(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 104581732 B
(45)授权公告日 2019.04.05

(21)申请号 201410828720.7

(22)申请日 2014.12.25

(65)同一申请的已公布的文献号
申请公布号 CN 104581732 A

(43)申请公布日 2015.04.29

(73)专利权人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 朱大立 庞娜 范哲铭

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 李相雨

(51)Int.Cl.
H04W 12/12(2009.01)

(56)对比文件
CN 103796241 A,2014.05.14,
CN 103906116 A,2014.07.02,
CN 104244254 A,2014.12.24,
US 2012184245 A1,2012.07.19,

审查员 叶鼎晟

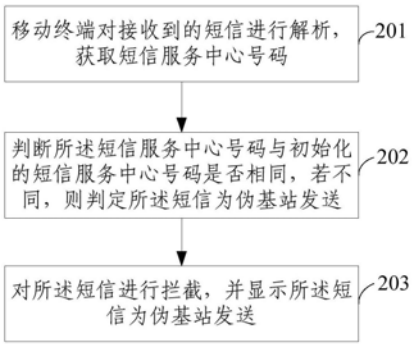
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种基于短信的伪基站实时判别方法及系统

(57)摘要

本发明提供了一种基于短信的伪基站实时判别方法，所述方法包括：移动终端对接收到的短信进行解析，获取短信服务中心号码；判断所述短信服务中心号码与初始化的短信服务中心号码是否相同，若不同，则判定所述短信的为伪基站发送；对所述短信进行拦截，并显示所述短信为伪基站发送的短信。本发明还提供了一种基于短信的伪基站实时判别系统，该系统包括解析模块、判定模块及拦截模块。本发明能够对伪基站短信进行实时拦截，有效地防止隐私泄露。



CN 104581732 B

1.一种基于短信的伪基站实时判别方法,其特征在于,所述方法包括:

移动终端向客服发送任意字符的短信;

当收到自动回复短信后,获取所述短信的协议数据单元PDU格式的十六进制字符串;

对所述字符串以字节为单位进行高低半字节换位,解析出所述短信中的短信息中心号码,得到初始化的短信息中心号码;

判断移动终端是否换卡或跨市区,若是,重新向客服发送任意字符短信,否则,对移动终端进行实时监测;

移动终端对接收到的短信进行解析,获取短信服务中心号码;

判断所述短信服务中心号码与初始化的短信服务中心号码是否相同,若不同,则判定所述短信的为伪基站发送;

对所述短信进行拦截,并显示所述短信为伪基站发送的短信;

将所述伪基站的经纬度上报至路测系统;所述经纬度由所述伪基站发送的短信解析得到;

根据路测系统中伪基站存在的概率,绘制伪基站概率分布图;采用无线电侧向定位技术,对所述伪基站概率分布图中伪基站密集的地方进行定位查处。

2.根据权利要求1所述的方法,其特征在于,所述移动终端对接收到的短信进行解析,获取短信服务中心号码,包括:

移动终端接收到短信后,获取PDU格式的十六进制字符串短信;

对所述十六进制字符串短信以字节为单位进行高低半字节换位,解析出所述短信中的短信服务中心号码。

3.根据权利要求2所述的方法,其特征在于,所述PDU格式的十六进制字符串包括发送者号码、短信服务中心号码、短信息长度、短信息发送内容及主叫号码类型。

4.一种基于短信的伪基站实时判别系统,其特征在于,所述系统包括:

初始化模块,用于向客服发送任意字符的短信,当收到自动回复短信后,获取所述短信的PDU格式的十六进制字符串,对所述字符串以字节为单位进行高低半字节换位,解析出所述短信中的短信息中心号码,得到初始化的短信息中心号码,判断移动终端是否换卡或跨市区,若是,重新向客服发送任意字符短信,否则,对移动终端进行实时监测;

解析模块,用于对接收到的短信进行解析,获取短信服务中心号码;

判定模块,用于判断所述短信服务中心号码与初始化的短信服务中心号码是否相同,若不同,则判定所述短信的为伪基站发送;

拦截模块,用于对所述短信进行拦截,并显示所述短信为伪基站发送的短信;

定位模块,用于将所述伪基站的经纬度上报至路测系统;所述经纬度由所述伪基站发送的短信解析得到,根据路测系统中伪基站存在的概率,绘制伪基站概率分布图,采用无线电侧向定位技术,对所述伪基站概率分布图中伪基站密集的地方进行定位查处。

