物联网卡业务运营风险监控系统的研究

赵俊[1]，刘浩明[1]，王伟杰[2]

(1 中国移动通信集团广东有限公司，广州 510630 ；2 中移（杭州）信息技术有限公司，杭州 310012)

摘　要　在物联网高速发展的同时，也暴露出一系列的安全问题。本文首先总结了物联网卡业务运营过程中出现的风险场景，然后探讨了物联网卡风险行为特征的提取方法，最后提出了物联网卡异常行为的提取规则，搭建物联网业务运营风险监控系统，以告警并协助处理异常网卡，保障物联网的完全运营。

关键词　物联网卡；风险监控；电话诈骗；机卡分离

中图分类号　TP309　　**文献标识码**　A　　**文章编号**　1008−5599（2019）01−0067−06

DOI:10.13992/j.cnki.tetas.2019.01.015

1　研究背景

1.1 物联网的飞速发展

近年来，物联网卡行业发展日益迅速，物联网快速井喷的信号不断涌现。 2017 年 1 月，工信部发布《物联网“十三五”规划》，明确了物联网产业“十三五”的发展目标，完善技术创新体系，构建完善标准体系，推动物联网规模应用，完善公共服务体系，提升安全保障能力等具体任务。

在时代背景和国家政策的推动下，中国移动将物联网作为实现集团“大连接战略”的重要引擎。根据 2017 年全球合作伙伴大会中的数据，中国移动已实现 346 个城市 NB−IoT 连续覆盖和全面商用，物联网连接数突破 2 亿，是全球最大的物联网连接提供商。

1.2 物联网面临的安全风险

在物联网迅速发展的过程中，对于物联网卡的安全管理暴露出来许多问题。基于物联网业务场景多、设备种类复杂、网络接入方式多样的特点，其在业务管理、运营和技术上都存在许多安全风险及挑战。

现阶段物联网面临的各类安全风险主要可以分为以下 3 点。

（1）管理风险：主要为安全管理体系不完善，安全责任界面不清，卡无法准确溯源风险及存量行业存在源头管控风险等。

（2）运营风险：主要为业务滥用、业务漏洞、机卡分离等。

（3）技术风险：主要为系统脆弱性风险、信息泄露风险、接入认证风险和拒绝服务风险。

本文以物联网运营风险为主要切入点，针对物联网运营环节产生的问题，建立物联网卡业务异常识别模型，识别异常行为，并通过该物联网监控平台进行告警并协助处置异常卡。

收稿日期：2018−11−12

2 物联网异常业务场景概述

由于物联网卡自身需求多样化、套餐多样化、业务复杂、计费方式多样的特点，物联网业务运营过程中暴露了一系列的问题。主要分为业务风险场景识别、骚扰／诈骗码号识别两部分。

