作者：涵空

针对电商平台上的作弊行为，阿里巴巴一直秉承着零容忍的态度，在虚假交易的识别防控以及处罚力度上没有最强只有更强。经过多年在全球最大的电商平台大数据上的沉淀和积累，阿里电商反作弊形成了一套监控预警、识别分析和处罚管控的多维度监管机制，特别是对虚假交易的数据监控和算法识别上应用了覆盖全链路大数据的实时分析处理能力以及大规模图搜索技术来鉴别作弊行为。

一、淘宝反作弊体系结构

淘宝反作弊体系结构可以从数据、算法、和系统三个维度来解释

数据：主要是将识别的作弊数据汇总到买家、宝贝、订单和卖家四个维度并全量提供给了数据平台供各业务方使用，即可用作算法训练样本的特征，也方便系统查询和监控作弊数据的趋势变化情况；

算法：覆盖了包括账号网、交易网、资金网和物流网四网合一的大数据，彻底打通了售前、售中、售后全链路业务，可以多方位识别各种作弊行为；

系统：主要是建立在数据层基础之上的一套包含监控预警、在线分析和风险运营系统，能快速高效地窥视刷单行踪并及时阻断其获利点；

此外，淘宝反作弊系统还引入了评估体系，是评价淘宝反作弊的效果和价值的一套完整方法，主要包括人工和算法结合的评测，召回率和准确率用来评估算法模型本身的覆盖面和精准度，落地率、纯净率和反弹率来评估业务效果和价值。

二、淘宝反作弊算法

淘宝反作弊算法体系是伴随着淘宝平台而不断优化和完善的，早期作弊的形式非常简单，比如频繁修改商品上下架时间来获取有利的商品排名，这种作弊手段往往经过简单的分析处理就可以制定相关的规则来处理，随着平台业务场景的多元化，作弊手段也随着变化多样，但大部分还是集中在商品基础信息层面上的作弊，比如类目错放、标题词滥用、夸大宣传、低价炒信、广告商品、重复铺货、刷流量和查询词等等，或者机器刷单模式，比如批量注册一批机器账号然后快速刷单来获取高销量。这些刷单手法也主要是针对平台业务不断的壮大和发展见缝插针式的达到获取更多免费流量的作弊方法。随着淘宝业务的不断更新和反作弊算法的不断优化，这种作弊形式也非常容易被识破和处罚。

道高一尺魔高一丈，无论刷单手法多么诡计多端，淘宝反作弊算法体系都能快速响应。其中最重要的就是实现了一套覆盖全链路（售前、售中、售后）大数据（账号网、交易网、资金网、物流网）的实时分析处理能力，因此任何一条隐蔽性强的“精刷”作弊路径都可以被海量大数据从多个点来进行算法建模和交叉分析，从而能快速地识别并控制住风险。淘宝反作弊算法框架大致见下图1。