5.根据权利要求4所述的系统,其特征在于,所述解析模块,具体用于:

接收到短信后,获取PDU格式的十六进制字符串短信;

对所述十六进制字符串短信以字节为单位进行高低半字节换位,解析出所述短信中的短信服务中心号码。

6.根据权利要求4所述的系统,其特征在于,所述PDU格式的十六进制字符串包括发送

者号码、短信服务中心号码、短信息长度、短信息发送内容及主叫号码类型。

一种基于短信的伪基站实时判别方法及系统

技术领域

[0001] 本发明涉及通信技术领域，具体涉及一种基于短信的伪基站实时判别方法及系统。

背景技术

[0002] 在蜂窝移动通信系统中，当移动终端选择一个新的公用陆地移动网(Pubilc Land Mobile Network，简称PLMN)后，会尝试驻留在下行链路解码可靠且上行链路通信质量良好的小区，以便移动终端接收到该PLMN的寻呼信息以及系统信息并且可以和此小区建立呼叫过程等行为。同时监测可重选邻区频点的广播控制信道(Broadcast Control CHannel，简称BCCH)载波，伪基站通过设置BCCH载波为某个邻区的BCCH，增大发射信号强度使得目标区域的移动终端接收到伪基站信令重选到伪基站上。伪基站是移动通信网络之外的非法小区，为了提取移动终端信息或与其进行信息传递伪装成公共移动通信运营商基站的无线电收发信电台，利用一个信号比运营商基站的强的小型便携的基站，利用相同的电磁波频率，覆盖了真正运营商的信号，非法占用频谱资源发送大量垃圾短信给人民群众的生活造成严重危害。

[0003] 现有伪基站判定方法有：一是当终端接收短信后，根据关键字和手机号判断是否为垃圾短信，若是，则立即触发短信或语音业务，若网络不通，就判断此处为伪基站疑似覆盖区，再由终端的GPS芯片记录此处的经纬度，待网络覆盖恢复时，将疑似伪基站覆盖位置上传基站，再通过路测工具绘制伪基站覆盖区域；二是在提供合法基站的信息数据库的基础上，利用手机客服端获取基站信息，在合法基站信息数据库中查询手机客户端获取的基站信息，若无法查询到手机客户端获取的基站信息，判断该基站为伪基站；若查询到该基站信息，将该基站在数据库中查询到的地理位置信息与定位到的所述手机客户端的地理位置信息进行比较，若查询到的基站地理位置与定位到的所述手机客户端的地理位置差距超过预定距离，则判定该基站为伪基站。

[0004] 上述方法中虽然从不同方面对伪基站进行了研究，但它们局限到用户收到垃圾短消息之后对消息内容的分析，或者通过查询数据库对比地理位置，但是测试结果显示基站地理位置很模糊，不能清晰得定位经纬度，即便是正常基站，也不能准确的定位到基站具体地点，手机客户端的地理位置也必须打开定位服务数据数据访问才可以获得，这种方法级部准确也要消耗很大的流量资源、以及消耗很大的手机电量。所以这些方法所能应对的安全威胁范围比较窄。无法手动短息主动判定伪基站的存在以便及时对伪基站发送的短消息进行拦截。目前对于伪基站的嗅探主要是基于用户受骗后的投诉然后根据路测系统进行追踪，但用户投诉具有时间延误，因此增加了定位追踪的工作量。

发明内容

[0005] 针对现有技术的缺陷，本发明提供一种基于短信的伪基站实时判别方法及系统，通过解析PDU短信息来实时判断伪基站的存在，并对伪基站短信进行实时拦截，能够有效地

