DOI:10.13878/j.cnki.jnuist.2016.04.006

郭锐[1]　冯志杰[1]　张浩然[1]

多制式移动终端身份感知系统研究

摘要

移动终端的合法监管是国家安全部门保障移动网络安全的重要手段,获取移动终端身份标识是实现监管的基础.首先阐述了移动终端的主要身份标识,以及监管系统相关研究现状;然后给出一种面向双频点 GSM 网络和 WCDMA 网络的多制式移动终端身份感知系统设计方案,阐明系统技术原理与实现方法,并提出对该系统进行优化的技术方案;最后进行测试,验证了方案的可行性.

关键词

移动终端;身份感知;自组织网络;全球移动通信系统(GSM);宽带码分多址(WCDMA)

中图分类号 TN929.53

文献标志码 A

0　引言

移动通信网络迅猛发展,给人们带来生活便利的同时也滋生了违法犯罪行为,引入监管系统十分必要.要进行语音、短信等话务活动和非话务活动监管,甚至完全接管移动终端,前提是识别移动终端.

移动终端的身份标识主要包括 4 项:1)IMSI(International Mobile Subscriber Identification Number,国际移动用户识别码),与 SIM(Subscriber Identity Module,客户识别模块)卡或 USIM 卡绑定,全球范围内唯一识别移动用户;2)TMSI(Temporary Mobile Subscriber Identity,临时移动用户标识),由网络为移动用户临时分配,特定区域特定时间内有效,减少 IMSI 使用频率,保护隐私安全;3)IMEI(International Mobile Equipment Identity,国际移动设备标识),与移动台设备绑定,用于全球范围内唯一识别移动台设备;4)MSISDN(Mobile Subscriber International ISDN/PSTN Number,移动用户国际 ISDN/PSTN 码),代表主叫用户呼叫移动用户所拨打的号码,即手机号码.本文的移动终端身份感知就是识别出附近移动用户的 4 项身份标识号码.

传统的监管方法是通过核心网警用接口,由运营商提供合法侦听技术[1].随着 3G、4G 网络的发展,以 Femtocell 为代表的家庭基站正在普及,分流了运营商宏基站的流量,增强了室内信号覆盖效果.对于部署了家庭基站的应用场景,合法侦听可以在核心网侧和家庭基站侧两方面展开[2].针对 GSM 网络,利用软件无线电平台、GSM 模块以及 GSM 开源协议栈设计身份监管系统,可以获取移动终端的身份标识[3].在此基础上,设计实现短消息监管系统[4]以及语音短信监管系统[5],并且实现在中国移动 GSM 和中国联通 GSM 双频点同步监管.现有的监管系统存在诸多局限性:监管成功率不够高,监管系统附近终端经常无法被感知;移动通信网络发展至今,多种网络制式并存,监管系统面向单一制式,感知系统的应用受到限制.

本文给出一种多制式移动终端身份感知系统设计方案,方案中监管基站采用 SON(Self-Organizing Network,自组织网络)相关算法进行自配置优化,从而提高移动终端接入成功率和身份感知成功率,系统面向 GSM 和 WCDMA 两种网络制式,GSM 包含中国移动频点和中国联通频点,使得监管系统的应用场景得到扩展.

收稿日期 2016-01-08

资助项目 国家高技术研究发展计划(2013AA01A214)

作者简介

郭锐,男,工程师,主要研究方向为移动通信.120195102@qq.com

张浩然(通信作者)男,硕士,研究实习员,主要研究方向为移动通信、嵌入式技术.ahxxzhr@qq.com

1　中国科学院信息工程研究所,北京,100195

1 系统设计原理

1.1 IMSI/TMSI/IMEI 感知原理

移动终端开机时,将执行小区选择流程,寻找最合适的小区进行驻留;之后,如果移动终端处于空闲模式,将不断计算相邻小区的 C1 值和 C2 值,判断并执行小区重选流程,保证移动终端驻留在最合适的小区中;小区选择和小区重选后,移动终端将从小区广播消息中得到 LAC(Location Area Code,位置区码),通过比较,如果和 SIM 卡中存储的 LAC 值不同,则执行 IMSI 附着位置更新流程,即移动终端根据附近网络 BCCH(Broadcast Control Channel,广播控制信道)信道中的参数值决定是否进行小区选择或小区重选;涉及到位置区改变时,触发位置更新,而在位置更新流程中,网络侧向移动终端索取 IMSI 号码等身份信息,故引导移动终端接入自行搭建的可控监管基站,在移动终端位置更新的过程中解析信令消息,可以获取到 Um 接口传送的 IMSI/TMSI/IMEI 等身份标识.

