ICS 35.100.05
L 79

YD

# 中华人民共和国通信行业标准



# 移动伪基站网络侧监测技术要求

Technical requirements for pseudo base station monitoring on network-side



2016-07-11 发布　　2016-10-01 实施

中华人民共和国工业和信息化部　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国移动通信集团公司、中国移动通信集团设计院有限公司、中国联合网络通信集团有限公司、华为技术有限公司、武汉烽火科技集团有限公司。

本标准主要起草人：张　滨、赵　刚、孟德香、杜雪涛、李祥军、朱艳云、杜　刚、刘利军、张　晨、王馨裕、张　艋、袁捷、冯运波、娄　涛、檀鹏、朱安南、陈　璟、叶　猛。

# 移动伪基站网络侧监测技术要求

## 1 范围

本标准规定了通过在GSM网络侧监测发现伪基站活动的具体技术要求，主要包括：监测的架构及流程、信令采集要求、数据处理、智能识别、预警分析、定位分析、活动规律分析、实时预警与追踪等内容。

本标准适用于对伪基站的网络侧监测。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3GPP TS 24.008 移动无线接口层3规范（Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification）

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**移动伪基站 Pseudo Basestation**

非法使用运营商的频率，假冒运营商网络，伪装成运营商基站的假基站。它利用大功率发射信号和无线参数优选设置诱骗客户手机接入，收集客户信息同时可伪造任意发送号码强行向覆盖区内的手机发送不良信息。伪基站发送垃圾短信原理及危害参见附录A。

## 4 缩略语

下列缩略语适用于本文件。

| | | |
|---|---|---|
| GSM | Global System for Mobile communication | 全球移动通信系统 |
| GIS | Geographic Information System | 地理信息系统 |
| LAC | Location Area Code | 位置区编码 |
| IMSI | International Mobile Subscriber Identification Number | 国际移动用户识别码 |
| TMSI | Temporary Mobile Subscriber Identity | 临时识别码 |
| CI | Cell Identity | 小区识别码 |
| BSC | Base station controller | 基站控制器 |
| MSC | Mobile Switch Center | 移动交换中心 |
| DT | Drive Test | 路测 |

## 5 伪基站网络侧监测概述

本标准定义的伪基站网络侧监测技术是指在 GSM 网络侧监测骚扰用户的伪基站活动，通过监测实

现对疑似伪基站活动的实时、准确预警，跟踪伪基站的影响程度和范围，并快速定位伪基站的位置，实时监控其动态。

## 5.1 伪基站网络侧监测架构

伪基站网络侧监测是通过从GSM网络的BSC和MSC之间获取LAC位置更新相关信令，从外部获取包括网络工程参数表、网络邻区关系表等基础数据，结合基础数据及信令进行位置更新异常分析发现伪基站活动，并进行实时预警及定位（网络侧可监测到的异常LAC信号参见附录B）。伪基站网络侧监测的位置如图1所示。