防止隐私泄露。

[0006] 第一方面，本发明提供了一种基于短信的伪基站实时判别方法，所述方法包括：

[0007] 移动终端对接收到的短信进行解析，获取短信服务中心号码；

[0008] 判断所述短信服务中心号码与初始化的短信服务中心号码是否相同，若不同，则判定所述短信的为伪基站发送；

[0009] 对所述短信进行拦截，并显示所述短信为伪基站发送的短信。

[0010] 优选地，所述对所述短信进行拦截，并显示所述短信为伪基站发送的短信的步骤后，该方法还包括：

[0011] 将所述伪基站的经纬度上报至路测系统；所述经纬度由所述伪基站发送的短信解析得到；

[0012] 根据路测系统中伪基站存在的概率，绘制伪基站概率分布图；

[0013] 采用无线电侧向定位技术，对所述伪基站概率分布图中伪基站密集的地方进行定位查处。

[0014] 优选地，所述移动终端对接收到的短信进行解析，获取短信服务中心号码的步骤前，该方法还包括：

[0015] 移动终端向客服发送任意字符的短信；

[0016] 当收到自动回复短信后，获取所述短信的PDU格式的十六进制字符串；

[0017] 对所述字符串以字节为单位进行高低半字节换位，解析出所述短信中的短信息中心号码，得到初始化的短信息中心号码。

[0018] 优选地，所述移动终端对接收到的短信进行解析，获取短信服务中心号码，包括：

[0019] 移动终端接收到短信后，获取PDU格式的十六进制字符串短信；

[0020] 对所述十六进制字符串短信以字节为单位进行高低半字节换位，解析出所述短信中的短信服务中心号码。

[0021] 优选地，所述PDU格式的十六进制字符串包括发送者号码、短信服务中心号码、短信息长度、短信息发送内容及主叫号码类型。

[0022] 第二方面，本发明提供了一种基于短信的伪基站实时判别系统，所述系统包括：

[0023] 解析模块，用于对接收到的短信进行解析，获取短信服务中心号码；

[0024] 判定模块，用于判断所述短信服务中心号码与初始化的短信服务中心号码是否相同，若不同，则判定所述短信的为伪基站发送；

[0025] 拦截模块，用于对所述短信进行拦截，并显示所述短信为伪基站发送的短信。

[0026] 优选地，所述系统还包括定位模块，具体用于：

[0027] 将所述伪基站的经纬度上报至路测系统；所述经纬度由所述伪基站发送的短信解析得到；

[0028] 根据路测系统中伪基站存在的概率，绘制伪基站概率分布图；

[0029] 采用无线电侧向定位技术，对所述伪基站概率分布图中伪基站密集的地方进行定位查处。

[0030] 优选地，所述系统还包括初始化模块，具体用于：

[0031] 向客服发送任意字符的短信；

[0032] 当收到自动回复短信后，获取所述短信的PDU格式的十六进制字符串；

[0033] 对所述字符串以字节为单位进行高低半字节换位，解析出所述短信中的短信息中心号码，得到初始化的短信息中心号码。

[0034] 优选地，所述解析模块，具体用于：

[0035] 接收到短信后，获取PDU格式的十六进制字符串短信；

[0036] 对所述十六进制字符串短信以字节为单位进行高低半字节换位，解析出所述短信中的短信服务中心号码。

[0037] 优选地，所述PDU格式的十六进制字符串包括发送者号码、短信服务中心号码、短信息长度、短信息发送内容及主叫号码类型。

[0038] 由上述技术方案可知，本发明提供一种基于短信的伪基站实时判别方法及系统，通过解析PDU短信息来实时判断伪基站的存在，并对伪基站短信进行实时拦截，能够有效地防止隐私泄露。

附图说明

[0039] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些图获得其他的附图。

[0040] 图1是伪基站系统结构；

[0041] 图2是本发明一实施例提供的一种基于短信的伪基站实时判别方法的流程示意图；

[0042] 图3是本发明另一实施例提供的一种基于短信的伪基站实时判别方法初始化的流程示意图；

[0043] 图4是本发明一实施例提供的一种基于短信的伪基站实时判别系统的结构示意图。

具体实施方式

[0044] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0045] 伪基站系统结构如图1所示，主要由基站系统和操控平台组成，基站系统又由基站单元(Base Station Subsystem，简称BSS)和移动业务交换中心(Mobile Switching Center，简称MSC)组成。系统仿制正常合法基站向移动终端提供空口接入，没有连接运营商网络。

[0046] 伪基站的运行流程如下：

[0047] 一、监听与伪装：

[0048] (1)工程机获取邻小区BCCH频率。

[0049] (2)工程机选定BCCH信号最弱的小区频率。

[0050] (3)伪基站设置相同移动国家码(Mobile Country Code，简称MCC)和移动网络号

码(Mobile Network Code,简称MNC),增大功率发射伪装后的BCCH信号。

[0051] 二、将手机吸入伪基站:

[0052] (1)伪基站通过增大发射强度,发射伪装后的BCCH信号,手机进行小区选择。

[0053] (2)伪基站要求手机鉴权,在手机反馈后,直接确认反馈成功。

[0054] (3)伪基站通过BCCH广播设置位置区码(Location Area Code,简称LAC)值,手机识别LAC发生变化后立即出发位置更新请求。

[0055] (4)伪基站向手机发送识别请求认证,获取手机临时识别码(Temporary Mobile Subscriber Identity,简称TMSI)、国际移动用户识别码(International Mobile Subscriber Identification number,简称IMSI)及移动设备国际身份码(International Mobile Equipment Identity,简称IMEI)。

[0056] 三、发送短消息过程:

[0057] (1)根据用户IMSI判断是否已经发送短信息。

[0058] (2)若没有,则设置主叫号码,在独立专用控制信道(Stand-Alone Dedicated Control CHannel,简称SDCCH)发送短消息。

[0059] 四、剔除手机过程:

[0060] (1)伪基站更新LAC被手机识别到,触发了手机的位置更新请求。

[0061] (2)伪基站通过IMSI判断是否已发短消息,如果没有发送,启动发送短消息过程,若果已经发送,伪基站拒绝位置更新。

[0062] (3)手机小区进行重选,接入正常基站。

[0063] 接收短消息实质上就是从客户识别模块(Subscriber Identity Module,简称SIM)或缓存中读出消息。这主要利用AT+CMGR和AT+CMGL两条指令来完成,由于无线模块不同的厂商对AT指令集的解释代码和响应消息不一样,所以首先要确认能否与MODEM建立起通信,一般用AT指令完成此确认;然后用AT+CMGF指令选定短消息的数据格式;在收到MODEM的正确回答后以AT指令完成读出功能。一般用AT+CMGL读取以前的信息,在收到MODEM的Ring(振铃)数据时,用AT+CMGR读取实时信息。以下是用H6221—W的接收SMS的一个实例,它说明了协议数据单元(Protocol Data Unit,简称PDU)模式的应用。操作过程如下({}内为注释):

[0064] 发送:AT

[0065] 回答:OK{已建立连接}

[0066] 发送:AT+CMGF=0{选用PDU格式}

[0067] 回答:OK{允许选用PDU格式}

[0068] 发送:AT+CMGF=0、2{列出已有的短信息}

[0069] 回答:+CMGL:1,2,,,,24{1表示信息个数,2表示未发信息,24表示信息总容量}

[0070] 以下为获取的PDU格式的十六进制字符串:0D91683108370105F0040B8131791332
08F1000002608041003380263218 4CF682D95E30DC2B36D3D170A0243106933D97A02451068B
1983492608

[0071] 如图2所示,为本发明一实施例提供的一种基于短信的伪基站实时判别方法的流程示意图,该方法包括如下步骤:

[0072] 201、移动终端对接收到的短信进行解析,获取短信服务中心号码。

[0073] 202、判断所述短信服务中心号码与初始化的短信服务中心号码是否相同，若不同，则判定所述短信的为伪基站发送。

[0074] 进一步地，若所述短信服务中心号码与初始化的短信服务中心号码是相同的，则判定该短信为正常短信。

[0075] 203、对所述短信进行拦截，并显示所述短信为伪基站发送的短信。

[0076] 本实施例中，步骤203后，该方法还包括：

[0077] 将所述伪基站的经纬度上报至路测系统；所述经纬度由所述伪基站发送的短信解析得到；

[0078] 根据路测系统中伪基站存在的概率，绘制伪基站概率分布图；

[0079] 采用无线电侧向定位技术，对所述伪基站概率分布图中伪基站密集的地方进行定位查处。

[0080] 本实施例中，步骤201之前，该方法还包括初始化过程，如图3所示，初始化过程具体包括如下步骤：

[0081] 301、移动终端向客服发送任意字符的短信。

[0082] 举例来说，移动号码向10086发送任意字符的短信，联通号码向10010发送任意字符的短信，而电信用户，由于中国电信不是全球移动通信系统(Global System for Mobile Communication，简称GSM)制式，不对其进行伪基站监测。

