基于GSM信令监测的SIM卡克隆预警系统设计

江川贵　庞琳　曾键

（中国移动通信集团四川有限公司　成都 610081）

摘　要　随着移动通信业务的高速发展，收入流失风险也在逐步加大，各种不法分子利用SIM卡克隆进行高额欺诈的手段越来越复杂，给移动运营商造成较大损失和不良影响。本文介绍了一种以“GSM信令监测进行SIM卡克隆预警”的技术方案，在快速预警SIM卡克隆欺诈上能起到较好的作用。

关键词　GSM信令　SIM卡克隆　欺诈

1　背景

随着国际漫游业务的不断发展，各种不法分子利用SIM卡克隆进行国际业务欺诈的事件越来越多，手段越来越复杂，涉及的金额越来越大，致使各运营商面临巨大的风险。特别是通过克隆SIM卡在国外运营商网络同时发起多通通话的重大欺诈事件发生的频率逐步增加，涉及的范围逐渐扩大，给电信运营商造成巨大经济损失和不良的社会影响。现有的欺诈监控手段主要是通过分析计费系统话单方式实现，属于事后控制。由于受漫游方运营商高额报告和通话话单回传速度的限制，从欺诈事件发生到采取有效手段周期较长，欠费风险进一步扩大，往往出现单个用户欠费几十万到数百万等，造成了巨大的损失。因此如何缩短SIM卡克隆欺诈发现的时间、快速有效地对欺诈行为进行响应和控制来最大限度减少欺诈损失成为收入保障和规避运营风险的一块重要工作。

2　控制思路

SIM卡克隆高额欺诈实际上是一种犯罪行为，从控制社会犯罪程度降低的角度来讲，更应该偏向于犯罪事件的防范而不是把重点放在对犯罪分子事后的惩罚上，因此SIM卡克隆欺诈犯罪的控制重心应该放在如何有效预防上。SIM卡克隆欺诈行为的发生都是由于话单达到计费系统的时间差造成，时间延迟越大，给欺诈行为留下的空间就越多。目前利用话单来分析用户欺诈行为的处理方式属于事后行为，当用户的欺诈行为被发现的时候实际收入已经流失。因此解决问题的关键是缩短发现用户欺诈行为的时间，以达到提前控制用户欺诈行为发生的目的。要在用户欺诈行为发生前预防，必须借助GSM核心交换网的信令消息数据来实时跟踪用户的状态和使用业务情况，技术原理如图1所示。

由于无论用户在国内或出访到国外，其位置更新信令数据（Location Update）都要落地到归属地本地HLR，因此通过实时采集本地HLR上用户的位置更新信令数据就可以掌握用户的业务使用情况，以达到最快发现问题的目的。各网元实体的功能如下。

2.1 归属地HLR

实时记录用户的GSM位置更新信令数据。

2.2 信令监控系统

（1）监控用户在拜访地MSC/VLR与HLR发生的信

江川贵：中国移动通信集团四川有限公司业务支撑中心工程师，从事业务支撑网维护工作。
庞　琳：中国移动通信集团四川有限公司业务支撑中心副总经理，从事业务支撑网管理工作。
曾　键：中国移动通信集团四川有限公司业务支撑中心总经理，从事业务支撑网管理工作。