1.2 MSISDN 感知原理

在移动通信流程中,被叫终端所接收的信令消息包含主叫的 MSISDN 号码,故发起呼叫相关流程即可获取 MSISDN 号码.

对于 GSM 制式的终端,在感知到 IMSI 号码的基础上,利用开源 GSM 协议栈,搭建主叫终端平台,模拟被感知移动终端的身份,通过真实网络的鉴权,呼叫被叫终端,即可利用被叫终端的来电显示功能提取到被感知移动终端的 MSISDN 号码.

对于 WCDMA 制式的终端,在感知到 IMSI 号码的基础上,利用 WCDMA 协议栈搭建汇聚网关服务器,该服务器完成监管基站到业务网关之间的呼叫信令转接,通过 Femtocell 给移动终端发送信令,呼叫被叫终端,截取信令数据并解析出 MSISDN 号码,然后终止呼叫.

1.3 系统采用的核心技术

系统采用的核心技术主要包括以下 3 个方面:

1)SON 技术:监管基站利用 SON 算法实现开机时自配置,运行中自优化,减小监管基站对外部网络的影响,提高监管基站的覆盖效果与感知成功率;

2)GSM 通信技术:根据设定的感知流程修改开源 GSM 协议栈信令流程;

3)WCDMA 通信技术:根据设定的感知流程修改 WCDMA 协议栈信令流程.

2 系统实现

系统结构如图 1 所示,整个系统由被监管移动终端、监管基站、主叫终端、被叫终端、串口通信模块以及业务网关组成,包含软件及硬件.监管基站实现 GSM 网络下 IMSI/TMSI/IMEI 号码的感知,在 GSM 网络感知 MSISDN 号码时协助完成网络鉴权,并在 WCDMA 网络下完成整个感知流程.主叫终端用于 GSM 网络下 MSISDN 号码感知,被叫终端用于 GSM 和 WCDMA 网络下 MSISDN 号码感知,串口通信模块用于 GSM 网络下感知 MSISDN 号码,业务网关用于 WCDMA 网络下 MSISDN 号码感知.

2.1 主要模块的实现

2.1.1 监管基站的实现

监管基站是被感知移动终端与感知系统的唯一接口,构成一个小范围低功率的移动通信基站网络环境,是实现移动终端身份感知的基础,在初始的 IMSI 号码感知、进一步的 MSISDN 号码感知以及后续的短信、语音等监管中,都需要监管基站稳定地工作.

监管基站的 GSM 部分,由软件无线电平台和 GSM 基站协议栈模块组成:2 个软件无线电平台为硬件设备,分别工作在中国移动 GSM 频点和中国联通 GSM 频点上,负责无线电信号的发送与接收、调制与解调以及 AD 转换;GSM 基站协议栈模块运行在 PC 端,实现了 GSM 协议全部 3 层代码功能,实现上行数据解析和下行数据封装.

监管基站的 WCDMA 部分,由家庭基站 Femtocell 和汇聚网关模块组成:Femtocell 工作在中国联通 WCDMA 频点上,负责无线电信号的发送与接收、调制与解调以及 AD 转换;汇聚网关模块运行在 PC 或服务器端,实现上行数据解析、信令转接和下行数据封装.

2.1.2 主叫终端的实现

主叫终端用于 GSM 制式下 MSISDN 号码的感知,由手机模块和手机协议栈模块组成:2 个手机模块为硬件设备,分别内置中国移动 SIM 卡和中国联通 SIM 卡,烧入 GSM 协议栈手机侧 L1 层代码,负责无线电信号的发送与接收、调制与解调以及 AD 转换;手机协议栈模块运行在 PC 端,实现了 GSM 协议栈 L2、L3 层代码,实现上行数据封装和下行数据解析.

2.1.3 被叫终端的实现

被叫终端用于 MSISDN 号码的感知,一方面附

着在外部移动通信网络上等待被叫,另一方面能够连接 PC 从而设置并读取来电显示信息.

被叫终端由 GSM 模块和外围电路组成:GSM 模块采用华为公司 EM310 模块,外围电路包含 RS232 串口,用于连接 PC 端.