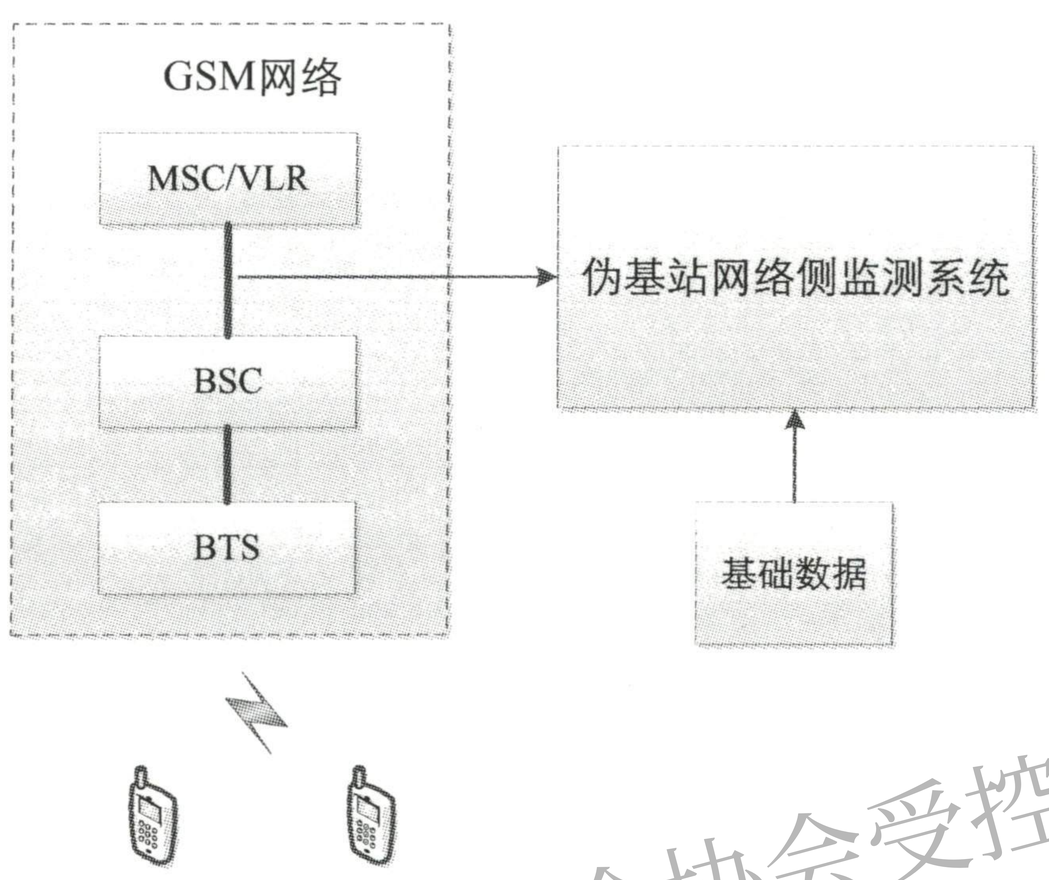


**图 1 伪基站网络侧监测系统位置**

伪基站网络侧监测系统架构如图2所示。伪基站网络侧监测系统由三个功能模块构成：数据采集模块、数据处理与分析模块、实时预警与追踪模块。

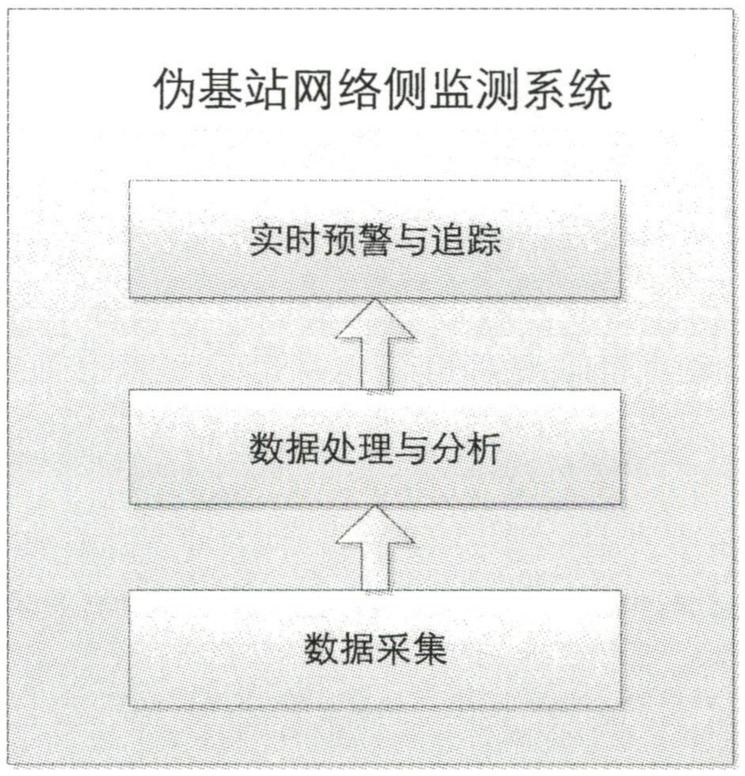


**图 2 伪基站网络侧监测系统架构**

数据采集模块从现网获取信令并合成指定LAC话单；数据处理与分析对不断更新的LAC话单进行实时处理与分析；实时预警与追踪实现对伪基站活动的实时预警和定位追踪。

## 5.2 伪基站网络侧监测流程

伪基站网络侧监测流程如图3所示。

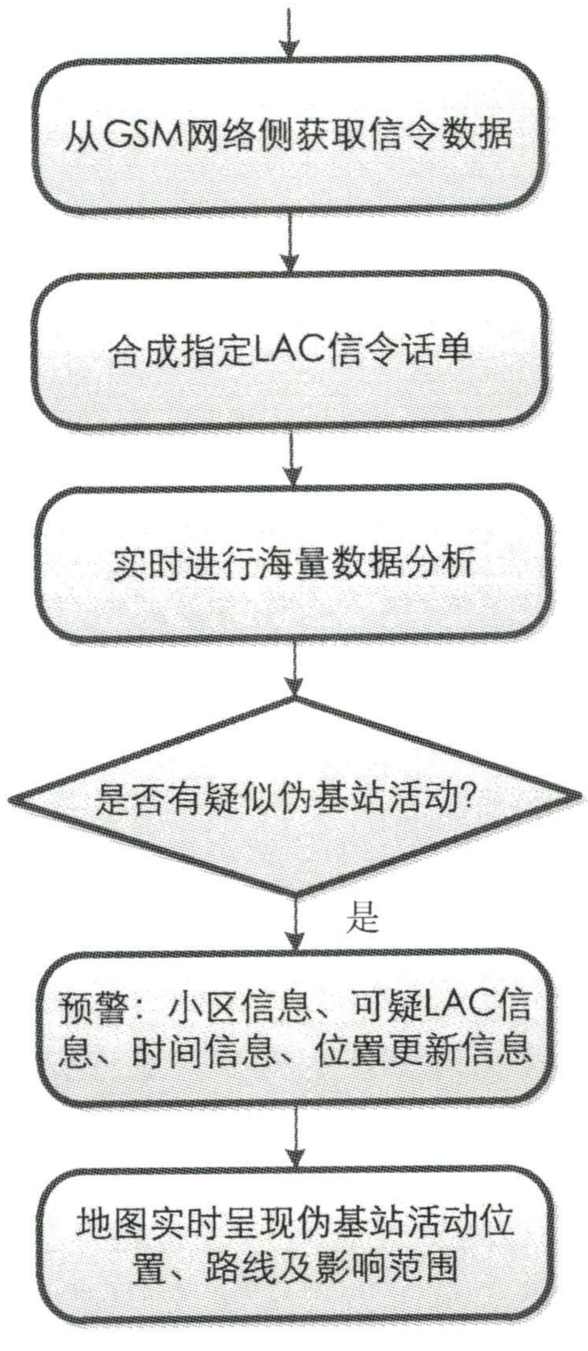


**图 3　伪基站网络侧监测流程**

伪基站网络侧监测的流程步骤如下：

a）伪基站网络侧监测系统从 GSM 网络 BSC 和 MSC 之间不断获取 LAC 位置更新相关信令；

b）对信令数据进行 LAC 话单合成处理；

c）以小区为单位，对海量的话单数据进行实时分析判断是否有异常情况；

d）若发现有疑似伪基站活动，则进行实时预警，综合呈现出各种预警信息：小区信息、可疑 lAC 信息、时间信息、位置更新信息等；

e）同时结合 GIS 地图信息，分析及呈现出伪基站的活动位置、影响范围及活动路线。

## 6　伪基站网络侧监测技术要求

### 6.1　数据采集

#### 6.1.1　（准）实时信令采集

（准）实时信令采集能够从GSM网络BSC和MSC之间获取位置更新相关的信令，并自动合成指定LAC话单。

LAC话单应包括如下字段：

——开始时间；

——结束时间（可选）；

——源 LAC；

——目的 LAC；

——目的 CI；

——位置更新类型：

- 正常位置更新；
- 周期性位置更新；
- IMSI 附着。

——位置更新执行结果：

- 成功；
- 失败。

——TMSI（可选）；

——IMSI（可选）。

为最大程度上确保疑似伪基站活动预警的实时性，LAC话单的更新周期应在20s~5min之间，建议为1min。

信令采集也可以利用现有平台，如现网的信令监测平台（或协议处理机或信令采集系统）。

