺序;
其中第一被索引的 SMS 消息的有效载荷携带:指示 PDP 的总数量以及每个所述 PDP 的长度的内部报头,
其中其它被索引的 SMS 消息的有效载荷携带:所述 PDP 数据的至少一部分;以及
 - b2) 从所述发送者发射多个被配置的 SMS 消息。
3. 根据权利要求 2 所述的方法,其中根据公共密钥基础设施(PKI)、使用预共享密钥(PSK)或者两者,对所述多个 SMS 消息中的每一个的所述有效载荷进行加密。
4. 根据权利要求 3 所述的方法,其中所述有效载荷还携带循环冗余校验(CRC),其中所述多个被配置的 SMS 消息中的每一个还携带微证书。
5. 根据权利要求 2 所述的方法,其中所述多个 SMS 消息的辅助部分携带相同的 MAC 值。
6. 根据权利要求 2 所述的方法,还包括:
 - c) 当一个或多个 PDP 的所确定的数据数量小于或等于单个 SMS 消息的预定最大值时,
 - c1) 配置单个 SMS 消息以携带一个或多个 PDP 的数据,其中所述单个 SMS 消息的 SMS 报头携带:指示它是一序列的唯一 SMS 消息的消息索引(MI);
其中所述单个 SMS 消息的有效载荷携带:指示 PDP 的总数量和每个所述 PDP 的长度的内部报头;以及
 - c2) 从所述发送者发射被配置的单个 SMS 消息。
7. 根据权利要求 2 所述的方法,还包括:
 - d) 当所确定的数据数量为与零个 PDP 相关联的空时,
 - d1) 配置单个 SMS 消息以携带零个 PDP,
其中所述单个 SMS 消息的 SMS 报头携带:指示它是一序列的唯一 SMS 消息的消息索引;
 - d2) 从所述发送者发射被配置的单个 SMS 消息。
8. 根据权利要求 2 所述的方法,还包括:
 - e) 在接收者处接收所述至少一个 SMS 消息;以及

f) 当多个 SMS 消息被接收时,根据它们的消息索引设置所述多个 SMS 消息。

9. 根据权利要求 8 所述的方法,其中所述至少一个 SMS 消息携带消息认证码(MAC)值,且进一步包括:在步骤 e) 之后,执行验证所述至少一个 SMS 消息的 MAC 值的步骤 g),其中如果所述 MAC 值不能被验证,则执行丢弃所述至少一个 SMS 消息的步骤 h)。

10. 根据权利要求 8 所述的方法,还包括:

j) 将包括所述一个或多个 PDP 的至少一个响应 SMS 消息从所述接收者发射至所述发送者,其中所述至少一个响应 SMS 消息包括所接收的 SMS 消息的一个或多个 PDP 中的每一个。

安全 SMS 消息发送

技术领域

[0001] 本发明涉及短消息服务(SMS)消息发送。

背景技术

[0002] 短消息服务(SMS)协议可以被各种电信设备使用。SMS 消息可以被移动设备和有线计算机设备发送和接收。SMS 消息可使用最大 140 字节,且当使用 GSM 7 位字符时,可使用最大 160 字符。

发明内容

[0003] 根据本发明的实施例,提供了一种发送一个或多个安全短消息服务(SMS)消息的方法,包括以下步骤:(a)在发送者处确定与零个或多个专用数据包(proprietary data parcel,PDP)相关联的数据数量,以在一个或多个 SMS 消息中发送;(b)配置一个或多个被配置的 SMS 消息中的每一个的经加密的有效载荷(payload),以携带 PDP 的总数量,其中当有效载荷的大小将会导致 SMS 消息超过 140 字节时,配置步骤包括配置多个 SMS 消息以携带所述有效载荷;以及(c)从移动发起设备(mobile originated device)发射一个或多个被配置的 SMS 消息。

[0004] 根据本发明的另一个实施例,提供了一种发送一个或多个安全短消息服务(SMS)消息的方法,包括以下步骤:(a)在发送者处确定与零个或多个专用数据包(PDP)相关联的数据数量,以在至少一个 SMS 消息中发送;以及(b)当一个或多个 PDP 的所确定的数据数量大于单个 SMS 消息的预定最大值时,(b1)配置多个 SMS 消息,以携带所述一个或多个 PDP 的数据,其中多个 SMS 消息中的每一个的 SMS 报头(header)携带:与 SMS 消息的级联序列(concatenated sequence)相关联的消息索引(MI),所述 SMS 消息的级联序列指示所述序列中的顺序;其中第一被索引的 SMS 消息的有效载荷携带:指示 PDP 的总数量以及每个 PDP 的长度的内部报头,其中其它被索引的 SMS 消息的有效载荷携带:所述 PDP 数据的至少一部分;以及(b2)从所述发送者发射多个被配置的 SMS 消息。

[0005] 本发明还公开了如下技术方案。

[0006] 1、一种发送一个或多个安全短消息服务(SMS)消息的方法,包括以下步骤:

a)在发送者处确定与零个或多个专用数据包(PDP)相关联的数据数量,以在一个或多个 SMS 消息中发送;

b)配置所述一个或多个 SMS 消息中的每一个的经加密的有效载荷,以携带所述 PDP 的总数量,其中当所述有效载荷的大小将会导致 SMS 消息超过 140 字节时,配置步骤包括配置多个 SMS 消息以携带所述有效载荷;以及

c)从移动发起设备发射一个或多个被配置的 SMS 消息。

[0007] 2、一种发送一个或多个安全短消息服务(SMS)消息的方法,包括以下步骤:

a)在发送者处确定与零个或多个专用数据包(PDP)相关联的数据数量,以在至少一个 SMS 消息中发送;以及

b) 当一个或多个 PDP 的所确定的数据数量大于单个 SMS 消息的预定最大值时,

b1) 配置多个 SMS 消息,以携带所述一个或多个 PDP 的数据,

其中多个 SMS 消息中的每一个的 SMS 报头携带:与 SMS 消息的级联序列相关联的消息索引(MI),所述 SMS 消息的级联序列指示所述序列中的顺序;

其中第一被索引的 SMS 消息的有效载荷携带:指示 PDP 的总数量以及每个所述 PDP 的长度的内部报头,

其中其它被索引的 SMS 消息的有效载荷携带:所述 PDP 数据的至少一部分;以及

b2) 从所述发送者发射多个被配置的 SMS 消息。

[0008] 3、根据方案 2 所述的方法,其中根据公共密钥基础设施(PKI)、使用预共享密钥(PSK)或者两者,对所述多个 SMS 消息中的每一个的所述有效载荷进行加密。

[0009] 4、根据方案 3 所述的方法,其中所述有效载荷还携带循环冗余校验(CRC),其中所述多个被配置的 SMS 消息中的每一个还携带微证书。

[0010] 5、根据方案 2 所述的方法,其中所述多个 SMS 消息的辅助部分携带相同的 MAC 值。

[0011] 6、根据方案 2 所述的方法,还包括:

c) 当一个或多个 PDP 的所确定的数据数量小于或等于单个 SMS 消息的预定最大值时,

c1)配置单个 SMS 消息以携带一个或多个 PDP 的数据,其中所述单个 SMS 消息的 SMS 报头携带:指示它是一序列的唯一 SMS 消息的消息索引(MI);

其中所述单个 SMS 消息的有效载荷携带:指示 PDP 的总数量和每个所述 PDP 的长度的内部报头;以及

c2) 从所述发送者发射被配置的单个 SMS 消息。

[0012] 7、根据方案 6 所述的方法,其中根据公共密钥基础设施(PKI)、使用预共享密钥(PSK)或者两者,对所述单个 SMS 消息的有效载荷进行加密。

[0013] 8、根据方案 7 所述的方法,其中所述有效载荷还携带循环冗余校验(CRC),其中所述单个 SMS 消息还携带微证书,所述微证书携带与私人密钥相关联的公共密钥。

[0014] 9、根据方案 6 所述的方法,其中所述单个 SMS 消息的辅助部分携带 MAC 值。

[0015] 10、根据方案 2 所述的方法,还包括:

d) 当所确定的数据数量为与零个 PDP 相关联的空时,

d1) 配置单个 SMS 消息以携带零个 PDP,

其中所述单个 SMS 消息的 SMS 报头携带:指示它是一序列的唯一 SMS 消息的消息索引;

其中所述 SMS 消息的有效载荷携带:指示零个 PDP 的内部报头;以及

d2) 从所述发送者发射被配置的单个 SMS 消息。

[0016] 11、根据方案 10 所述的方法,其中根据公共密钥基础设施(PKI)、使用预共享密钥(PSK)或者两者,对所述单个 SMS 消息的有效载荷进行加密。