2.2 系统优化

在传统的监管系统[3-5]中,监管基站开启后,以较高的 C1、C2 值广播系统消息,监管基站的配置参数是人为手动设定的,在引导移动终端接入的同时,也对附近移动通信网络产生较大影响.将 SON 技术引入监管基站系统中,在监管基站开启后,首先侦听周围基站,搜索附近小区,根据搜索到的邻区信息自动配置自身参数,以达到系统间干扰最小,同时提高监管基站覆盖效果与感知成功率.

在移动通信网络中,基站引导移动终端附着在自身小区的过程,是移动终端执行切换的过程.优化

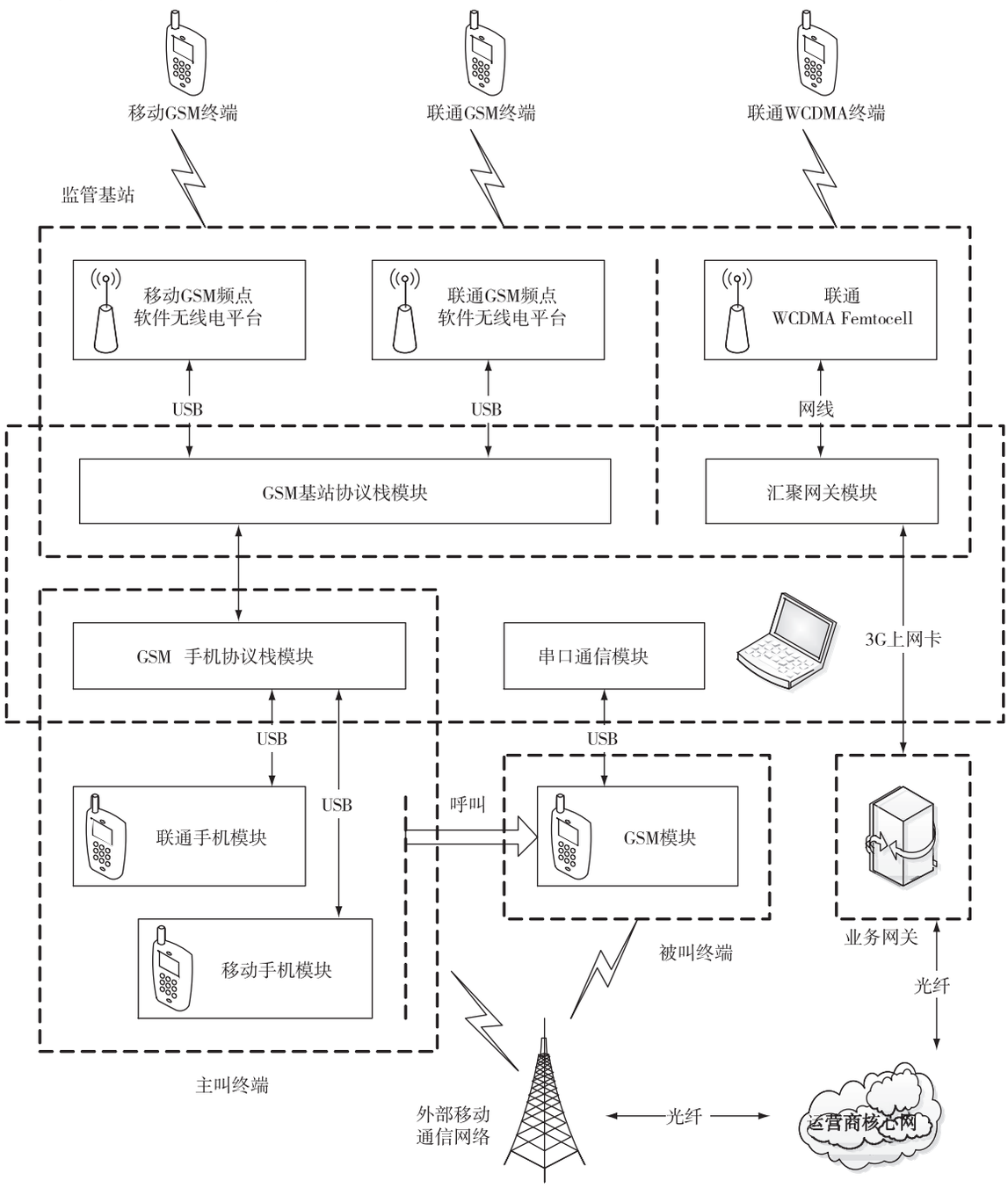

图 1 多制式移动终端身份感知系统结构

Fig. 1 Block diagram of multiformat identity detection system for mobile terminal

切换算法,动态调整 TTT、HYS 和 MSH 等参数,可以降低切换导致的无线链路失败率[6].从测量机制和算法两方面入手,可改进家庭基站的 SON 测量机制、切换判决算法以及切换准入算法[7].本文的监管基站软件实现中,参考了以上文献的研究成果,具体在 GSM 基站协议栈模块和联通 WCDMA Femtocell 等处修改代码实现.