[0083] 302、当收到自动回复短信后，获取所述短信的PDU格式的十六进制字符串。

[0084] 303、对所述字符串以字节为单位进行高低半字节换位，解析出所述短信中的短信息中心号码，得到初始化的短信息中心号码。

[0085] 304、判断移动终端是否换卡或跨市区，若是，则转至步骤301，否则转至步骤305。

[0086] 305、对移动终端进行实时监测。

[0087] 上述初始化过程，只需要用户在开启此应用后，第一次点击“发送短信至客服”。在手机没有换卡或换市区时，此伪基站监测过程不会再次开启初始化过程。

[0088] 本实施例中，步骤201，具体包括：

[0089] 移动终端接收到短信后，获取PDU格式的十六进制字符串短信；对所述十六进制字符串短信以字节为单位进行高低半字节换位，解析出所述短信中的短信服务中心号码。

[0090] 其中，所述PDU格式的十六进制字符串包括发送者号码、短信服务中心号码、短信息长度、短信息发送内容及主叫号码类型等。

[0091] 本实施例提供的一种基于短信的伪基站实时判别方法，通过解析PDU短信息来实时判断伪基站的存在，并对伪基站短信进行实时拦截，能够有效地防止隐私泄露。

[0092] 如图4所示，为本发明一实施例提供的一种基于短信的伪基站实时判别系统的结构示意图，该系统包括解析模块401、判定模块402及拦截模块403。

[0093] 其中，解析模块401，用于对接收到的短信进行解析，获取短信服务中心号码。

[0094] 判定模块402，用于判断所述短信服务中心号码与初始化的短信服务中心号码是否相同，若不同，则判定所述短信的为伪基站发送。

[0095] 拦截模块403，用于对所述短信进行拦截，并显示所述短信为伪基站发送的短信。

[0096] 可选地，所述系统还包括定位模块，具体用于：

[0097] 将所述伪基站的经纬度上报至路测系统；根据路测系统中伪基站存在的概率，绘

制伪基站概率分布图;采用无线电侧向定位技术,对所述伪基站概率分布图中伪基站密集的地方进行定位查处。

[0098] 可选地,所述系统还包括初始化模块,具体用于:

[0099] 向客服发送任意字符的短信;当收到自动回复短信后,获取所述短信的PDU格式的十六进制字符串;对所述字符串以字节为单位进行高低半字节换位,解析出所述短信中的短信息中心号码,得到初始化的短信息中心号码。

[0100] 本实施例中,解析模块401,具体用于:

[0101] 接收到短信后,获取PDU格式的十六进制字符串短信;对所述十六进制字符串短信以字节为单位进行高低半字节换位,解析出所述短信中的短信服务中心号码。

[0102] 其中,所述PDU格式的十六进制字符串包括发送者号码、短信服务中心号码、短信息长度、短信息发送内容及主叫号码类型。

[0103] 以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解;其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