2.1 物联网卡骚扰／诈骗电话风险场景

物联网卡在骚扰／诈骗的风险点在于群拨骚扰／诈骗电话（即语音欺诈，分为响一声、呼死你和诈骗电话3类）。

（1）响一声：是指对用户发起骚扰呼叫，响一声即挂掉，诱使用户回拨，上当受骗。

（2）呼死你：是指即用户在一定时间内接到响一声就挂的高频骚扰电话轰炸，导致用户无法正常使用电话。

（3）诈骗电话：是指冒充公检法、亲友等，设置各种诈骗剧本，对用户实施欺诈。

2.2 物联网卡其它业务风险场景

针对通话量、短信或流量业务的滥用行为，分别以不同时期业务量使用状况作为参考，建立业务量异常场景识别模型，其主要风险点如下。

（1）使用猫池设备：模拟多部手机进行通话／短信／上网等行为，形成渠道套利及各种欺诈场景。

（2）“薅羊毛”：一次性获得大量未注册的账号，在电商平台通过验证码套利、抢佣金等享受优惠。

（3）流量盗用：由于物联网卡的流量资费较大网卡更低廉，存在套利空间。

综上所述，物联网卡运营中会出现的风险场景可以分为6种，如表1所示。

表1 不同类型的风险场景

数学符号	风险场景
d_1	使用猫池设备
d_2	薅羊毛
d_3	流量盗用
d_4	响一声
d_5	呼死你
d_6	诈骗电话

3 物联网卡风险场景行为特征提取

以跨省使用、机卡分离、流量异常和骚扰／诈骗电话4个维度为基础，分别提取相应的行为特征，建立物联网卡的行为画像，用以准确识别不同业务场景下的风险卡号。

3.1 物联网卡跨省市使用和机卡分离异常行为特征提取

物联网卡跨省市使用识别的具体流程如图1所示。

机卡分离的识别主要依据是设备的IMEI码。IMEI码由GSMA协会统一规划，并授权各地区组织进行分配，在中国由工业和信息化部电信终端测试技术协会（TAF）负责国内移动设备的入网认证，其他分配机构包括英国BABT、美国CTIA等。物联网卡在注册激活时，会记录其激活的IMEI码。因此，可以通过设备在通话或上网过程中采集的IMEI信息识别出是否发生机卡分离现象。

3.2 物联网流量异常行为特征提取

在对物联网卡检测的过程中，可通过对历史数据的特征提取，构建物联网卡流量使用画像，并基于流量使用情况对物联网卡进行分类。然后针对不同类别的物联网卡，获取一组样本数据。而当日的使用流量即可作为待检测一个离群值，即可以获取当日业务量的统计量，对比检出水平 α 和剔除水平 α^* 对应的临界值即可判定当日该用户的业务量使用情况是否异常。具体业务量异常识别步骤如下。

（1）获取当日活跃用户号码，并通过号段识别出物联网卡成员并编号（1，2……n），依次检测该 n 个用户是否发生业务量异常。

（2）基于物联网卡流量使用情况，构建物联网卡资产画像，将物联网卡分为 L 类。

（3）设类别 l 包括 i 个用户，依次选取第 i 个用户，根据历史的通话记录、流量使用记录及短信使用记录进行特征提取。以流量使用记录为例，主要获取当日使用时长、上行流量、下行流量、总使用流量、使用次数5组数据。