### 6.1.2 基础数据采集

伪基站网络侧监测系统需要从外部获取基础数据，基础数据包括网络工程参数表、网络邻区关系表，用于辅助伪基站活动的分析及实时预警与追踪的呈现。

#### 6.1.2.1 网络工程参数表

网络工程参数表提供了小区的物理参数信息。对于移动伪基站网络侧监测系统监控到的小区，应提供如下字段：

——小区中文名称。

——LAC。

——CI。

——经度。

——纬度。

——区县。

——小区类型：

- 2G；
- 3G；
- 4G。

——所属 BSC（可选）。

——所属 MSC（可选）。

对于网络工程参数表应当不定期更新。

#### 6.1.2.2 网络邻区关系表

网络邻区关系表提供了小区的邻区关系信息。对于移动伪基站网络侧监测系统监控到的小区，应至少提供如下字段：

——小区中文名称；

——LAC；

——CI；

——邻小区 CI；

——邻小区 LAC；

——邻小区名称。

上述网络工程参数应当不定期更新。

### 6.2 数据处理与分析

#### 6.2.1 数据处理

数据处理需对获取的LAC话单以小区为单位按照指定周期进行快速聚合与快速入库，确保实时预警数据的时效性。

#### 6.2.2 智能识别

监测系统能够按照一定的规则对每个小区进行位置更新次数的分析，以能够发现并为各小区设置独立合理的预警门限，提高预警准确性。

智能识别的对象可选择：

——小区位置更新次数的总数：迁入到该小区的位置更新总次数；

——小区位置更新的分 LAC 次数：每个 LAC 号迁入到该小区的位置更新次数。

智能识别的结果可选择：

——最大值；

——均值。

智能识别需考虑的因素包括：

——不同时段：以小时为单位，一天 24 个时段。

——小区所处本 LAC 的位置：

- LAC 边缘区；
- LAC 非边缘区。

#### 6.2.3 预警分析

预警分析能够对获取的数据进行实时分析，发现存在疑似伪基站活动的小区。预警分析中应考虑如下因素：

——网络工程参数表；

——网络邻区关系表；

——智能识别结果。

应能够在收到LAC话单后，在指定时间（建议20s~2min），内完成疑似伪基站活动的预警，预警以受影响的小区为单位产生。

为保证预警信息的全面性，预警分析能够支持以下功能：