2.3 系统工作流程

监管基站的 GSM 基站协议栈模块和汇聚网关模块、主叫终端的 GSM 手机协议栈模块以及串口通信模块均运行在 PC 端,软件无线电平台通过 USB 连接 PC,Femtocell 通过网线连接 PC,手机模块通过 TTL 转 USB 连接 PC,GSM 模块通过 RS232 转 USB 连接 PC,PC 通过 3G 上网卡连接互联网.

系统对于 GSM 制式和 WCDMA 制式的移动终端感知流程略有不同,GSM 制式移动终端感知流程如下:

1)系统启动阶段:各硬件模块上电启动,并运行 PC 端程序;监管基站完成自配置,完成有关发射功率、小区信息、无线频点 ARFCN 等参数的设置,构建中国移动 GSM 和中国联通 GSM 两个小范围移动通信网络,向周围广播消息;监管基站做出设置,使得主叫终端和被叫终端不驻留在监管基站构建的网络上,二者均内置 SIM 卡,附着在外部真实移动通信网络上.

2)感知 IMSI/TMSI/IMEI 号码阶段:监管基站成功开启后,引导附近的移动终端用户驻留在自行构建的小区内,基站协议栈模块和移动频点软件无线电平台实现附近移动 GSM 终端 IMSI/TMSI/IMEI 号码的感知,和联通频点软件无线电平台实现附近联通 GSM 终端 IMSI/TMSI/IMEI 号码的感知,信令流程如图 2 所示.在移动终端回传身份信息后,监管基站的基站协议栈模块解析信令数据,提取出 IMSI/TMSI/IMEI 号码,并将 IMSI 传递给主叫终端.

3)主叫终端模拟被监管移动终端通过网络鉴权阶段:该阶段信令流程如图 3 所示.该阶段手机协议栈模块依次分别控制移动手机模块和联通手机模块呼叫被叫终端.主叫终端接收到 IMSI 号码,手机协议栈模块重新封装 CM 业务请求消息,以被监管移动用户的身份与外部移动通信网络通信,业务类型为移动发起呼叫;外部网络发起鉴权,验证用户身份,主叫终端收到鉴权请求消息后,由手机协议栈模块解析出鉴权随机数 RAND,传递给监管基站;基站协议栈模块将随机数 RAND 重新封装,从软件无线电平台发送给移动终端;移动终端收到鉴权随机数后,利用自身 SIM 卡内存储的 Ki 和 A3 算法得出鉴权结果 SRES,并回送至监管基站;经基站协议栈解析、手机协议栈封装,从手机模块在规定时间内将鉴权结果 SRES 返回至外部网络,最终完成鉴权.至此,主叫终端成功模拟被监管移动终端的身份,可继续呼叫被叫终端.

图 2 IMSI/TMSI/IMEI 号码感知流程

Fig. 2 Detection process of IMSI/TMSI/IMEI under GSM network

4)提取 MSISDN 号码阶段:在 PC 端的串口通信模块中,通过 AT 命令设置被叫终端的来电显示功能,在被叫终端收到主叫终端的呼叫后,即可提取来电显示信息,从而得到被监管移动终端的 MSISDN 号码.

WCDMA 制式下移动终端身份感知的系统启动阶段和 IMSI/TMSI/IMEI 号码感知阶段与 GSM 制式下类似.在感知到 IMSI 号码的基础上,汇聚网关模块通过 Femtocell 向移动终端发送指令,使其呼叫被叫终端,捕获主叫信令流程,解析出被感知 WCDMA 移动终端的 MSISDN 号码,然后终止主叫流程.

3 系统测试

为验证系统的有效性,进行了一系列测试实验.

被叫终端插入联通 2G SIM 卡.被感知手机移动终端选用 iPhone 4s、iPhone 5s、iPhone 6、HTC M8、nubia Z9 Max、小米 Note、三星 Galaxy Note4、华为 P8、魅族 MX5、联想 K50-t5 等 10 种常用手机,分别插入移动 2G(GSM 制式)、联通 2G(GSM 制式)和联通 3G(WCDMA 制式)的 SIM 卡.测试时做 2 种设计,一是感知系统先启动,被感知移动终端后开机;二是被感知移动终端先开机,感知系统后启动.