[0017] 12、根据方案 10 所述的方法,其中所述有效载荷还携带循环冗余校验(CRC),其中所述单个 SMS 消息还携带微证书。

[0018] 13、根据方案 2 所述的方法,还包括:

e) 在接收者处接收所述至少一个 SMS 消息;以及

f) 当多个 SMS 消息被接收时,根据它们的消息索引设置所述多个 SMS 消息。

[0019] 14、根据方案 13 所述的方法,其中所述至少一个 SMS 消息携带消息认证码(MAC)值,且进一步包括:在步骤 e)之后,执行验证所述至少一个 SMS 消息的 MAC 值的步骤 g),其中如果所述 MAC 值不能被验证,则执行丢弃所述至少一个 SMS 消息的步骤 h)。

[0020] 15、根据方案 14 所述的方法,其中步骤 e)还包括接收多个 MAC 值,每个 MAC 值与多个 SMS 消息相关联,其中步骤 h)还包括如果所述 MAC 值不是相同的且如果至少一个 MAC 值没有被验证,则丢弃所述多个 SMS 消息。

[0021] 16、根据方案 13 所述的方法,还包括:步骤 i)如果所述 SMS 消息的任何 SMS 报头不能被验证,则丢弃所述多个 SMS 消息。

[0022] 17、根据方案 13 所述的方法,其中所述发送者是呼叫中心,所述接收者是交通工具信息通讯单元,或者其中所述接收者是所述呼叫中心,所述发送者是所述交通工具信息通讯单元。

[0023] 18、根据方案 13 所述的方法,还包括:

j)将包括所述一个或多个 PDP 的至少一个响应 SMS 消息从所述接收者发射至所述发送者,其中所述至少一个响应 SMS 消息包括所接收的 SMS 消息的一个或多个 PDP 中的每一个。

附图说明

[0024] 下文将会结合附图描述本发明的一个或多个实施例,其中类似的标号指代类似的元件,且其中:

图 1 是显示能够利用在本文公开的方法的通信系统的实施例的框图;

图 2A 阐述了短消息服务(SMS)消息架构的一个实施例;

图 2B 阐述了图 2A 所示的 SMS 架构的另一个实施例;

图 2C 阐述了图 2A 所示的 SMS 架构的另一个实施例;

图 3 阐述了配置和发射图 2A 所示的 SMS 消息的方法;

图 4 阐述了短消息服务(SMS)消息架构的另一个实施例。

具体实施方式

[0025] 以下描述的系统和方法一般适于配置、发射和接收短消息服务(SMS)消息。在一些环境中,可能期望在两个或多个无线设备之间或者在移动设备和使用 SMS 的服务器实体之间进行专用数据包(PDP)通信。PDP 可包括命令或指令,或者可包括敏感信息数据。例如,PDP 可以是从一个无线设备发向另一个无线设备的命令。两个无线设备可以是任何两个合适的设备;例如,以下的公开描述了包括呼叫中心和交通工具信息通讯单元的运行环境;例如,呼叫中心可使用 SMS 来命令信息通讯单元(例如,携带 PDP 的 SMS 消息以解锁交通工具的门或者启动发动机)。以下的公开进一步描述了如何可以使用单个 SMS 消息或者一系列级联的 SMS 消息来发送一个或多个 PDP。在一些情况下,这可改善在发送者和接收者之间的 SMS 消息发送的经济性——例如,发送者可使用一个或至少更少的 SMS 消息来传输多个 PDP,而不是每个 SMS 消息发送一个 PDP。应该明白,以下描述的运行环境仅仅是一个实例,其它的实施方案也是可能的。

[0026] 通信系统——

参照图 1,示出了包括移动交通工具通信系统 10 且可被用于实施在本文中公开的方法

的运行环境。通信系统 10 大体包括交通工具 12、一个或多个无线载波系统 14、地面通信网络 16、计算机 18 以及呼叫中心 20。应该理解所公开的方法能够与任何数量的不同系统一起使用,并不特定地限于此处示出的运行环境。同样,系统 10 的架构、构造、设置和运行以及它的单独部件在现有技术中通常是已知的。因此,以下的段落仅仅简单地提供了一个这样的通信系统 10 的简短概述;但是在此没有示出的其它系统也能够使用所公开的方法。

[0027] 交通工具 12 在阐述的实施例中被描述为客车,但是应该明白,任何其它的交通工具也能够被使用,包括摩托车、卡车、运动型多功能车(SUV)、游艺车(RV)、海上船只、飞行器等。一些交通工具电子件 28 大体在图 1 中示出,包括信息通讯单元 30、麦克风 32、一个或多个按钮或者其它控制输入 34、音频系统 36、可视显示器 38、以及 GPS 模块 40 和多个交通工具系统模块(VSM) 42。这些设备中的一些能够直接连接到信息通讯单元,例如麦克风 32 和按钮 34,而其它的使用一个或多个网络连接间接连接,例如通信总线 44 或者娱乐总线 46。合适的网络连接的实例包括控制器局域网(CAN)、媒体导向系统转移(MOST)、局部互联网络(LIN)、局域网(LAN)以及其它合适的连接,例如以太网或者符合已知的 ISO、SAE 和 IEEE 标准和规定的其它连接,这仅仅例举一小部分。

[0028] 信息通讯单元 30 可以是 OEM 安装(嵌入)或者配件市场设备,它安装在交通工具中,且能够在无线载波系统 14 上且经无线联网进行无线声音和/或数据通信。这能使交通工具与呼叫中心 20、其它启用信息通讯的交通工具、或者一些其它实体或者设备通信。信息通讯单元优选地使用无线电广播来与无线载波系统 14 建立通信信道(声音信道和/或数据信道),使得声音和/或数据传输能够在信道上被发送和接收。通过提供声音和数据通信,信息通讯单元 30 能使交通工具提供多种不同的服务,包括与导航、电话、紧急救援、诊断、信息娱乐等相关联的那些服务。数据能够经数据连接(例如经数据信道上的分组数据传输,或者经使用现有技术中已知技术的声音信道)被发送。对于包括声音通信(例如,在呼叫中心 20 处具有现场顾问(live advisor)或者声音响应单元)和数据通信(例如,提供 GPS 位置数据或者车辆诊断数据至呼叫中心 20)两者的组合服务,系统可利用在声音信道上的单个呼叫,并根据需要在声音信道上在声音和数据传输之间切换,这可以使用本领域技术人员已知的技术来完成。此外,可使用短消息服务(SMS)发送和接收数据(例如,PDP);信息通讯单元可被配置为移动终止和/或发起,或者被配置为应用终止和/或发起。

[0029] 根据一个实施例,信息通讯单元 30 根据 GSM 或者 CDMA 标准利用蜂窝通信,因此包括用于声音通信(例如免提呼叫)的标准蜂窝芯片集 50、用于数据传输的无线调制解调器、电子处理设备 52、一个或多个数字存储器设备 54 以及双天线 56。应该明白,调制解调器能够通过存储在信息通讯单元内的软件实施且由处理器 52 执行,或者它能够是位于信息通讯单元 30 内部或者外部的分开的硬件部件。调制解调器能够使用任何数量的不同标准或者协议(例如 EVDO、CDMA、GPRS 和 EDGE)来运行。交通工具和其它联网设备之间的无线联网也能够使用信息通讯单元 30 来执行。为此目的,信息通讯单元 30 能够被配置为根据一个或多个无线协议(例如,IEEE 802.11 协议、WiMAX 或者蓝牙中的任何一种)无线通信。当用于例如 TCP/IP 的分组交换数据通信时,信息通讯单元能够被配置具有静态 IP 地址,或者能够被设置以从网络上的另一个设备(例如路由器)或者从网络地址服务器自动接收所分配的 IP 地址。

[0030] 处理器 52 可以是能够处理电子指令的任何类型的设备,包括微处理器、微控制

器、主处理器、控制器、交通工具通信处理器、以及专用集成电路(ASIC)。它能够是仅用于信息通讯单元 30 的专用处理器或者能够与其它交通工具系统共享。处理器 52 执行各种类型的数字存储指令,例如存储在存储器 54 中的软件或者固件程序,它能使信息通讯单元提供较宽的多种服务。例如,处理器 52 能够执行程序或者处理数据,以执行本文讨论的方法的至少一部分。