——能够分析出位置更新异常的小区；

——能够分析出位置更新异常的 LAC 号；

——能够分析出未知 LAC 号；

——能够分析出疑似伪基站活动起止时间。

预警分析要以指定的周期（可配置，建议20s~5min）持续进行，为保证实时性，建议尽量采用较短的时间周期。

### 6.2.4 定位分析

定位分析能够网络侧实时监测结果，结合GIS引擎、网络工程参数表、网络邻区关系表，快速定位疑似伪基站的位置。

定位分析能够支持以下功能：

——能够分析出哪些小区受同一伪基站影响；

——能够分析出小区受伪基站影响的程度；

——能够分析出伪基站位置；

——结合 GIS 系统，自动调用相关地区地图，在地图上标注出伪基站的位置。

定位分析应能够能够精确到街区级，要求每20s~5min之间（默认1min）定位一次，定位精度在200m～500m之间，以便为后续的现场侦测提供有利的引导。

在定位分析中，为提高准确度，应考虑如下因素：

——小区受影响程度；

——受影响小区地理位置；

——小区间的距离；

——GIS 图层中的道路信息。

### 6.2.5 活动规律分析

活动规律能够通过挖掘历史数据，分析出伪基站的活动规律。分析结果包括但不限于：

——各时段告警次数：以小时为单位，统计一天 24h 内各时段的告警总次数；

——各区域告警次数：

- 以小时为单位，统计各区域内的告警次数；
- 以天为单位，统计各区域内的告警次数。

——告警时长 TOPN 小区：

- 以天为单位，统计出告警时长排名位于前 *N* 位的小区；
- 以周为单位，统计出告警时长排名位于前 *N* 位的小区。

——告警次数 TOPN 小区：

- 以天为单位，统计出告警次数排名位于前 *N* 位的小区；
- 以周为单位，统计出告警次数排名位于前 *N* 位的小区。

——受影响程度较深 TOPN 小区：

- 以天为单位，统计出受影响程度排名位于前 *N* 位的小区；
- 以周为单位，统计出受影响程度排名位于前 *N* 位的小区。

——伪基站活动高发时段：

- 以一天为分析周期，分析一天之中告警时长长、告警次数多、对小区影响较为严重的时间段；
- 以一周为分析周期，分析一天之中告警时长长、告警次数多、对小区影响较为严重的时间段。