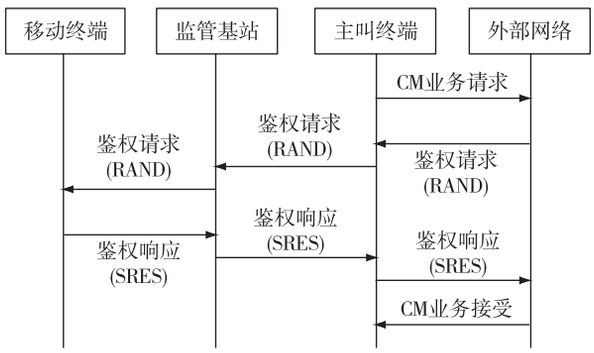

图 3 GSM 网络 MSISDN 号码感知鉴权流程

Fig. 3 Authentication process during MSISDN detection under GSM network

经测试,以上情况下,被感知移动终端在距离感知系统 10、30 和 50 m 的范围内均能被正确感知.

4 结束语

本文给出的多制式移动终端身份感知系统方案,能够感知附近的中国移动 GSM 终端、中国联通 GSM 终端以及中国联通 WCDMA 终端的 IMSI/TMSI/IMEI 以及 MSISDN 号码;监管基站利用 SON 自配置后对周围移动通信网产生的影响较小;系统感知成功率较高,长期运行较可靠,为移动通信网络监管提供了切实可行的方案.

参考文献

References

[1] 陈捷,万莉莉.通信网络合法侦听研究[J].电力系统通信,2008,29(5):48-50
CHEN Jie,WAN Lili.Research on lawful interception in communication networks [J]. Telecommunications for Electric Power System,2008,29(5):48-50

[2] 许星宇,郑燕琳,徐征,等.基于 CDMA 1x 分组域家庭基站合法侦听的研究[C]//2011 年全国电子信息技术与应用学术会议论文集,2011
XU Xingyu, ZHENG Yanlin, XU Zheng, et al. The research for lawful interception of Femtocell base on CDMA 1x packet switched domain [C] // 2011 National Conference on Electronic Information Technology and Application,2011

[3] 胡锡利.基于 Um 接口的身份监管系统研究与实现[D].南京:东南大学,2012
HU Xili. The research and realization of supervision system for identity based on Um interface[D].Nanjing: Southeast University,2012

[4] 黄泽.面向 GSM 网络的移动终端身份感知与短信监管系统研究与实现[D].南京:东南大学,2013
HUANG Ze.The research and realization of identity perceiving and SMS supervision system of mobile terminal for GSM network[D].Nanjing:Southeast University,2013

[5] 秦雨.GSM 网络移动终端双频点身份感知及语音短信监管系统研究[D].南京:东南大学,2014
QIN Yu.The research of identity perceiving,SMS and call supervision system for dual-ARFCN of GSM network [D].Nanjing:Southeast University,2014

[6] 张临,陈勇,林小雅.基于 SON 的 LTE HeNB 切换参数优化算法研究[J].信息通信,2013(10):197-199
ZHANG Lin,CHEN Yong,LIN Xiaoya.Research on optimization algorithm of LTE HeNB handover parameters based on SON[J].Information & Communications,2013 (10):197-199

[7] 范霞萍.LTE 家庭基站切换算法的研究与实现[D].南京:南京邮电大学,2013
FAN Pingxia.Research and realization of LTE Femtocell handover algorithm [D]. Nanjing: Nanjing University of Posts and Telecommunications,2013

Multiformat identity detection system of mobile terminal

GUO Rui[1] FENG Zhijie[1] ZHANG Haoran[1]

1 Institute of Information Engineering,Chinese Academy of Sciences,Beijing 100195

Abstract Lawful supervision of mobile terminals is an important means of national security sectors to guarantee mobile network security.And access of identity of mobile terminal is basis for supervision.Based on description of the main identities of mobile terminal and the research status of supervision system,this paper proposes a design scheme of multiformat mobile terminal identity detection system,which can be applied to dual-arfcn GSM network and WCDMA network,clarifies its technical principle and implementation processes,and presents a technical solution for system optimization.The multiformat identity detection scheme is verified through system test.

Key words mobile terminal; identity detection; Self-Organizing Network; Global System for Mobile Communitation;Wideband Code Division Multiple Access