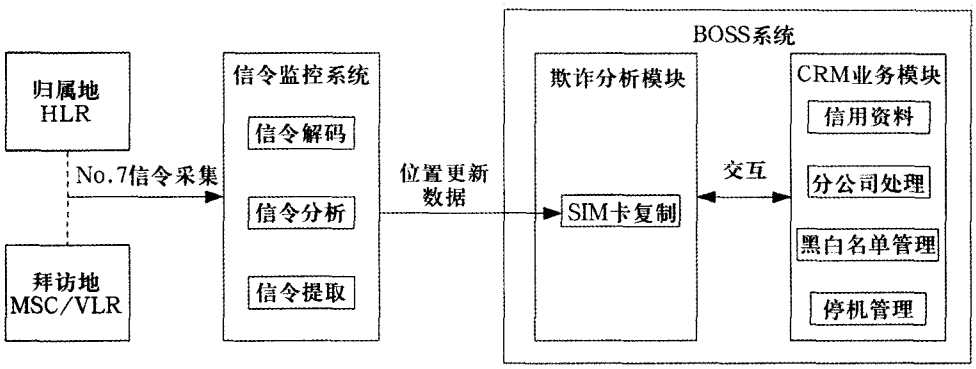

图1 SIM卡克隆监控原理图

令交互数据；

(2) 通过信令的解码、分析、合成、提取等一系列技术环节单独分离出欺诈系统需要的位置更新数据。

2.3 BOSS 欺诈分析模块

(1) 实时取得用户的位置更新数据，分析用户的位置更新异常数据和结合用户在 BOSS 系统里的相关信用资料，对用户的行为进行欺诈分析；

(2) 将确定的欺诈用户和具备欺诈嫌疑的用户号码实时提交 BOSS CRM 业务模块做后续处理。

2.4 BOSS CRM 业务模块

(1) 向欺诈分析模块提供用户信用相关资料的数据；

(2) 对于欺诈分析模块确定的欺诈用户通过向 HLR 发送停机指令进行实时停机；

(3) 高端用户以及特殊用户的白名单管理，欺诈行为恶劣用户实现黑名单管理。

3 实现方案

3.1 组网结构

用户处于漫游状态下反欺诈关键环节是在 HLR 上对用户的位置更新数据实现实时提取，采用如图的组网结构可以通过 No.7 信令监控系统实现了对位置更新信令数据的实时采集，该方案选取的信令监控链路为 HLR-LSTP，该监控策略可以实现用户在以下状态下的位置更新信令数据的实时监测；

(1) 用户国际漫游出访；

(2) 用户在国内漫游；

(3) 用户在省内漫游。

在该组网方案中，No.7 信令监测系统向 BOSS 提供的用户位置更新数据至少应包括以下内容：MSISDN、IMSI、位置更新时间、拜访地国家区号、拜访地 VLR 地址。

3.2 预警实现过程

(1) SIM 卡克隆监测系统通过信令监控系统实时获取用户的位置更新数据（包括国际漫游、省际漫游、省内漫游）；

(2) SIM 卡克隆监测系统对同一 MSISDN（或同一 IMSI 号码）的位置更新数据进行持续跟踪和分析，从时间、空间两个维度设置的逻辑规则来判定该张 SIM 卡具备克隆欺诈的嫌疑（如用户在 30min 内有分别来自北京和伦敦的 MSC/VLR 相互矛盾的位置更新信息），如图 3 所示；

(3) SIM 卡克隆监测系统将 SIM 卡克隆嫌疑的用户号码传递 BOSS，由 BOSS 系统结合用户的信用资料等相关信息判断是否为欺诈行为，对于确认欺诈的用户可以对其实施直接停机的操作。