——伪基站活动高发区域：

- 以一天为分析周期，分析伪基站出现较多的区域；
- 以一周为分析周期，分析伪基站出现较多的区域。

——伪基站活动高发路线：

- 以一天为分析周期，分析伪基站出现较多的道路；
- 以一周为分析周期，分析伪基站出现较多的道路。

## 6.3 实时预警与追踪

### 6.3.1 实时预警

实时预警能够对存在疑似伪基站活动的小区进行实时告警，告警信息应至少包括：

——小区名称；

——可疑 LAC 号；

——开始时间；

——当前更新频次；

——未知 LAC 号；

——持续时长。

还可以提供更多的辅助信息，如下：

——小区 ID；

——结束时间；

——更新频次阈值；

——异常级别。

为提高预警信息的直观性和友好性，实时预警还应支持以下功能：

a）能够直观标识不同的告警状态。告警状态分为：

——未结束；

——已结束。

b）能够直观标识不同的 LAC 号使用情况。LAC 号使用情况包括：

——现网在用；

——现网未使用。

c）能够直观动态显示告警信息中小区的位置更新频次情况，并进行实时更新。如以柱状图形式显示出当前时间点之前 30min 的小区位置更新频次。

d）能够在动态图中直观标识不同位置更新频次状态。位置更新频次状态可按照设定规则进行判定，包括：

——异常状态；

——正常状态。

e）能够显示同一小区中所有 LAC 的位置更新频次情况。并能够标识不同的 LAC 号情况。

实时预警能够按照指定的周期（可配置，默认1min），对告警信息进行更新。



### 6.3.2 定位追踪

定位追踪应能够将伪基站的位置、影响范围以及伪基站的历史路线在地图上呈现出来，以便用户更直观的观测到伪基站的情况。对伪基站进行现场定位的作业方法可参考附录C。

定位追踪应：

a）能够标识出伪基站当前的位置；

b）能够标识出伪基站的影响范围；

c）能够标识出受影响小区的异常程度；

d）能够呈现出指定时间段内（如 30min）伪基站的历史轨迹；

e）能够按照城市/区域/小区的范围在地图上呈现伪基站总体情况；

f）能够按照城市/区域的范围呈现受伪基站影响小区的列表；

g）支持地图的缩放功能，当选中受伪基站影响的小区时，能够以小区为中心点进行缩放；

h）在选择受伪基站影响小区时，能够关联该小区的预警相关信息；

i）能够显示指定区域内所有小区分布情况。

# 附　录　A
（资料性附录）
# 移动伪基站原理及危害

## A.1　伪基站发送垃圾短信原理

伪基站通常在人员密集区域部署，通过假冒运营商网号等方式，迫使覆盖区域的手机用户从正常的运营商网络切换到伪基站网络,然后通过模拟网络信令，伪造短信并下发给用户。

以某运营商网络为例，现有2G/3G网络采用单向鉴权认证，即手机不鉴权网络的合法性，仅在网络侧对手机进行鉴权，导致手机无法有效辨别基站的真伪。

伪基站设置某运营商网号，使用该运营商GSM频段，并设置更优的小区重选参数；当手机进入伪基站覆盖区域时，很容易通过位置更新切换到伪基站小区。其基本示意图如图A.1所示。