[0031] 信息通讯单元 30 能够被用于提供不同范围的交通工具服务,包括至和 / 或来自交通工具的无线通信。这样的服务包括:转向指引(turn-by-turn directions)以及与基于 GPS 的交通工具导航模块 40 结合提供的其它导航相关联的服务;安全气囊部署通知以及 与一个或多个碰撞传感器接口模块(例如主体控制模块(未图示))结合提供的其它紧急或路边救援相关联的服务;使用一个或多个诊断模块的诊断报告;以及信息娱乐相关联的服务,其中音乐、网页、电影、电视节目、视频游戏和 / 或其它信息被信息娱乐模块(未图示)下载,并被存储用于当前或稍后回放。以上列出的服务决不是信息通讯单元 30 的所有能力的详尽列表,而仅仅是信息通讯单元能够提供的一些服务的列举。此外,应该理解,至少一些上述模块能够以存储在信息通讯单元 30 内部或外部的软件指令的形式实施,它们可以是位于信息通讯单元 30 内部或外部的硬件部件,或者它们可以是彼此集成的和 / 或共享的,或者与位于整个交通工具中的其它系统集成和 / 或共享,这仅列举几种可能性。在模块作为位于信息通讯单元 30 外部的 VSM 42 实施的情况下,它们可利用交通工具总线 44 与信息通讯单元交换数据和命令。

[0032] GPS 模块 40 从 GPS 卫星的星座 60 接收无线电信号。从这些信号,模块 40 能够确定交通工具的位置,该交通工具的位置被用于给交通工具驾驶者提供导航和其它位置相关联的服务。导航信息能够被呈现在显示器 38 上(或者交通工具内的其它显示器)或者能够用语言呈现,例如当提供转向导航时完成。能够使用专用的交通工具内的导航模块(可以是 GPS 模块 40 的一部分)来提供导航服务,或者一些或全部导航服务可以经信息通讯单元 30 来完成,其中位置信息被发送到远程位置,以便于为交通工具提供导航地图、地图标注(感兴趣的点、餐馆等)、路线计算等等。位置信息能够被提供给呼叫中心 20 或者其它远程计算机系统,例如计算机 18,以用于其它的目的,例如车队管理。并且,新的或者更新的地图数据能够经信息通讯单元 30 从呼叫中心 20 下载至 GPS 模块 40。

[0033] 除了音频系统 36 和 GPS 模块 40 之外,交通工具 12 能够包括电子硬件部件形式的其它交通工具系统模块(VSM)42,其它交通工具系统模块(VSM)42 位于整个交通工具中,通常从一个或多个传感器接收输入,并使用所感测到的输入来执行诊断、监测、控制、报告和 / 或其它功能。VSM 42 中的每一个优选地通过通信总线 44 连接到其它 VSM,也连接到信息通讯单元 30,并且能够被编程以运行交通工具系统和子系统诊断测试。例如,一个 VSM 42 能够是控制发动机运行的各方面(例如,燃料点火和点火时间)的发动机控制模块(ECM),另一个 VSM 42 能够是调节交通工具的动力传动系的一个或多个部件的运行的动力传动系控制模块,且另一个 VSM 42 能够是管理位于整个交通工具中的各个电部件(如同交通工具的电动门锁和前灯)的主体控制模块。根据一个实施例,发动机控制模块装备有车载诊断(OBD)特征,车载诊断特征提供大量实时数据,例如从各种传感器(包括交通工具排放传感器)接收的数据,并提供标准化系列的诊断故障代码(DTS),诊断故障代码允许技术人员快速地识别和维修交通工具内的故障。如本领域的技术人员所明白的,以上提及的 VSM 仅仅是可以

在交通工具 12 内使用的一些模块的实例,许多其它的模块也是可能的。

[0034] 交通工具电子件 28 还包括多个交通工具用户接口,为交通工具司乘人员提供了提供和 / 或接收信息的装置,包括麦克风 32、按钮 34、音频系统 36 和可视显示器 38。如在本文所使用的,术语“交通工具用户接口”广泛地包括任何合适形式的电子设备,包括硬件和软件部件,该电子设备位于交通工具上,且能使交通工具用户与交通工具的部件通信或者通过交通工具的部件通信。麦克风 32 提供了至信息通讯单元的音频输入,以能使驾驶者或者其他司乘人员提供声音命令,并执行经无线载波系统 14 的免提呼叫。为此目的,它能够连接到车载自动化声音处理单元,车载自动化声音处理单元利用现有技术中已知的人机接口(HMI)技术。按钮 34 允许手动用户输入至信息通讯单元 30,以发起无线电话呼叫和提供其它数据、响应或者控制输入。分开的按钮能够被用于发起紧急呼叫以及常规服务求助呼叫至呼叫中心 20。音频系统 36 提供音频输出至交通工具司乘人员且能够是专用的单机系统或者主交通工具音频系统的一部分。根据此处所示的具体实施例,音频系统 36 可运行地联接到交通工具总线 44 和娱乐总线 46,且能够提供 AM、FM 和卫星广播、CD、DVD 和其它多媒体功能。这个功能能够与以上描述的信息娱乐模块结合提供或者独立提供。可视显示器 38 优选地是图形显示器,例如仪表板上的触摸屏或者从挡风玻璃反射的抬头显示器,且能够被用于提供多种输入和输出功能。各种其它交通工具用户接口也能够被利用,因为图 1 中的接口仅仅是一种具体实施方案的实例。

[0035] 无线载波系统 14 优选地是蜂窝电话系统,包括多个蜂窝塔 70 (仅示出一个)、一个或多个移动交换中心(MSC)72 以及将无线载波系统 14 与地面网络 16 连接所要求的任何其它的联网部件。每个蜂窝塔 70 包括发送和接收天线以及基站,来自不同蜂窝塔的基站直接连接到 MSC 72 或者经中间装置(例如基站控制器)连接到 MSC 72。蜂窝系统 14 可实施任何合适的通信技术,包括例如模拟技术(例如 AMPS)或者更新的数字技术(例如 CDMA (例如 CDMA2000) 或 GSM/GPRS)。如本领域的技术人员将会明白的,各种蜂窝塔 / 基站 / MSC 设置都是可能的,且可与无线系统 14 一起使用。例如,基站和蜂窝塔能够共同位于相同的地点,或者它们能够彼此定位较远,每个基站能够响应单个的蜂窝塔或者单个基站能够服务各个蜂窝塔,各个基站能够联接到单个 MSC,这仅仅例举一小部分可能的设置。

[0036] 除了使用无线载波系统 14 之外,卫星通信形式的不同无线载波系统能够被用于提供与交通工具的单向或者双向通信。这能够使用一个或多个通信卫星 62 和上行链路发射站 64 来完成。单向通信能够是例如卫星广播服务,其中节目内容(新闻、音乐等)被发射站 64 接收、打包用于上传、且接下来发送到卫星 62,卫星 62 将节目广播到用户。双向通信能够是例如使用卫星 62 在交通工具 12 和站 64 之间中继电话通信的卫星电话服务。如果使用,这种卫星电话能够被附加到无线载波系统 14 或者代替无线载波系统 14 使用。

[0037] 地面网络 16 可以是常规的陆基无线电通信网络,它连接到一个或多个固定电话,并将无线载波系统 14 连接到呼叫中心 20。例如,地面网络 16 可包括公共交换电话网络(PSTN),例如被用于提供有线电话、分组交换数据通信以及互联网基础设施的 PSTN。地面网络 16 的一个或多个部分能够通过使用标准的有线网络、光纤或者其它光学网络、电缆网络、电力线、其它无线网络(例如无线局域网(WLAN))、或者提供宽带无线访问(BWA)的网络及其任何组合来实施。地面网络 16 还可以包括用于存储、上传、转换和 / 或在发送者和接收者之间传输 SMS 消息的一个或多个短消息服务中心(SMSC)。例如,SMSC 可以从呼叫中心

20 或者内容提供商(例如,外部短消息实体或者 ESME)接收 SMS 消息,且 SMSC 可以将 SMS 消息传输给交通工具 12(例如,移动终端设备)。SMSC 和它们的功能对于技术人员来说是已知的。此外,呼叫中心 20 不必经地面网络 16 连接,但是可以包括无线电话设备,使得它能够直接与无线网络(例如无线载波系统 14)通信。

[0038] 计算机 18 能够是多个计算机中的一个,这多个计算机可经私人或者公共网络(例如互联网)访问。每个这样的计算机 18 都能够被用于一个或多个目的,例如交通工具可经信息通讯单元 30 和无线载波器 14 访问网页服务器。其它这样的可访问计算机 18 能够是例如:服务中心计算机,其中诊断信息和其它交通工具数据能够经信息通讯单元 30 从交通工具上传;交通工具所有者或者其他用户为例如如下目的而使用的客户端计算机:访问或者接收交通工具数据,或者设置或配置用户参数,或者控制交通工具的功能;或者第三方库,无论是通过与交通工具 12 还是呼叫中心 20 通信,或者与两者通信,交通工具数据或者其它信息被提供至或者来自该第三方库。计算机 18 还能够被用于提供互联网连接,例如 DNS 服务,或者作为使用 DHCP 或者其它合适的协议来分配 IP 地址给交通工具 12 的网络地址服务器。