（4）依次确定业务量对应的 M 个特征的历史使用情

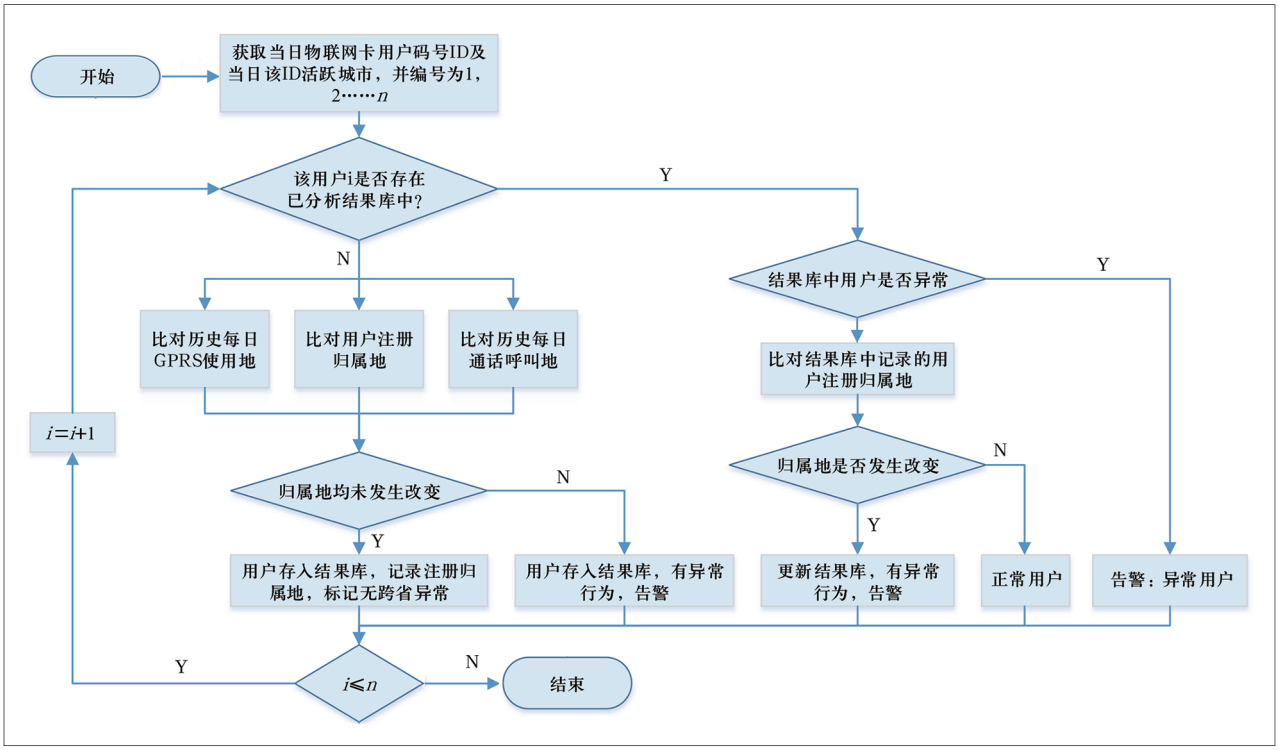

图1 跨省识别流程图

况，以流量使用总量为例，确定其上月日均流量、前3日日均使用总量、前3日每日使用总量等，构成一组用于判定的样本数据。

(5) 以特征 m_j 的当日使用情况作为离群值，采用奈尔检测法确定是否发生相应的业务量使用异常，若统计量大于剔除水平 α^* 对应的临界值，定义该用户的该特征为高度异常，发生告警。

(6) 若 $j>m$，跳至下一步，否则继续执行步骤5。

(7) 跳至步骤3，依次循环识别每个类别 l 中的物联网卡号 i 流量使用情况，直至全量识别完成。

(8) 结束。

具体的流程图如图2所示。

3.3 物联网卡骚扰／诈骗电话行为特征提取

3.3.1 基本特征提取

根据上述基于语音、上网、短信数据表的字段信息，以用户号码为聚合键，可对该号码一天内的使用情况进行整合汇总，总共有6大维度，如图3所示。

在进行物联网卡异常事件检测时，需要对物联网卡的使用特征进行描述，主要涉及六大维度，各维度使用的字段如附表所示。模型中涉及到的主要字段如下。

3.3.1.1 开通业务

由于13位的物联网卡仅能开通一种功能，故根据开通业务维度，可以将开通短信或数据功能的物联网卡号筛除，仅保留开通语音业务的卡号。

3.3.1.2 联系人熵

联系人信息熵可以很好地衡量物联网卡主叫联系人分布的随机程度。联系人随机性越大，信息熵越大。一般来说，物联网卡主叫对象应仅限于其用户，若联系人拨打次数分布不均且随机性较大，则存在诈骗骚扰的嫌疑。信息熵的计算方法：