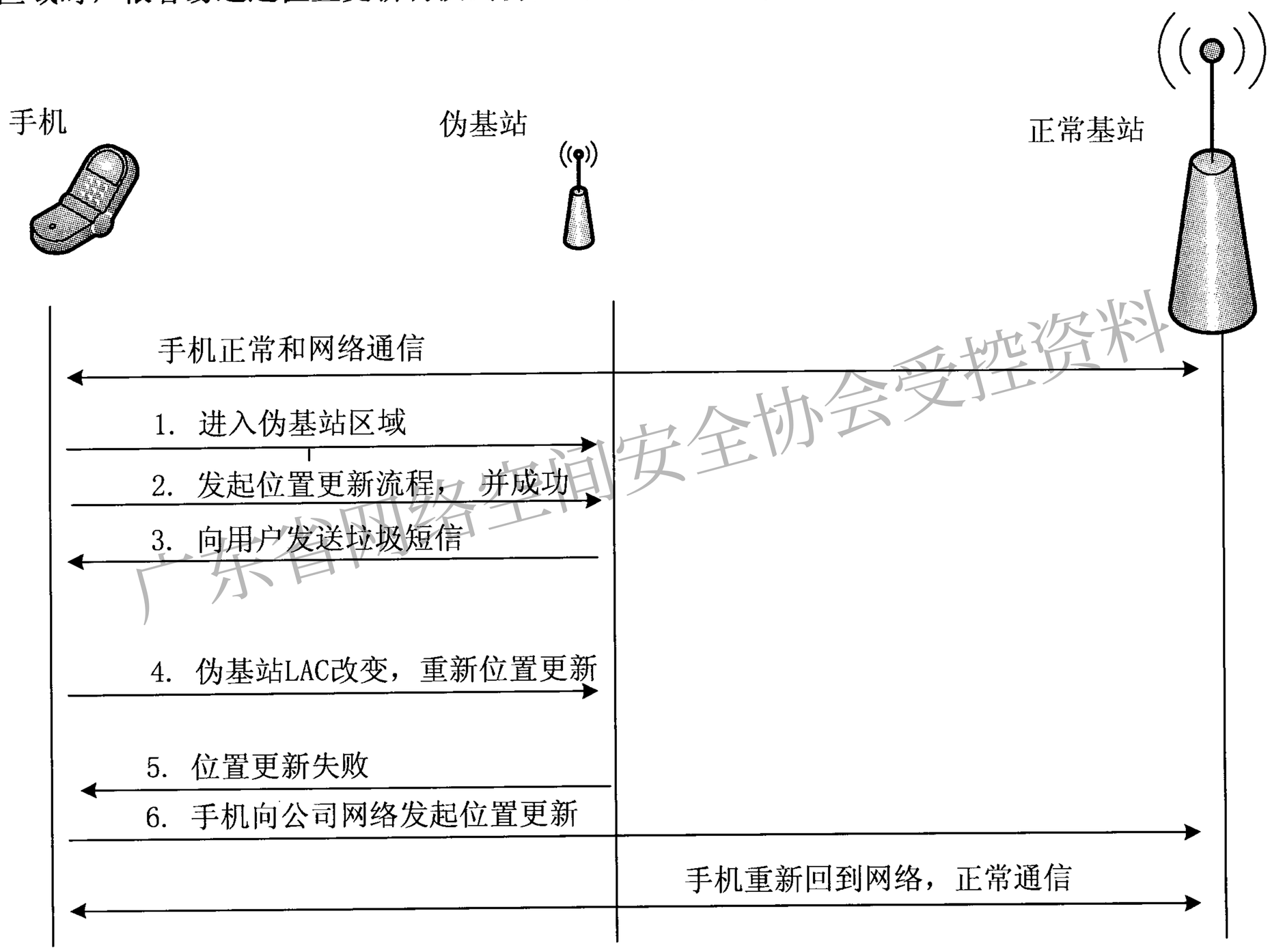


**图 A.1　伪基站发送垃圾短信流程**

一般情况下，为了降低被发现的机率，伪基站只会向手机发送一条短信，具体流程如下：

步骤1）手机进入到伪基站覆盖范围时，自动重选接入到伪基站小区；

步骤2）手机发送位置更新请求，伪基站接受请求，并下发位置更新成功消息（在此期间，伪基站也获取了用户的 IMSI 和 IMEI）；

步骤3）伪基站按照短信被叫流程，向手机下发短消息；

步骤4）伪基站主动变更LAC，通过广播消息告知已接入手机，触发手机再次位置更新；

步骤5）本次位置更新被伪基站拒绝，手机位置更新失败，手机脱离伪基站；

步骤6）手机重新位置更新，并切换回运营商网络。

为了提高用户接入伪基站的成功率，技术上存在伪基站通过干扰3G、4G多模终端，导致3G、4G多模终端回落到GSM网络，从而再接入到伪基站的可能。

## A.2 伪基站危害

伪基站非法使用运营商的频率，假冒运营商网络，伪装成运营商基站，利用大功率发射信号和无线参数优选设置，诱骗客户手机接入，收集客户信息，同时可伪造任意发送号码强行向覆盖区内的手机发送不良信息。伪基站不但干扰了用户正常生活，影响了公司商誉，还侵害了用户合法财产权益，严重扰乱了市场秩序，破坏了社会稳定。

伪基站的危害可以概括为以下三点：

a）严重干扰通信

非法占用运营商电信频率，利用大功率发射信号和无线参数优选设置，强制手机脱离运营商的正常网络，使其接入自身的伪小区。在接入伪小区期间，手机无法使用运营商提供的正常业务，造成大范围用户通信中断。同时，“伪基站”发送短信息行为需要大量终端的位置信息多次更新，严重消耗运营商信道资源。

b）严重骚扰用户

根据目前统计数据，单台伪基站每日发送的垃圾信息量最多可以达到10万～20万条，且主要集中在商场、酒店、车站等人口密集区。通过伪基站发送短信不通过正常通信网络，没有任何发送记录，运营商无法进行监测拦截和投诉查证。伪基站严重影响了用户的通信体验，用户往往不堪其扰，引发了大量投诉。

c）严重危害社会

伪基站可以任意设置信息的发送号码（例如假冒运营商客服号码、银行客服号码、政务信息专用号码等）发送大量违法信息，极易引发诈骗等其他治安或刑事案件。

# 附 录 B
（资料性附录）
网络侧监测的异常LAC号

## B.1 位置拒绝原因类型

由附录A.1可知，伪基站拒绝终端位置更新后，手终端位置更新失败脱离伪基站，之后向运营商网络重新发起位置更新，位置更新成功后会接入到正常网络。