[0039] 呼叫中心 20 被设计以提供多种不同的系统后端功能给交通工具电子件 28,并且根据在此示出的示例性实施例,呼叫中心 20 通常包括一个或多个交换机 80、服务器 82、数据库 84、现场顾问 86、以及自动声音响应系统(VRS)88,它们在现有技术中全部都是已知的。这些各种呼叫中心部件优选地经有线或者无线局域网 90 彼此联接。交换机 80 能够是专用交换分机(PBX),路由进入的信号,使得声音传输通常通过普通电话发送到现场顾问 86 或者使用 VoIP 发送到自动声音响应系统 88。现场顾问电话也能够使用 VoIP,如图 1 中的虚线所指示。VoIP 和通过交换机 80 的其它的数据通信经连接在交换机 80 和网络 90 之间的调制解调器(未图示)来实施。数据传输经调制解调器传递到服务器 82 和 / 或数据库 84。数据库 84 能够存储账户信息,例如用户身份验证信息、交通工具标识符、数据图表(profile)记录、行为模式以及其它有关的用户信息。数据传输也可以由无线系统来执行,例如 802.11x、GPRS 等等。此外,可使用短消息服务(SMS)发送和 / 或接收数据(例如,PDP);且呼叫中心 20 可被配置为移动终止和 / 或发起,或者被配置为应用终止和 / 或发起。虽然所阐述的实施例已经被描述为它将会与使用现场顾问 86 的有人控制的呼叫中心 20 一起使用,但是将会明白呼叫中心可代替使用 VRS 88 作为自动顾问,或者 VRS 88 和现场顾问 86 的组合可以被使用。

[0040] 方法——

在至少一种实施方案中,上述运行环境的信息通讯单元 30 和呼叫中心 20 可被用于发送和 / 或接收具有专用数据包(PDP)的 SMS 消息。如之前所描述的,PDP 可包括命令、指令或者请求,或者可包括敏感信息数据。例如,一个 PDP 可包括从呼叫中心至交通工具 12 以解锁交通工具的门的命令;另一个 PDP 可包括至交通工具以提供交通工具诊断更新的命令;另一个 PDP 可包括当前数据和时间的信息。在其它的实例中,从交通工具至呼叫中心的 PDP 可以是用于娱乐或者信息娱乐服务的请求;另一个 PDP 可以是 GPS 位置数据相关的信息或者配置;且另一个 PDP 可以是对呼叫中心请求(例如,确认发送被接收、各种交通工具诊断数据等)的响应。再次地,这些全部仅仅是实例;呼叫中心和交通工具之间的其它实施方案也是存在的,进一步的其它命令、指令、请求和信息也可以存在于其它的运行环境

中。

[0041] 在描述如何在呼叫中心和交通工具(例如,交通工具 12)之间传输 PDP 之前,将会讨论 SMS 的组成或者它的架构。转到图 2A,示出了短消息服务(SMS)消息 200 的架构的一个实施例。阐述的 SMS 消息 200 被划分为多个部分或区段(section),该多个部分或区段包括主的或者总的或者总体的或者 SMS 报头 202、第一保留的或者辅助的部分 204、SMS 有效载荷 206 以及第二保留的或者辅助的部分 208。架构包括每个区段(202、204、206、208)可使用或要求多少个字节(例如,行)210 和 / 或位(例如,列)212 的实例。图示的字节和位的数量和分组仅仅是一个实例;其它的实例或者实施方案是可能的。将会从主报头 202 开始,依次讨论每个区段。

[0042] 在一个实施例中,主报头 202 可包括第十个字节(例如,字节 0-9)。字节 0 可以是 SMS 消息长度(L_{SMS})或者长度值(例如,没有填充位(padding)的整个 SMS 消息中的字节的数量)。例如,如果整个 SMS 消息的长度是 131 字节,则长度值可以是“10000011”,或者如果 SMS 长度是 140 字节,则长度值可以是“10001011”,每个 0 或者 1 对应于位列(7 至 0)。

[0043] 在字节 1,位 0-2 可包括 SMS 版本号(VER #)(例如,SMS 2.0 或者“010”);位 3 可指示安全短消息(SSM),即它是否被加密(例如,是或者否,“0”或者“1”);位 4 可指示响应是否被请求(RR)(例如,是或者否,“0”或者“1”);以及位 5-7 可包括请求 / 响应代码(RRC)(例如,由 SMS 消息的接收者使用;当没有使用时它可以是空或者“000”)。字节 2 可包括序列号(SEQ#);即它可以是唯一的标识符,以将多个 SMS 消息分类,这多个 SMS 消息是消息团簇或者捆绑(an association or bundle of messages)的一部分,如以下将更详细地讨论的。在字节 3,位 0-3 可包括最后的消息索引(FMI);且位 4-7 可包括消息索引(MI)。FMI 和 MI 两者都可以是介于 0 和 15 之间的数字的二进制表示(例如,“0000”,“0001”,...,“1111”)。如以下将更详细地讨论的,当多个 SMS 消息被捆绑且被发射,MI 和 FMI 可被用于使一个 SMS 消息与该捆绑的其它消息相关。字节 4-9 可包括 SMS 消息的期满时间(TOE);例如,TOE 可指示当 SMS 消息不再有效时的明确的日期和时间(或者它可以指示它从发送者或者 SMSC 发射之后的时间段,该时间段指示何时消息应该过期)。

[0044] 第一辅助部分 204 的字节数量可变化。在一个实施例中,第一辅助部分 204 可包括字节 10-52。此处,根据公共密钥基础设施,至少部分这些字节可携带关于微证书的信息。如技术人员将会明白的,使用公共密钥可要求签名的数字证书。例如,x.509 证书可要求 1024 字节的空間。但是在图 2 中,数字证书可以是被称为微证书的特定类型的数字证书,该微证书具有大约 44 字节,如美国专利公开 No. 2010/0202616 所描述,通过引用在本文中合并其全部内容。

[0045] 有效载荷 206 的字节数量也可变化。在阐述的实施例中,有效载荷 206 从字节 53 延伸至 N,有效载荷 206 包括次的或内部或级联或者有效载荷报头 216 和有效载荷主体 218。在图 2A 所示的实例中,内部报头 216 包括字节 53-57。字节 53 指示根据一个或多个 SMS 消息发送的 PDP 序列中的 PDP 的总数量 P。在图示的实例中,P 是四(例如,二进制“100”)且字节 54-57 对应于序列中的四个 PDP 中的每一个。更具体地,字节 54-57 指示 PDP 长度(例如,字节 54 是 PDP_1 的二进制长度,字节 55 是 PDP_2 的二进制长度,字节 56 是 PDP_3 的二进制长度,字节 57 是 PDP_4 的二进制长度)。有效载荷 206 的剩余字节包括它们自己级联或者串在一起的 PDP,或者至少一样多的 PDP 将会可行地配合在有效载荷 206 内,因为 SMS 消息

200 的大小被限制为 140 字节。这也将会在以下讨论。

[0046] 最后的部分,第二辅助部分 208,可包含 MAC 或者消息认证码值和 / 或填充位。MAC 值将会在以下更详细地讨论。在图 2A 所阐述的实例中,SMS 消息 200 的字节 N+1 至 N+8 携带或者包含 MAC 值。字节 N+9 至 139 被阐述为填充位(技术人员将会明白填充位的使用)。

[0047] 现在转到发送图 2A 所示的消息 200 的一个实例,SMS 消息 200 可用来发送多个 PDP,在其中 PDP 的大小导致单个 SMS 消息超过 140 字节。根据图 3 所示的一种方法 300,呼叫中心 20 可配置多个 SMS 消息(捆绑)且将它们发送到交通工具 12 中的信息通讯单元 30。方法 300 可以在步骤 302 开始,其中呼叫中心可确定与零个或更多个 PDP 相关联的数据数量或者二进制数量。例如,如果零个 PDP 被发送,则数据数量可以是 0 字节。当一个或多个 PDP 将被发送时,数据数量可变化(例如,值大于 0 字节)。例如,图 2A 所示的四个 PDP(例如,PDP₁、PDP₂、PDP₃、PDP₄)可分别具有 25 字节、75 字节、50 字节和 100 字节的数据数量。因此,四个 PDP 的总数据数量可以是 250 字节。根据一种实施方案,PDP 的大小可以在 0 和 255 字节之间变化,且如果必要的话,多达 16 个 SMS 消息可以捆绑在一起。