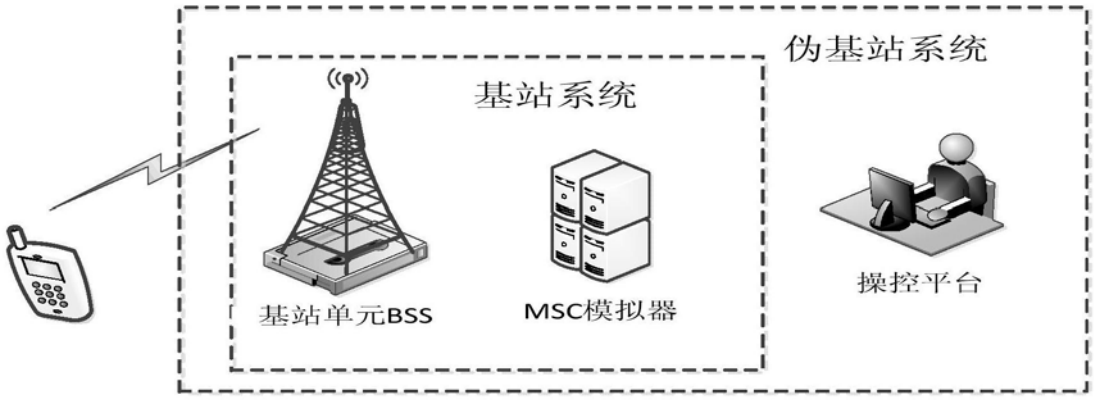

伪基站系统
基站系统
基站单元BSS
MSC模拟器
操控平台

图1

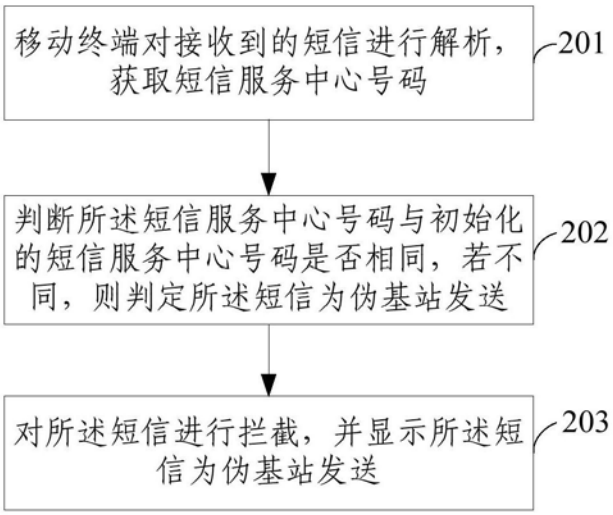

移动终端对接收到的短信进行解析，获取短信服务中心号码
201
判断所述短信服务中心号码与初始化的短信服务中心号码是否相同，若不同，则判定所述短信为伪基站发送
202
对所述短信进行拦截，并显示所述短信为伪基站发送
203

图2

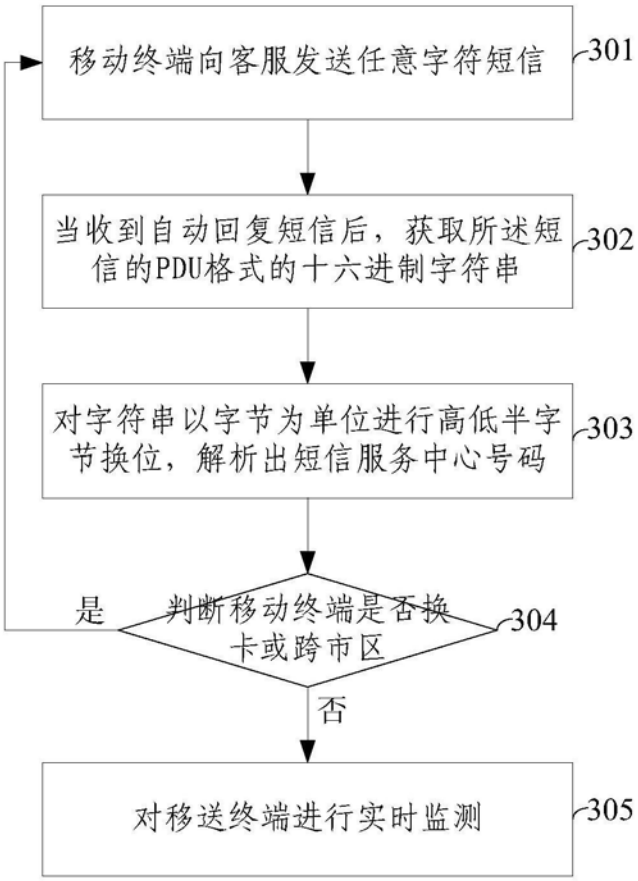

移动终端向客服发送任意字符短信
301
当收到自动回复短信后，获取所述短信的PDU格式的十六进制字符串
302
对字符串以字节为单位进行高低半字节换位，解析出短信服务中心号码
303
判断移动终端是否换卡或跨市区
304
是
否
对移送终端进行实时监测
305

图3

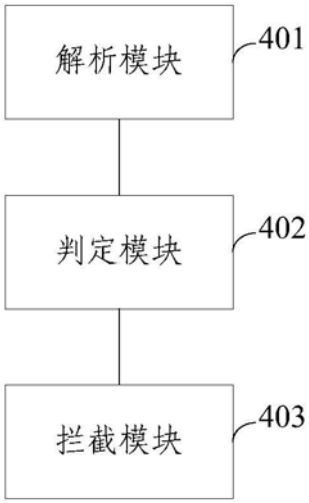

解析模块
401
判定模块
402
拦截模块
403

图4