在终端重新回归运营商网络时，会由于伪基站采用的位置拒绝原因不同而采用不同的源LAC号。根据3GPP TS 24.008，位置拒绝更新原因包括如下几种：

——#2 IMSI unknown in HLR；

——#3 Illegal MS；

——#6 Illegal ME；

——#11 PLMN not allowed；

——#12 Location Area not allowed；

——#13 Roaming not allowed in this location area；

——#15 No Suitabole Cells In location Area。

对于不同的拒绝原因，会有不同的后续处理：

a） #2 IMSI unknown in HLR

MS 将置位置更新状态为 ROAMING NOT ALLOWED，删除 TMSI，存储 LAI 和密钥序列，在关机之前认为 IMSI 非法。

b） #3 Illegal MS

MS 将置位置更新状态为 ROAMING NOT ALLOWED，删除 TMSI，存储 LAI 和密钥序列，在关机之前认为 IMSI 非法。

c） #6 Illegal ME

MS 将置位置更新状态为 ROAMING NOT ALLOWED，删除 TMSI，存储 LAI 和密钥序列，在关机之前认为 IMSI 非法。

d） #11 PLMN not allowed

MS 会删除 SIM 卡中 LAI，TMSI 和密钥序列，位置更新尝试计数器清零，位置更新状态置为 ROAMING NOT ALLOWED，将 PLMN ID 存储于"forbidden PLMN list"中，之后 MS 执行 PLMN 重选。

e） #12 Location Area not allowed

MS 会删除 SIM 卡中 LAI，TMSI 和密钥序列，位置更新尝试计数器清零，位置更新状态置为 ROAMING NOT ALLOWED，将 LAI ID 存储于 "forbidden location areas for regional provision of service" 列表中，之后 MS 执行小区重选。

f） #13 Roaming not allowed in this location area

MS 将位置更新尝试计数器清零，位置更新状态置为 ROAMING NOT ALLOWED，将 LAI ID 存储于 "forbidden location areas for roaming"列表中，之后 MS 执行 PLMN 重选。