[0048] 在步骤 304,方法 300 可确定将 PDP 作为序列发送所需要的 SMS 消息的所需数量。因此,呼叫中心 20 可估算在一个或多个 SMS 消息中可用的可用有效载荷空间。例如,当 140 字节中的一些被用于非有效载荷数据(例如,SMS 报头、第一辅助部分 204 中的微证书、第二辅助部分 208 中的 MAC 值和 / 或填充位)时,SMS 消息的有效载荷 206 可具有实际的限制。因此在至少一种实施方案中,取决于非有效载荷数据的小大,有效载荷的大小可以小于预定的最大值(例如,100 字节)。因此,如果在一种实施方案中,每个 SMS 消息的最大有效载荷数据是 90 字节,则发送四个 PDP 将会要求三个 SMS 消息。这个估算可包括考虑 PDP₁ - PDP₄(或者 250 字节)和内部报头 216(或者 5 字节,即图 2A 的字节 53-57)的总大小。更具体地,(250 字节 +5 字节)/90 字节 $\approx$ 2.8 SMS 消息,2.8 SMS 消息可以被取整为三个 SMS 消息的捆绑。

[0049] 步骤 306-314 示出了根据将发送的 PDP 的数量和即将使用的 SMS 消息的数量的各种可能的实施方案。例如:步骤 306 阐述了零个 PDP 作为一个 SMS 消息;步骤 308 阐述了一个 SMS 消息携带一个 PDP;步骤 310 阐述了一个 SMS 消息携带多个 PDP;步骤 312 阐述了 SMS 消息的捆绑携带多个 PDP;且步骤 314 阐述了 SMS 消息的捆绑携带一个 PDP。继续以上讨论的实例,方法 300 将会推进以确定在这种实施方案中,具有 255 字节的有效载荷数据将会使多个 SMS 消息成为必要(即,步骤 312)。

[0050] 在步骤 316 和 318,方法配置 SMS 消息。这些步骤包括配置主报头 202、配置辅助的部分 204、配置一个或多个 SMS 消息的有效载荷 206(例如,将有效载荷数据捆绑到在步骤 304 中确定的 SMS 消息的数量中),且配置辅助的部分 208。这些步骤还可以包括将有效载荷数据加密。

[0051] 在步骤 316(或者 318)的至少一种实施方案中,使用数据的主体(例如,二进制长度的消息)的(密钥的)加密散列函数(或者 MAC 算法),由发送者产生 MAC 值。例如,第一秘密密钥(发送者的密钥)和初始消息是散列函数的输入,MAC 值是输出。合适的散列函数的实例包括 MD5、SHA1、SHA256,仅举几个例子。此处,初始消息可以是全部 250 字节消息(即,以上讨论的四个 PDP)。继续该实例,三个捆绑的 SMS 消息(SMS₁、SMS₂、SMS₃)中的每一个都可被分配相同的 SMS 版本号、请求值相同的请求、相同的请求 / 响应代码、相同的序列号、相

同的 FMI 和相同的 TOE。每个捆绑的 SMS 消息的长度(L_{SMS})和 MI 可能不同(因为它索引那个特殊的 SMS 消息,例如,将它索引为第一、第二、第三等)。 L_{SMS} 可根据每个捆绑的 SMS 消息的总长度而变化。MI 值可在消息接收者处使得成捆的 SMS 消息的次序级联或者组织起来;例如,对于 SMS_1 , MI 的值可以是“0000”;对于 SMS_2 , MI 的值可以是“0001”;对于 SMS_3 , MI 的值可以是“0010”。因此, FMI 可以与这捆绑的最后的消息索引(MI)相同(即,与 SMS_3 相关联的“0010”)。

[0052] 步骤 316 和 318 可包括配置每个有效载荷(且确定 MAC 值)的呼叫中心 20。例如,在步骤 316,呼叫中心基于零个 PDP、一个 PDP 或者多个 PDP 的数据数量(从步骤 306、308 或者 310 得到)来配置单个 SMS 消息。且在步骤 318,呼叫中心基于一个 PDP 或者多个 PDP 的数据数量(从步骤 312 或 314 得到)来配置多个 SMS 消息。继续以上的实例,三个 SMS 消息(SMS_1 、 SMS_2 、 SMS_3)的有效载荷 206 被配置。该捆绑的第一 SMS 消息(SMS_1)可包括内部报头 216。如果可行,第一 SMS 消息还可携带附加的有效载荷——即,也携带一些 PDP 数据。第二和第三 SMS 消息(SMS_2 、 SMS_3)可以被配置为携带 PDP 数据的剩余部分。例如,在配置内部报头 216 时,有效载荷的第一字节(例如,图 2A, 字节 53)可指示 PDP 的数量(P)(例如, $P=4$ PDP 或者“00000100”)。接下来的字节可指示每个各自的 PDP 的长度(L)。例如, PDP_1 的长度($L=25$ 字节或者“00011001”)可以被字节 54 携带, PDP_2 的长度($L=75$ 字节或者“01001011”)可以被字节 55 携带, PDP_3 的长度($L=50$ 字节或者“00110010”)可以被字节 55 携带,且 PDP_4 的长度($L=100$ 字节或者“01100100”)可以被字节 56 携带。

[0053] 由于在这实例中 SMS_1 的内部报头仅消耗了 5 个字节,因此存在额外的有效载荷空间,该额外的有效载荷空间可以被呼叫中心 20 配置为携带一些 PDP 数据。此外, SMS_2 和 SMS_3 的全部有效载荷空间是可用的,如图 2B 所示;即,只有该捆绑中的第一 SMS 消息(SMS_1)可需要携带内部报头 216。例如(图 2A),第一 SMS 消息可以被配置为携带 PDP_1 (25 字节)和 PDP_2 的第一 60 字节(总共 90 字节;即 5 字节+25 字节+60 字节)。第二消息的有效载荷(图 2B)可以被配置为携带 PDP_2 的最后 15 字节、所有的 PDP_3 (50 字节)和 PDP_4 的第一 25 字节(总共 90 字节;即 15 字节+50 字节+25 字节)。第三 SMS 消息的有效载荷(图 2B)可被配置为携带 PDP_4 的剩余的 75 字节。这当然仅仅是一个实例,其它的组合是可能的。

[0054] 之后,每个有效载荷 206 被加密。例如, SMS_1 、 SMS_2 和 SMS_3 的有效载荷数据可以根据公共密钥基础设施(PKI)被呼叫中心持有的私人密钥加密,且根据美国专利公开 No. 2010/0202616 中公开的微证书,如上所讨论的,用于加密的微证书可以被配置为每个 SMS 消息的第一辅助部分 204 的一部分。其它的实施方案,包括使用预共享密钥(PSK)——即,由发送者和接收者两者持有的相同密钥,或者 PKI 和 PSK 的组合。其它的安全技术也可以被使用(例如,随机数口令(nonce challenge)等)。选择性地, SMS_1 、 SMS_2 和 SMS_3 的有效载荷数据可以个别地加密而不是作为整体加密。

[0055] 之后,呼叫中心确定的 MAC 值可以被添加到每个消息的第二辅助部分 208 或者被每个消息的第二辅助部分 208 携带;例如,它可以出现在 SMS_1 、 SMS_2 和 SMS_3 的每一个中。适当地,当辅助部分 208 没有填充所有可用的字节,填充位(例如,零或者“00000000”)可以被添加到 SMS 消息(SMS_1 、 SMS_2 、 SMS_3)的第二辅助部分 208 中的任何剩余的未使用字节。

[0056] 已经配置了捆绑中的每一 SMS 消息后,在步骤 320 消息(SMS_1 、 SMS_2 、 SMS_3)可以被发射。因此,它们可以从呼叫中心 20 发送到 SMSC,之后经信息通讯单元 30 发送至交通工

具 12。SMS 消息的发射和接收对于技术人员来说是已知的。在步骤 322, 消息(SMS₁、SMS₂、SMS₃)可以被接收和验证。验证可以包括验证在辅助部分 208 中接收的 MAC 值。例如, 接收者(例如, 交通工具 12)可以使用被发送者(例如, 呼叫中心 20)使用的合适 MAC 算法来验证初始消息(例如, 所有的 250 字节)。更具体地, 通过将初始消息和第二秘密密钥作为输入提供给相同的散列函数, 接收者可以确定另一个 MAC 值。已经执行计算后, 接下来接收者可以将这个新的 MAC 值与所发射的 / 所接收的 MAC 值(即, 辅助部分 208 携带的 MAC 值)进行比较。当两个 MAC 值的值匹配时, 接收者可确定初始消息是未被改变的、未更改的或者没有以其他方式被篡改的。第二秘密密钥可以与第一秘密密钥相同, 且可以由发送者(例如, 呼叫中心)经安全通信信道或者其它合适的安全装置提供至接收者(例如, 交通工具 12)。

