### GSM 系统移动终端模糊测试平台

### 使用说明

# 一 系统架构

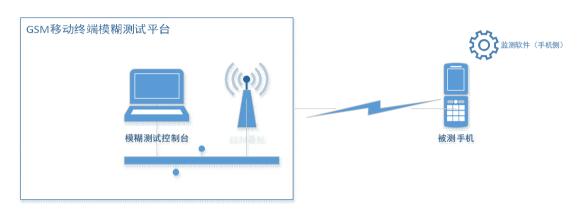


图 1 模糊测试平台整体架构

本系统由控制平台、GSM 基站以及手机侧监控软件三部分构成。

- 控制平台:提供交互界面,实现基站、被测手机的管理和维护,模糊测试数据的 生成、记录和管理测试结果;
- GSM 基站:负责通过无线链路向被测手机发送模糊信令,同时监测被测手机的运行情况,反馈给控制平台;
- 监测软件:实时监控手机运行状态,捕获手机的异常情况并及时上报给控制平台。手机与控制台之间通过 WIFI 通信,该软件目前仅支持华为手机平台,需要ROOT 权限,也可不必安装(也可通过 GSM 基站进行异常监测)

## 二 操作说明

### 2.1 控制平台操作

控制平台用户名密码: gsm:gsm。

控制平台通过有线连接与 GSM 相连,通过无线连接与被测手机通信。有线网址为192.168.0.1(静态 IP 地址),GSM 基站地址为192.168.0.2(静态 IP 地址)。

控制平台和手机的 WIFI IP 地址可动态获取,无需专门配置。



软件启动后,会根据配置文件设定的手机 IP 地址来拉取手机端的信息(需要安装手机软件)。

"手机参数"界面会显示手机端软件抓取的手机信息,包括手机的 CPU、内存、系统、基带等信息。可以通过点击刷新按钮来重新拉取手机信息。勾选框"测试时是否检测手机",可以让软件测试时同时查询手机状态(此功能需要手机端软件配合)。

机参数 基	站环境查询/设置	测试设置	测试执行	历史记录			
本参数			详细设置	<b>三查询</b>			
基站名称			控制参数 小区选择/重选参数				
CI			page (st. o. o. tit. o. tit. o. tit. o. tit.				
LAI			IMSI结合分离允许 (ATT)			1	
MCC	460		公用控制信道配置 (CCCH-CONF)			1	
MNIC	MNC 23		接入准许保留模块(BS-AG-BLKS-RES) 寻呼信道复帧数(BS-PA-MFRMS)			2	
						0	
LAC 1000		周期性位置更新定时器(T3212) 邻小区描述(Neighbour Cell Description)			12		
ARFCN					39 41 43		
工作频段 900			允许的网络色码(NCC Permitted)			1	
频点值 3			最大重发次数 (MAX retrans) 发送分布时隙数 (TX-integer) 小区禁止接入 (CELL-BAR-ACCESS)			1	
上行频率 935600 下行频率 890600		14					
		0					
117%			接入的等级控制(AC)				0

软件启动后也会自行拉取基站端的信息,然后显示到"基站参数查询、设置"界面。在这

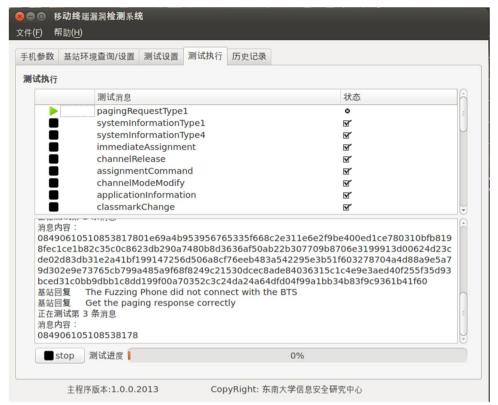
个界面可以通过点击"查询参数"重新拉取基站端的信息,也可以在修改参数后点击"修改参数"将参数更新到基站端。



"测试设置"界面用来对系统内部模糊器产生的模糊数据的参数进行配置,可以通过选择预定模式来快速设置参数。在"测试对象"列表中将所需的消息选择到"已选对象"中,来选择将要进行测试的消息。

测试之前必须设置测试手机的 IMSI。

可以通过将手机连接到基站后,可以直接通过按钮"getIMSI"获取手机的 IMSI 号。点击"开始测试"进行测试。



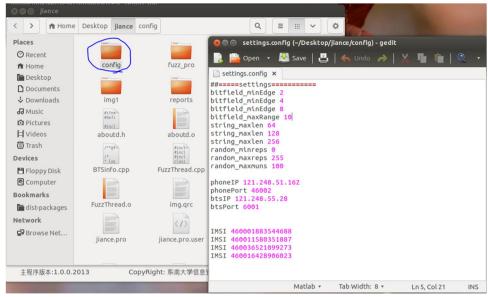
"测试执行"界面用来显示测试执行的状态。上部的列表框中显示测试消息的状态,以及是否检测出 bug。下面的文字框显示测试内核返回的状态消息。

点击"stop"按钮停止当前测试。当前不支持断点继续测试,停止后会重新从第一条开始测试。



测试同时会"历史记录"界面生成当前的测试报告。可以点击导出报告将报告保存。

在左边的文件窗口,可以通过点击查看记录查看保存的报告。



在程序主目录下的 config 文件夹,有一个 setting.config 配置文件。可以通过修改基站地址的 IP, 手机的 IP 地址。如非必要,不要修改其它的项的值。

### 2.2 手机软件安装说明

手机通过 WIFI 和控制平台相连。在获取手机的 wif ip 地址后,控制平台写入其配置文件,启动后即可与手机软件进行通信。

手机需 ROOT 才能运行软件,由于软件需要和底层硬件交互,因此不同厂商的手机实现方案不一样,目前仅支持华为手机。

软件安装方法:

电脑用 USB 线连接,在软件目录下执行如下命令:

Adb install package.apk.unaligned

当手机上出现软件图标即表明安装成功,点击该图标即可运行。

### 2.3 GSM 基站配置说明

GSM 基站通过有线直接和控制台相连。

GSM IP 地址为 192.168.0.2, 通信端口号为 6001, UDP 协议。

GSM 插上电源即可自动启动,无需人工干预。

GSM 基站支持远程登录, 采用 VNC 协议, 端口号 30000。登录用户名和密码为: root:bts