3.3 系统模块

基于 GSM 信令监测的 SIM 卡克隆预警系统主要包括 4 大模块：欺诈监测模块、预警信息模块、预警信息处理和反馈模块、统计报表模块，主要模块功能如下。

(1) 欺诈监测模块：主要对欺诈监测规则库和对用户发生位置更新冲突时间的阀值以及告警级别等配置内容进行设置；

(2) 预警信息模块：该模块为系统监测到的具有 SIM

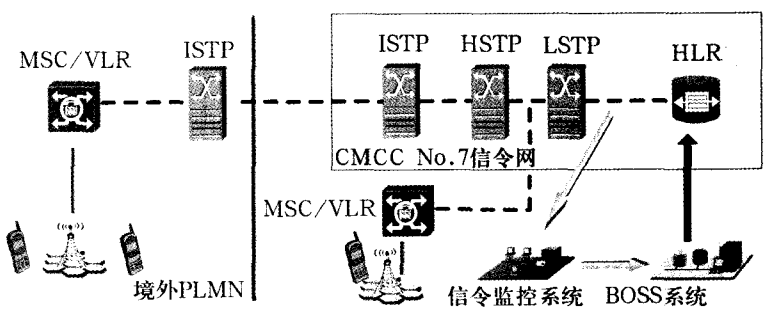

图2 SIM卡克隆欺诈预警组网结构

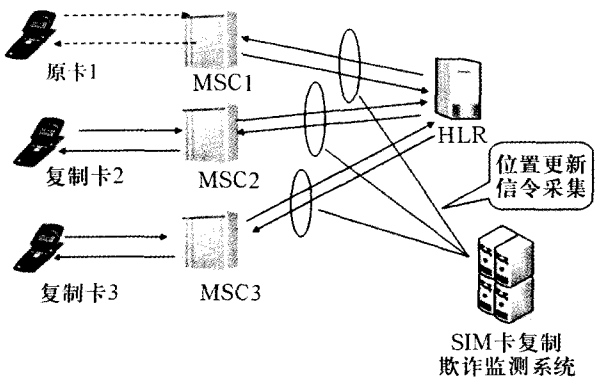

图3 SIM卡克隆欺诈监测预警逻辑图

卡克隆嫌疑的用户号码以及具体的用户位置更新详细数据，包括用户号码、IMSI 号码、国家代码、位置更新时间、告警时间、告警级别等信息；

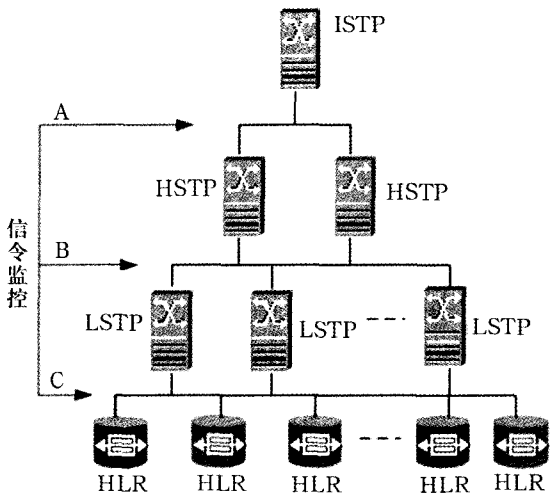

图4 SIM卡克隆欺诈信令监测部署方案

（3）预警信息处理和反馈模块：该模块向 BOSS 提供 SIM 卡克隆的嫌疑欺诈用户，可以在 BOSS 前台完成对欺诈用户的判断和停机等操作；

（4）统计报表模块：针对系统的预警信息内容以及处理其反馈结果等进行统计和分析，包括日常趋势图、地市欺诈分布图、高危欺诈国家分布图等内容。

4 结论

基于 GSM 信令监测的 SIM 卡克隆预警系统的关键技术点在于信令采集的部署，从技术原理上看可以选择的信令监控方式如图 4 中的 A、B、C，3 种监控方式的优劣点比较如表 1 所示。

表1 3种监控方式的优劣点比较

监控策略	监控链路	监控数据	监控用户	优点	缺点
A	ISTP–HSTP	国际漫游	全部HLR	投资少、监控用户多	监控数据少
B	HSTP–LSTP	国际漫游、省际漫游	部分HLR	投资中等、监控用户中等	监控数据中等
C	LSTP–HLR	国际漫游、省际漫游、省内漫游	指定HLR	所有漫游数据都能监控	投资大、监控用户少

电信运营商可以根据自己具体的国际、省际、省内漫游欺诈分布情况，选择最优的监控方案，充分利用和整合业务支撑网（BOSS）和交换网络（GSM）的核心数据资源建设 SIM 卡克隆预警系统，以期斩断高额话费欺诈黑手。

Design of SIM Card Clone Early Warning System Based on GSM Signaling

Jiang Chuangui Pang Lin Zeng Jian

(China Mobile Group Sichuan Co., Ltd., Chengdu 610081)

Abstract With the high-speed development of mobile communication business, the risk of arrear is becoming serious. the way of cheating by taking advantage of SIM card clone by some criminals is becoming more and more complex, which brings the mobile operator much loss and bad effect. This paper introduces a way of "early warning of SIM card clone based on GSM signaling " which can discern the cheating of SIM card clone soon.

Keywords GSM signaling, SIM card clon, cheating

（收稿日期：2010 年 3 月 15 日）