[0057] 在一些环境中, 如果所发射的 MAC 值没有被验证, 则信息通讯单元 30 可丢弃所有捆绑的 SMS 消息。信息通讯单元 30 还可以因其它原因丢弃 SMS 消息的捆绑。例如, 如果 SMS 消息的捆绑没有相同的 SMS 版本号或者有效的 TOE。倘若 MAC 值、版本号和 TOE 是有效的, 信息通讯单元接下来可尝试根据 SMS 消息的消息索引(MI)来设置 SMS 消息。因此, 当 FMI 指示三个消息(例如, "0010"), 信息通讯单元可验证在 TOE 之前, MI 等于 "0000"、"0001" 和 "0010" 的三个消息已经全部被接收。如果任何这些项目中任一个不能被验证(或者丢失), 信息通讯单元可标记潜在的错误。

[0058] 使用 MI, 每个 SMS 消息的有效载荷 206 能够被级联——例如, 抽取每个被加密的 SMS 有效载荷并根据 MI 的序列次序将它们端对端串接起来。因此, 虽然 PDP₁被划分在 SMS₁和 SMS₂之间, PDP₃被划分在 SMS₂和 SMS₃之间, 但是所有的 PDP 可以被重新设置到它们的初始序列中。

[0059] 步骤 322 也可以包括抽取微证书, 且使用它来解密消息(SMS₁、SMS₂、SMS₃)的级联的有效载荷 206。如果任何 SMS 消息的微证书不是相同的, 或者如果任何加密不能被认证, 则信息通讯单元 30 可标记潜在的错误。将会明白, 这个步骤可包括使用 PKI、PSK 或者其任何组合来解密。不能认证 SMS 捆绑中的任一个可指示恶意的篡改或者传送错误(SMS 的捆绑以及它们携带的 PDP 可以被忽略和 / 或删除)。

[0060] 当错误被标记时, 全部的 SMS 消息捆绑可以被忽略和 / 或删除。此外, 在步骤 324 信息通讯单元 30 可发送指示错误的响应; 例如, 这可以是预定的请求 / 响应代码(例如, 指示错误的三位二进制数)。此外, 信息通讯单元可以发送响应, 以指示消息捆绑被未篡改和完全完整无缺地接收(例如, 指示确认的预定请求 / 响应)。在一种实施方案中, 步骤 324 中的响应是重新传送所接收的 SMS 消息捆绑; 即, 信息通讯单元 30 将 PDP (PDP₁₋₄) 重新配置到消息(SMS₁、SMS₂、SMS₃)内, 且采用不同的预定请求 / 响应代码(即, 指示它是响应消息的代码)将它们发送到呼叫中心 20。在步骤 324 中响应的其它实施方案是可能的; 在一些情况下, 可没有响应被发送。

[0061] 替代性的实施例也存在。例如, 一个单个的 SMS 消息(图 2A)可携带所有的 PDP (即, 没有使用图 2B 的架构的附加 SMS 消息)。例如, 如果 PDP₁、PDP₂、PDP₃和 PDP₄在长度上全部是仅 10 字节, 那么 SMS₁可携带所有的有效载荷数据(内部报头 216 的 5 字节和 PDP₁₋₄的 40 字节), 且 SMS₂和 SMS₃不会被使用。在图 3 阐述的方法中, 方法将从步骤 304 推进至步骤 310 再至步骤 316。

[0062] 类似地, 如果仅需要一个 PDP 和一个 SMS (例如, 相对较小的 PDP 正在被发送, 例

如,小于 100 字节),则方法 300 将会从步骤 304 推进至步骤 308 再至步骤 316。

[0063] 另一个替代性的实施例在图 2C 中示出。此处,没有 PDP 被发送;因此, $P=0$ (例如,“00000000”或者空)。因此,内部报头在长度上是 1 字节(例如,“00000000”)。由于没有 PDP 被发送,全部的有效载荷 206' 在长度上仅仅是这 1 个字节(例如,字节 53)。这个有效载荷可仍然被加密,且图 3 所示的方法将从步骤 304 推进至步骤 306 再至步骤 316。

[0064] 另一个替代性的实施例可包括单个 PDP,该单个 PDP 足够长以需要多个 SMS 消息。例如,如果 PDP_1 在长度上是 250 字节,三个 SMS 消息(SMS_1 、 SMS_2 、 SMS_3)的捆绑可被使用。如之前所讨论的, SMS_1 可包括至少内部报头,且 PDP 数据可以在 SMS_1 、 SMS_2 和 SMS_3 之间分布,如合适的那样。此处,方法 300 将会从步骤 304 推进至步骤 314 再至步骤 318。

[0065] 在使用 MAC 的另一种实施方案中,第二密钥(即,由接收者交通工具 12 持有)可以与第一密钥(即,由发送者呼叫中心 20 持有)不同。例如,第二密钥可以是与第一密钥相关联的公共密钥。在这种情况下,接收者可接收初始消息的发射备份和所发射的 MAC 值。使用相同的散列函数作为发送者,接收者可将所发射的消息和第二密钥作为输入提供。输出可以是另一个 MAC 值。如果 MAC 值同样地匹配初始 MAC 值的发射备份,则接收者可确定(验证)初始消息的发射备份是未被改变的、未更改的或者没有以其他方式被篡改的。这仅仅是使用 MAC 值和 MAC 算法的另一个例子;其他的例子对于技术人员来说是明显的。

[0066] 另一个替代性的实施例在图 4 中示出。在这个实施例中,主报头 202 可以是相同的;但是,第一辅助部分、有效载荷和第二辅助部分可以不同。在图 4 中,第一辅助部分 204' 可以更短,且包括有限数量的未使用的和保留的字节(例如,四个字节或者字节 10-13)。有效载荷 206' 可包括内部报头 216' (例如,字节 14)。如之前所描述的,它将指示多少个 PDP 存在和它们各自的长度(例如,字节 15-18)。有效载荷 206' 也可以包括验证部分 230。在一个实施方案中,验证部分 230 携带循环冗余校验(CRC)且消耗 16 字节(例如,字节 19-34)。如之前所讨论的, SMS_1 的有效载荷 206' 的剩余部分可携带一些(或全部) PDP 数据。最后,在这个实例中,第二辅助部分 208' 仅包括填充位。

[0067] 方法 300 可以实施微证书,如之前所讨论的。有效载荷 206' 可以被加密——即,包括验证部分 230。当 SMS 消息被接收时,由接收者(例如,信息通讯单元)持有的密钥可被用于解密有效载荷 206'。除了之前描述的技术,CRC 可被用于验证 SMS 消息没有损坏(例如,使用 SMS 消息长度(L_{SMS})且根据已知的技术)。

[0068] 因此,已经公开了用于 SMS 消息的各种架构,SMS 消息用于携带可包括含命令、指令和/或敏感信息数据的专用数据包。此外,已经公开了各种安全 SMS 消息发送技术,以发射这些 PDP 和巩固所发送的 SMS 消息的数量。

[0069] 应理解,前述是本发明的一个或多个实施例的描述。本发明不限于在本文中公开的具体实施例,而是由所附的权利要求书自定义。此外,在前述描述中包含的声明涉及具体实施例,并不解释为对本发明的范围或者对在权利要求中使用的术语的定义的限制,除非术语或者短语在以上明确地定义。各种其它实施例、以及对所公开的实施例的各种改变和修改对于本领域的技术人员来说都是明显的。所有这样的其它实施例、改变和修改都旨在落入所附的权利要求的范围内。

[0070] 如在这份说明书和权利要求书中所使用的,术语“例如”、“譬如”、“比如”、“之类”以及“类似物”,动词“包括”、“具有”、“包含”以及它们的其它动词形式,当与一个或多个部

件或者其它物件的列表结合使用时,每一个都被解释为开放式的,意味着该列表并不会被认为是排除其它、附加部件或物件。其它的术语被解释为使用它们的最宽泛的合理含义,除非它们在要求不同解释的上下文中使用。