$$H(x)=\sum_{i=1}^{n}\frac{m_i}{m}\log\frac{m}{m_i} \quad (1)$$

其中，n 为联系人个数，m_i 为联系人 i 的拨打次数，m 为该物联网卡今日总拨打次数。

3.3.1.3 通话时长熵

通话时长信息熵可用于衡量物联网卡与联系人通话

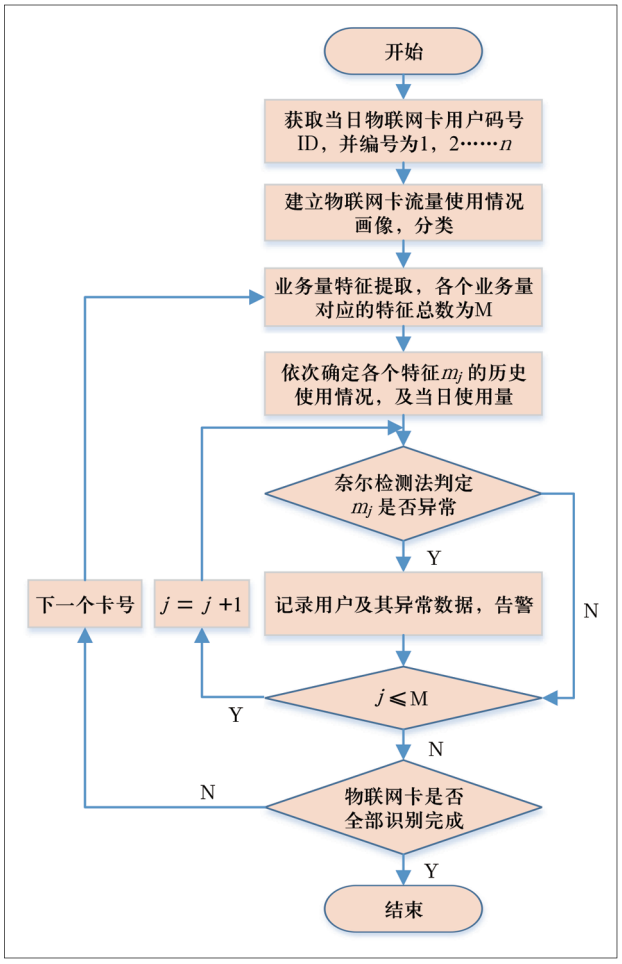

图2 物联网卡业务量异常识别流程图

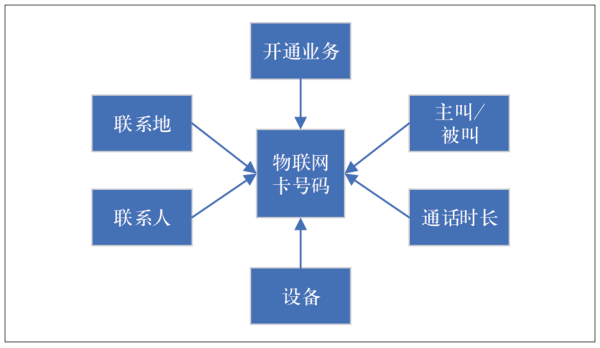

图3 提取的6大特征维度

的时长分布的随机程度。通话时长随机性越大，信息熵越大。一般来说，物联网卡与各联系人间的通话时长应大致相同，若联系人间通话时长不均且随机性较大，则存在诈骗骚扰的嫌疑。通话时长信息熵的计算公式同公式（1）。其中，n 为联系人个数，m_i 为与联系人 i 的通话总时长，m 为该物联网卡今日总通话时长。

3.3.1.4 各时段主叫次数熵

各时段主叫次数信息熵可用于衡量物联网卡在一天中各个时段主叫次数分布的随机程度。各时段主叫量的随机性越大，信息熵越大。一般来说，物联网卡主叫对象的应在一天中主要时段分布较为均匀，若主叫集中于某几个时段且起伏较大，则存在诈骗骚扰的嫌疑。通话时长信息熵的计算公式同公式（1），其中，n 为时段数，m_i 为与时段 i 中该卡主叫次数，m 为该物联网卡今日总主叫次数。

3.3.1.5 联系地熵

联系地信息熵可以很好地衡量物联网卡主叫联系地分布的随机程度。联系地随机性越大，信息熵越大。一般来说，物联网卡主叫对象的归属地应仅限于本地或若干特定地区，若联系地分布不均且随机性较大，则存在诈骗骚扰的嫌疑。联系地信息熵的计算公式同公式（1），其中，n 为联系地个数，m_i 为联系地 i 的拨打次数，m 为该物联网卡今日总拨打次数。