g） #15 No Suitabole Cells In location Area

MS 将位置更新尝试计数器清零，位置更新状态置为 ROAMING NOT ALLOWED，将 LAI ID 存储

于 "forbidden location areas for roaming"列表中，之后 MS 在另一个位置区寻找合适的小区。

## B.2 网络侧监测到的异常LAC号分析

通过对MS接收到位置拒绝后是否删除所存储的LAI进行分析，网络侧监测到的具体LAC号情况如下：

a） #2 IMSI unknown in HLR

后续处理是在关机之前认为 IMSI 非法，这种方式对用户感知影响太大，伪基站一般不会采用。

b） #3 Illegal MS

后续处理是在关机之前认为 IMSI 非法，这种方式对用户感知影响太大，伪基站一般不会采用。

c） #6 Illegal ME

后续处理是在关机之前认为 IMSI 非法，这种方式对用户感知影响太大，伪基站一般不会采用。

d） #11 PLMN not allowed

后续处理是将 PLMN ID 存储于"forbidden PLMN list"中，导致用户可能长时间不能登记到运营商网络，对用户感知影响太大，伪基站一般不会采用。

e） #12 Location Area not allowed

后续处理是 MS 会删除 SIM 卡中 LAI,将会导致用户在发起位置更新时，采用系统默认的 65534。

f） #13 Roaming not allowed in this location area

后续处理是 MS 没有删除所存储的 LAI，则 MS 再次发起位置更新时，将以 MS 存储的 LAC（上一次成功更新的位置区号）发起位置更新。

g） #15 No Suitabole Cells In location Area

后续处理是 MS 没有删除所存储的 LAI，则 MS 再次发起位置更新时，将以 MS 存储的 LAC（上一次成功更新的位置区号）发起位置更新。

# 附 录 C
## （资料性附录）
## 移动伪基站现场定位作业方法建议

伪基站网络侧监测能够在后台实时监测到伪基站活动，并实时跟踪定位，为前台缩小搜索范围，为提高定位效率，通常需要前后台联合进行现场精准定位，具体伪基站现场定位作业方法建议如下：

在开展具体行动时，伪基站网络侧监测系统操作员时时关注实时预警，对告警时间长、告警次数多的站点进行筛选提取，通报给后台各调度人员；各调度人员及时向现场网优测试人员通报出现疑似伪基站活动的区域，指导其跟踪发现伪基站出现的区域，并对伪基站进行精确定位。具体步骤如下。

步骤1）路线规划

根据网络侧监测系统历史规律统计，圈定伪基站较为集中的区域，然后计划好测试线路。

步骤2）锁定范围

根据规划好的测试路线驱车DT测试。

测试手机设置建议：空闲态、锁定900M频段。一旦测试手机上显示异常CI和LAC时，即可判定周围存在伪基站的嫌疑，即在周围来回测试验证，根据伪基站信号强度即可大致锁定伪基站停放的范围。

如在测试过程中还收到垃圾短信，将更加肯定该范围内必定存在伪基站，此时可下车步行排查（注意：下车步行排查时，最好使用隐蔽性扫频仪和工程测试手机等小型工具，以免引起注意）。

如果伪基站信号越来越强，说明伪基站离所处位置越来越近。

步骤3）目标识别

当距离伪基站最近时信号最强，因此从不同方位接近伪基站即可 锁定伪基站具体藏匿在哪里或那辆轿车里。即便是停放在车辆较多的停车场里，利用此方法也能准确判定是哪一辆车。

当锁定伪基站目标后需采集信息：具体地址、时间、车牌号码、车辆型号、并拍照保存。

步骤4）联合执法

定位伪基站后需第一时间向公安、无线电管理部门等执法部门报案，报案后需安排1~2组人员对伪基站进行隐蔽监视、跟踪，避免犯罪人员发现逃跑，等待与公安、无委执法部门到达现场后联合抓捕。

中华人民共和国
通信行业标准
移动伪基站网络侧监测技术要求
YD/T 3167-2016
*
人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷

*
开本：880 × 1230　1/16　　2016 年 10 月第 1 版
印张：1.25　　2016 年 10 月北京第 1 次印刷
字数：30 千字
15115 • 1186
定价：20 元