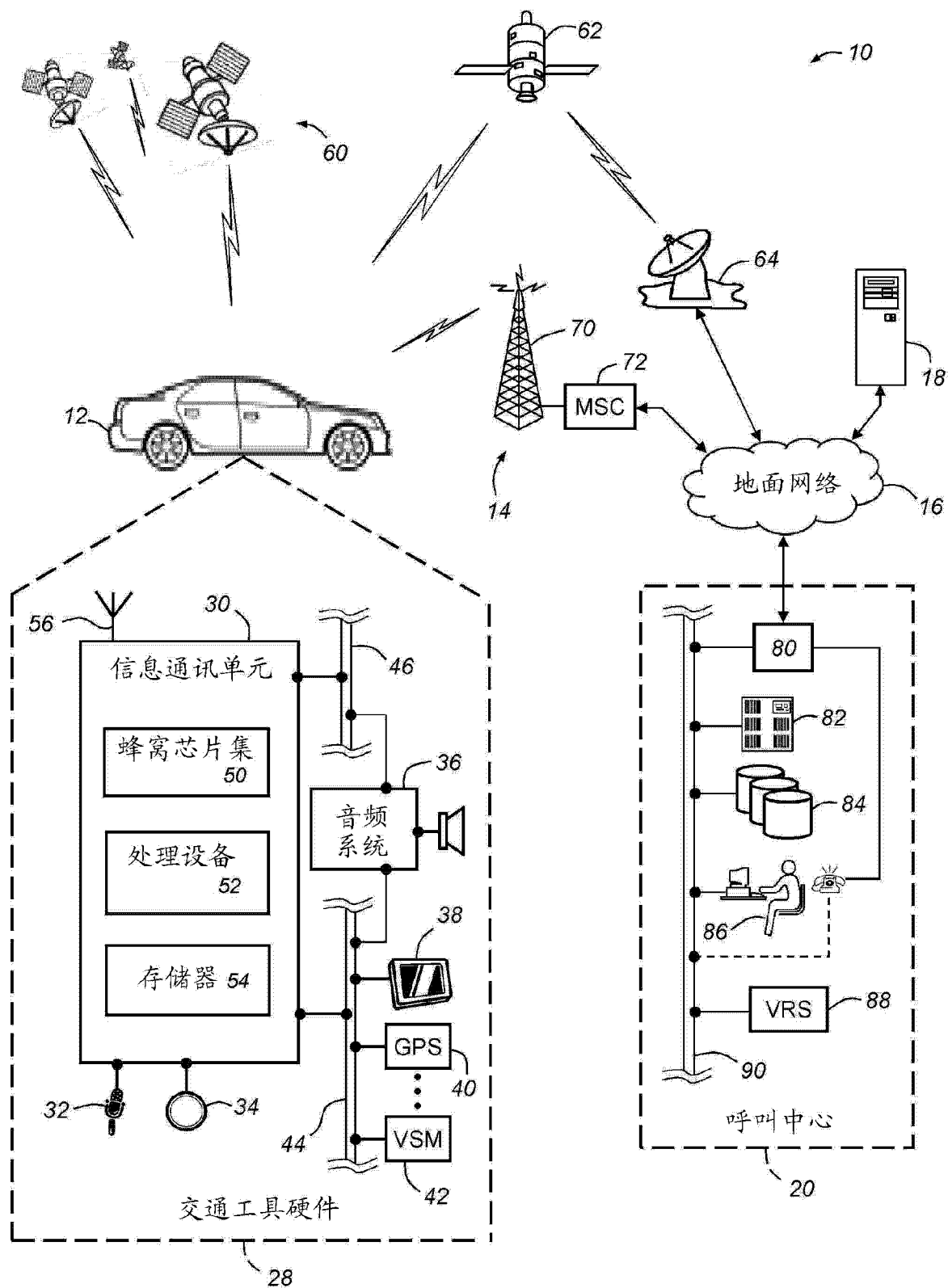


图 1

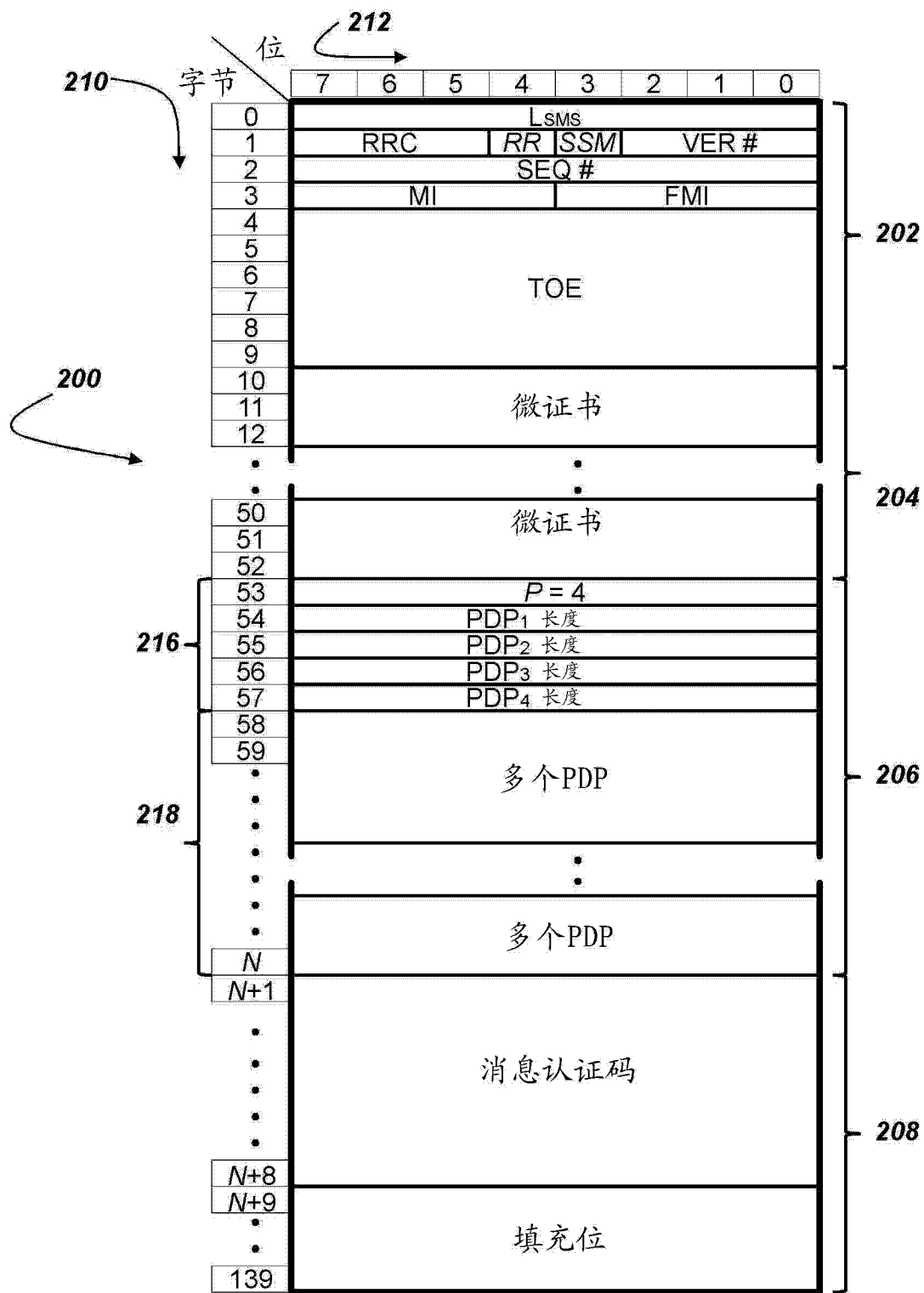


图 2A

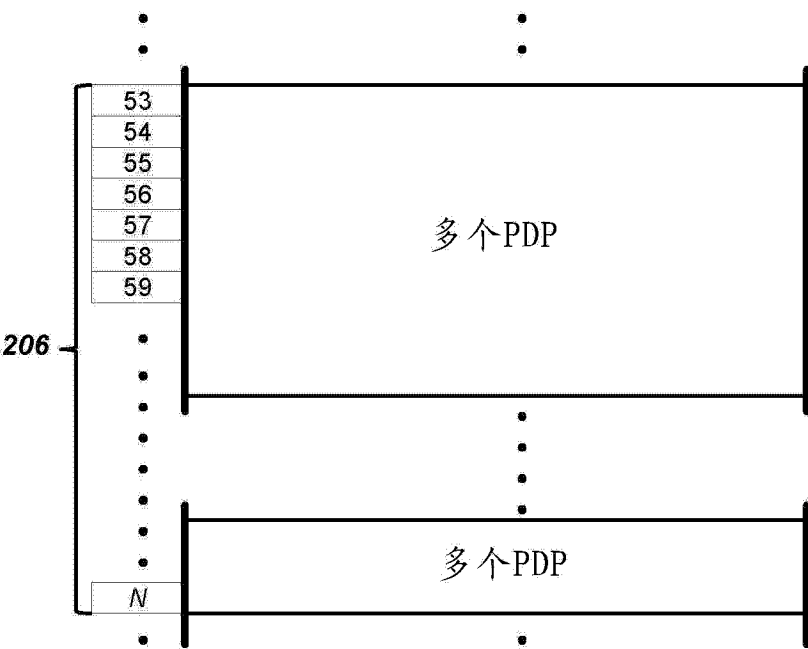


图 2B