3.3.1.6 设备熵

设备信息熵可以很好地衡量物联网卡所使用设备的随机程度。所使用设备随机性越大，信息熵越大。一般来说，物联网卡应符合专卡专用的原则，在特定设备中使用。若设备频繁更换且随机性较大，则存在利用猫池设备的嫌疑。设备信息熵的计算公式同公式（1），其中，n 为设备个数，m_i 为该号码使用设备 i 的拨打次数，m 为该物联网卡今日总拨打次数。

3.3.2 骚扰／诈骗电话的识别

依据提取后物联网卡的6类特征，分别作基于当日数据离群点分析的异常号码检测和基于历史数据时间序列分析的异常号码检测，结合二者的检测结果，确定卡号是否为骚扰／诈骗电话异常。

具体的识别模型如图4所示。

基于上述的4个维度的物联网卡异常行为识别模型，可以提取出重要的风险行为特征如表2所示。

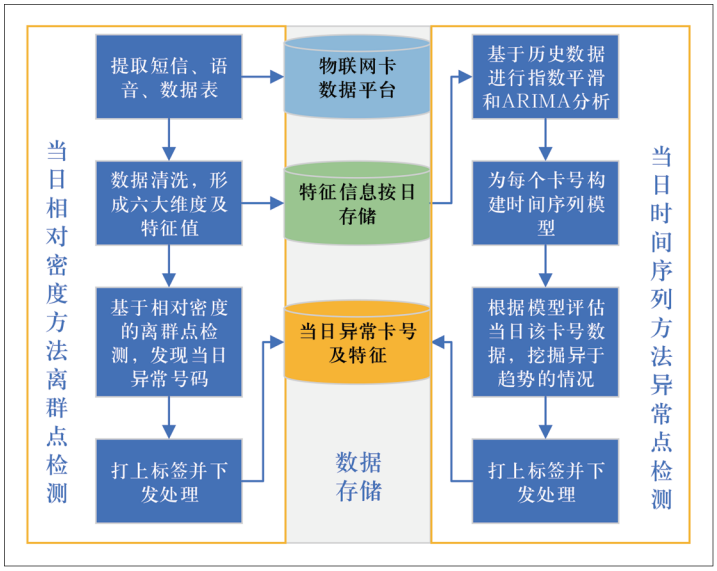

图4 物联网卡骚扰诈骗电话识别模型

4 异常物联网卡提取规则及风险级别定义

根据上节提取的四大维度的物联网卡行为特征，不同的卡号异常行为及风险级别提取策略如表3所示。

表3即为物联网卡异常行为提取策略表，根据物联网卡不同的风险场景和风险 $\tau_1 \sim \tau_{10}$ 分别代表物联网卡10类不同的风险行为特征，“a,b,c,d”等分别代表出现该行为特征，“$-a$”则表示未出现该行为。Decision表示最终的决策，即归属的场景 $d_1 \sim d_6$，Level代表该物联网卡号的风险级别。

表2 风险行为特征汇总表

风险特征	数学符号	具体的对应异常行为
当日语音使用情况	τ_1	主叫频次、通话时长、联系人等 $a \sim f_6$ 类行为
当日短信使用情况	τ_2	短信接收量大小、接收方等 $a \sim c_3$ 类行为
当日流量使用情况	τ_3	流量使用大小、分布情况等 $a \sim c_3$ 类行为
历史语音使用情况	τ_4	基于历史语音使用情况的 $a \sim e_5$ 类行为
历史短信使用情况	τ_5	基于历史短信使用情况的 $a \sim c_3$ 类行为
历史流量使用情况	τ_6	基于历史流量使用情况的 $a \sim c_3$ 类行为
当日IMEI	τ_7	当日是否出现机卡分离行为（$a \sim b$）
当日位置信息	τ_8	当日基站信息是否改变（$a \sim b$）
当日漫游信息	τ_9	当日是否发生漫游（$a \sim b$）
历史存在机卡分离	τ_{10}	历史是否存在机卡分离（$a \sim b$）