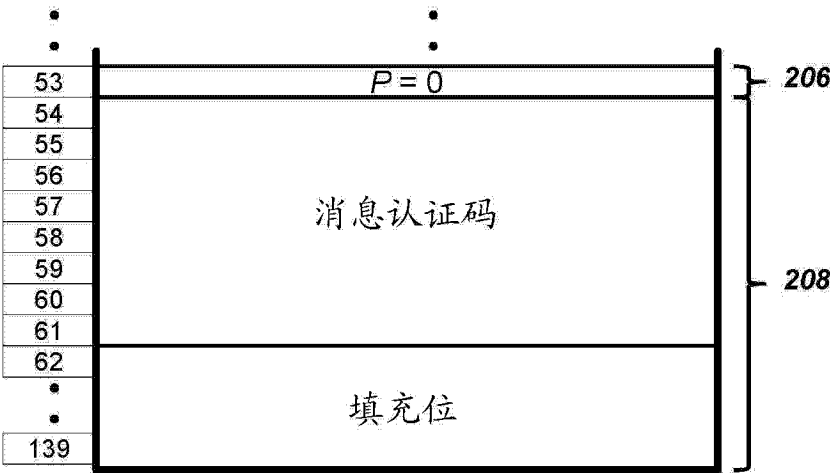


图 2C

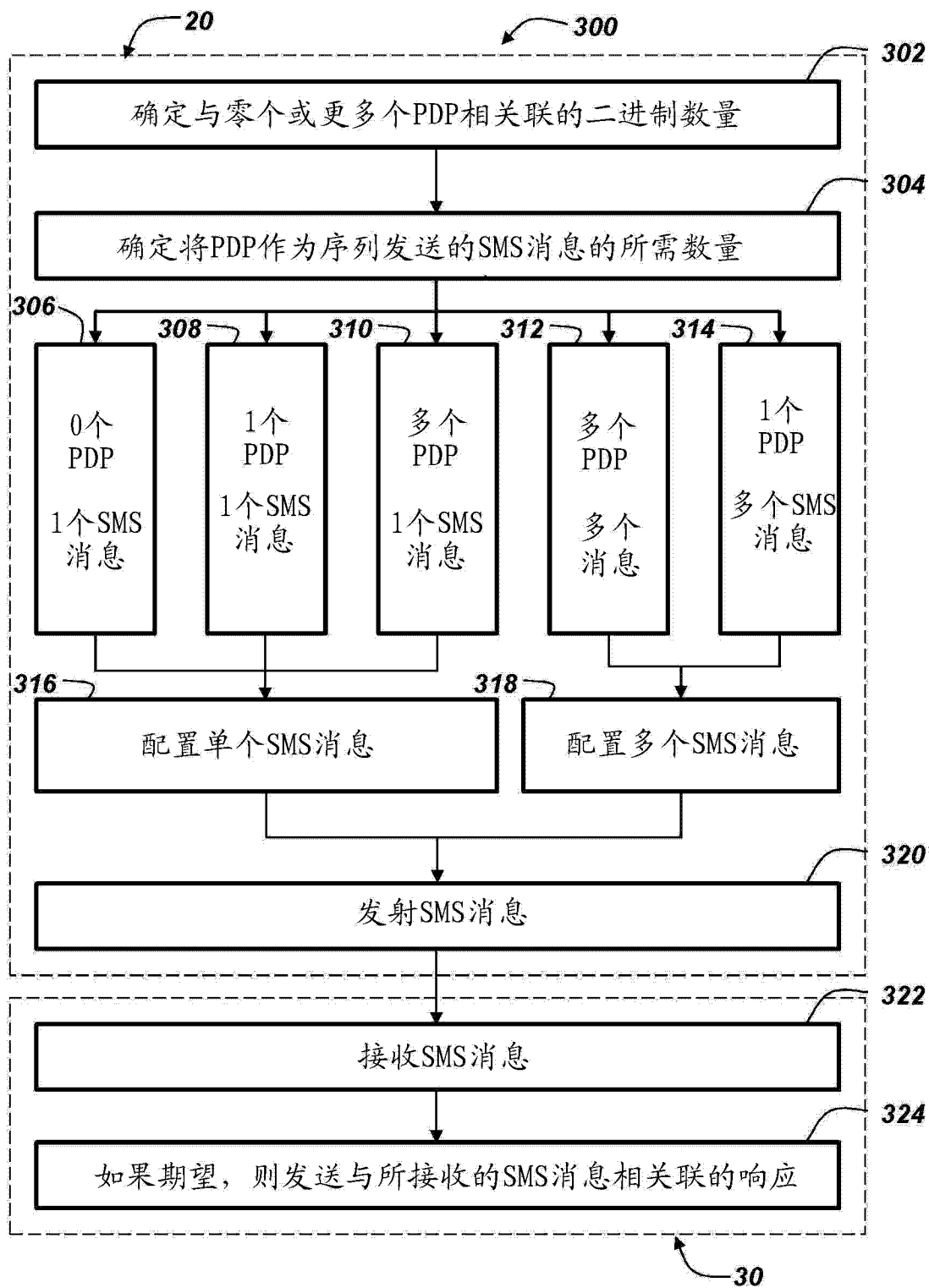


图 3

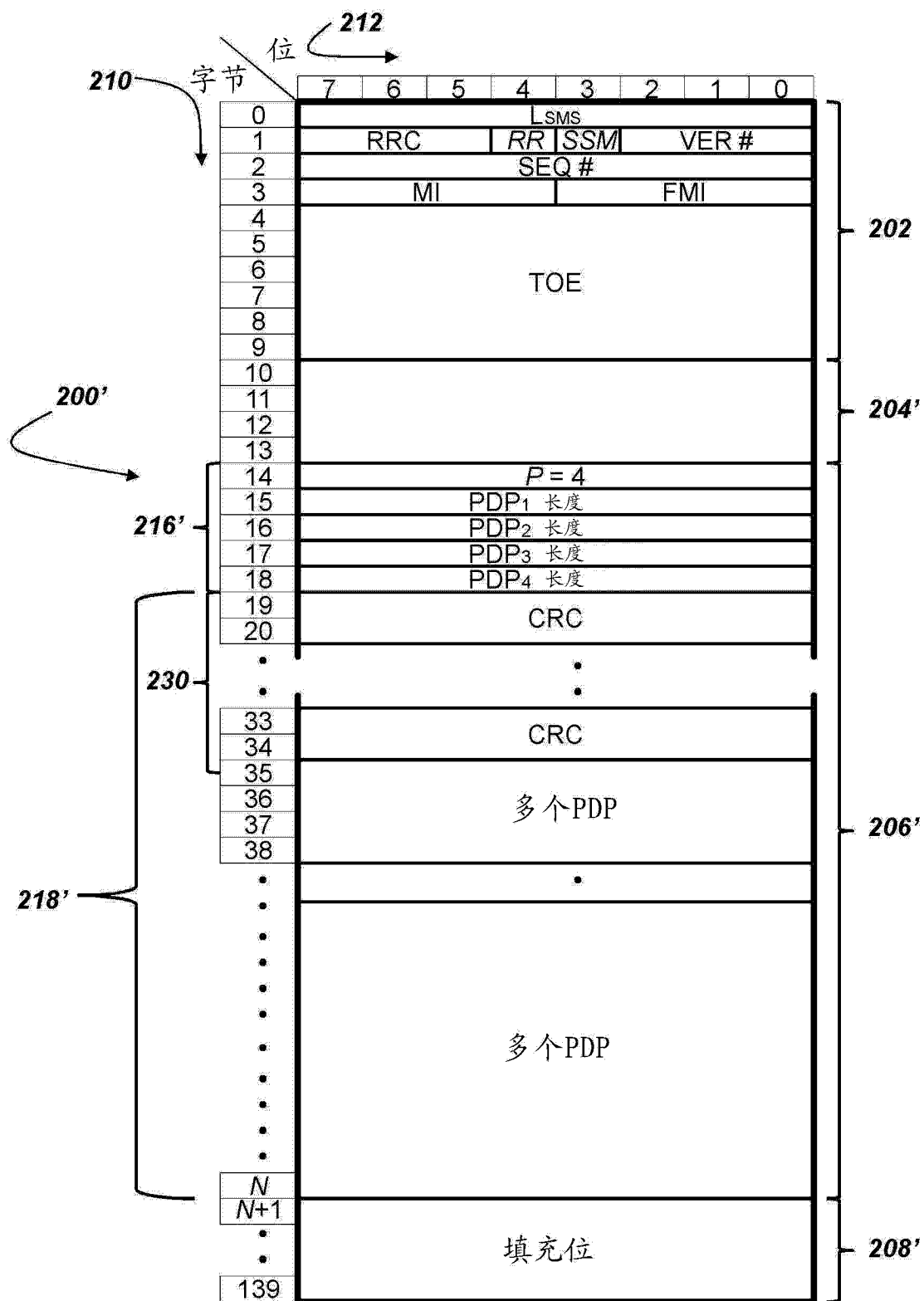


图 4