5 总结与展望

本文主要是对物联网业务运营风险监控系统的研究，提出了物联网卡风险行为特征的提取方法，并且给出了识别不同风险物联网卡号的策略。基于提出的策略建立的监控系统可以实现对物联网卡的业务监控，告警出现的异常风险卡，保障物联网卡的安全，规避风险。此外，虽然本文提出的监控系统可以实现基本的物联网卡安全保障，但是未来仍旧需要做进一步的完善，具体如下。

通过二次验证物联网卡监控系统的告警数据，优化风险识别模型，提高风险卡识别的准确率。

随着物联网业务的不断发展，丰富新的物联网卡业务运营的风险场景与其相应的识别策略。

表3 物联网卡异常场景提取规则表

τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	τ_9	τ_{10}	Decision	Level
	$-b$			$-b$		a	a		a	d_1	L
	b			b		a	b	$-a$	$-a$	d_1	M
	b			b		a	b	a	a	d_1	H
……											
e			d							d_6	M
f			e					a		d_6	H

News

中国移动助力中央广播电视总台建设我国首个国家级“5G新媒体平台”

2018年12月28日，我国第一个基于5G技术的国家级新媒体平台在中央广播电视总台开建。当天，中央广播电视总台与中国移动、中国电信、中国联通及华为公司在北京共同签署合作建设5G新媒体平台框架协议。

中宣部副部长、国务院新闻办公室主任徐麟，中宣部副部长、中央广播电视总台台长慎海雄，工业和信息化部副部长罗文，国家广播电视总局副局长张宏森，中央网信办总工程师兼网络安全协调局局长赵泽良，中国电信集团有限公司董事长杨杰，中国联合网络通信集团有限公司董事长王晓初，中国移动通信集团有限公司副总经理李正茂，华为技术有限公司董事长梁华等出席签约仪式。

根据协议，中央广播电视总台联合中国移动、中国电信、中国联通、华为公司，合作建设国家级5G新媒体平台。通过联合建设“5G媒体应用实验室”积极开展5G环境下的视频应用和产品创新。“5G媒体应用实验室”将在国内选取10个5G试点城市和相应的测试点，建立端到端的应用试验系统。全力推动5G核心技术在央视4K超高清节目传输中的技术测试和应用验证，研究制定基于5G技术进行4K超高清视频直播信号与文件传输、接收、制作技术规范等5G新媒体行业标准，引领5G新媒体技术应用。

5G网络是信息基础设施的又一次全面升级，能为跨领域、全方位、多层次的产业深度融合提供坚实支撑，将成为我国转型发展中的关键生产要素。5G技术“高速率、低时延、大容量”等特征，为超高清视频技术的大规模应用提供了必备基础，将促进数字内容制作、分发、呈现的全产业链升级。中国移动将全面参与、全力支持此次合作，在加快推进5G规模试验和应用示范的基础上，组建专门团队，深入运用人工智能、大数据、云计算等新技术，携手合作伙伴共筑新媒体产业生态，推动自主可控的5G新媒体平台达到国际领先水平，加快超高清产业的高质量发展。 （来源：中国移动通信集团有限公司官网）

Research on risk monitoring system of Internet of things business operation

ZHAO Jun[1], LIU Hao-ming[1], WANG Wei-jie[2]

(1 China Mobile Group Guangdong Co., Ltd., Guangzhou 510630, China; 2 China Mobile (Hangzhou) Information Technology Co., Ltd., Hangzhou 310012, China)

Abstract Along with the rapid development of Internet of things, a series of security problems have been exposed. This paper first summarizes the risk scenarios in the operation of IoT card business, then discusses the extraction methods of risk behavior characteristics of IoT card, and finally proposes the extraction rules of abnormal behaviors of IoT card, and the IoT business operation risk monitoring system is built to alert and assist in the processing of abnormal network cards to ensure the full operation of IoT.

Keywords Internet of things card; risk monitoring, phone fraud; machine card separation