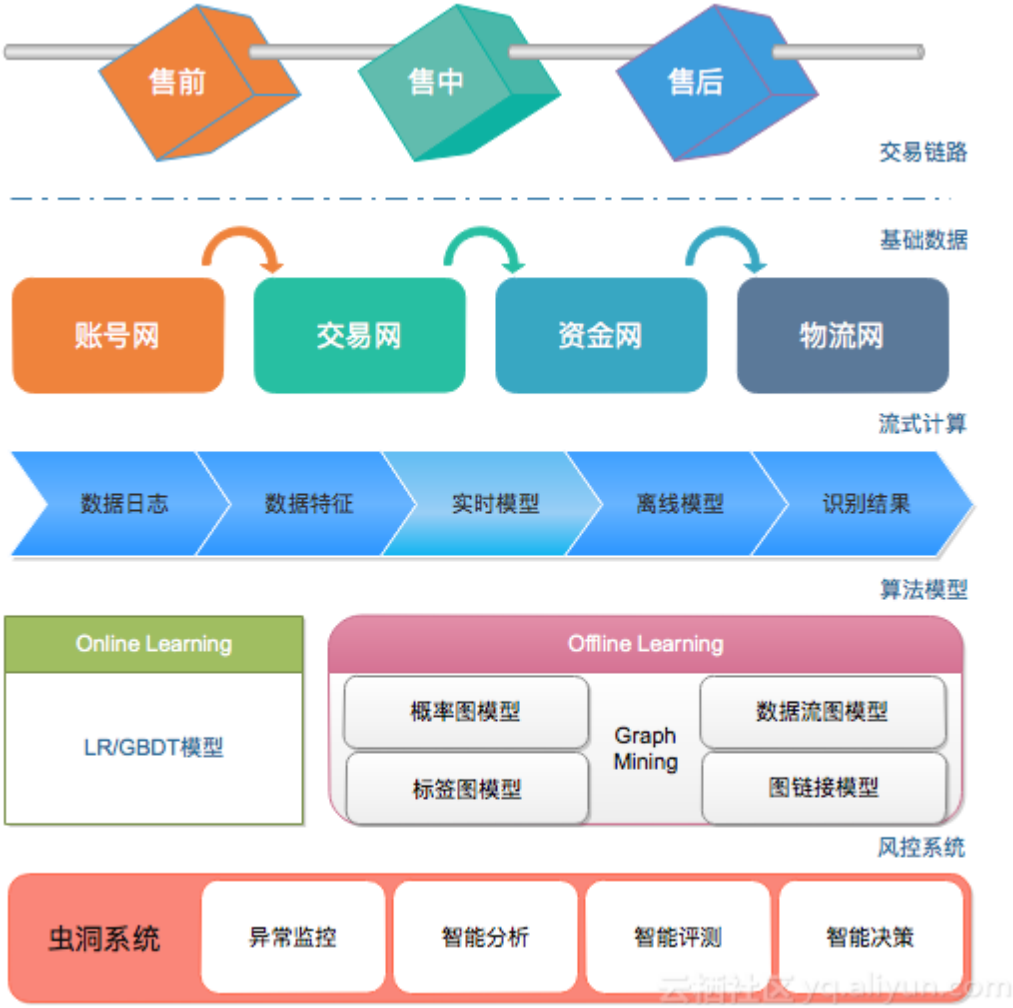


图1、淘宝反作弊算法框架。

岗位描述：

（1）对业务日常反馈的问题，能对相关的数据进行交叉验证和分析，建立相关模型，提高模型的准确性，减低模型的误差率，同时提高算法的健壮性、实时性、安全性和可解释性；

（2）分析作弊行为背后的买家、卖家、平台的关系，构建一个覆盖交易网、资金网、物流网的全链路关系网络，挖掘作弊行为背后的动机和作弊人群不同的行为模式，从数据上提供业务决策和落地的依据；

（3）分析外部舆情和平台的数据，结合识别的结果来预测作弊行为的趋势，以及挖掘传播的方式，从源头上监控作弊的动态

信息，从而采取有效的措施阻止作弊行为的扩散和影响，促进平台生态健康。

岗位要求：

（1）熟悉常用的数据挖掘和机器学习算法，有过GBDT、MLR等分类模型的开发经验，了解常用聚类算法和参数估计模型，对异构数据的融合和挖掘感兴趣；

（2）熟悉马尔科夫链、Bayesian Network Inference、EM、Label Propagation等概率论和图传播的模型，并了解大规模机器学习算法开发平台ODPS-GRAPH、MPI、Parameter Server其中一种的开发流程。

（3）有强烈的责任心和数据安全意识，有团队沟通协作精神，吃苦耐劳，善于总结和分析，熟悉和了解反作弊相关工作的优先。

首先整个反作弊算法框架融合了“账号网、交易网、资金网、物流网”四网大数据，并覆盖了电商“购物前-购物中-购物后”多个业务环节，算法模型是一种流式计算框架，数据日志经过实时和离线两大计算模块后会加工成一些交易属性特征作为识别算法的基础，其中实时计算主要是对一些异常的在线数据（比如商品销量异常或者卖家信誉增长异常）进行快速分析并转化为相应的特征，而离线计算是对全链路数据的特征加工和处理，结合在线和离线的计算可以将行为变化的长期和短期因素的影响在模型计算中综合考虑，从而进一步提高识别的时效性和精度。

淘宝反作弊算法框架主要覆盖了阿里电商两大场景：日常反作

弊和大促反作弊。
算法主要是以大规模图挖掘（Graph Mining）和在线学习（online learning）为核心，
在线学习可以对一些规则性的算法做到实时更新模型用来防范“试探性”地作弊手段，主要是基于规则的的模型（决策树和LR逻辑回归模型），根据一些交易特征建立强规则来进行识别计算，对那种明显的商品作弊模式的识别非常高效；
大规模图挖掘则是通过跳出行为“局部性”的方法考虑行为的“全局性”来深挖“精刷”类型的作弊手段。
(1). 概率图模型对用户行为路径进行时间序列建模（假设正常用户的行为轨迹的时间序列是服从某种概率分布，异常的行为轨迹在某些点上服从其他概率分布），对那种机器刷单或者固定模式刷单能非常有效地识别；
(2). 图标签传播模型可以来做团伙刷单的识别，对炒信平台隐蔽性高组织性强的“精刷”模式的识别非常高效准确。

为了进一步验证算法模型的精准性，反作弊体系也增加了实时干预模块来做交叉验证和分析，主要包括专家知识、人工举报、异常监控和人工评测，这些外部数据源加工处理后可以作为验证数据动态帮助模型进一步优化。
大规模图搜索技术在反作弊中的应用主要体现在下面四类核心算法：
1. 标签图模型：在大规模属性图结构上做社区和团伙挖掘；和以往的分类等机器学习算法不同的是，在属性图上有效地利用标签传播算法分析用户的行为可以挖掘出很多其他算法识别不到的同机团伙和协同炒作团伙；

2.概率图模型：在大规模图结构上挖掘变量之间的关系；利用概率图模型可以有效分析用户信息的风险程度（比如预防用户地址泄密）和用户购物行为链路之间的关联（比如识别账号异常行为）

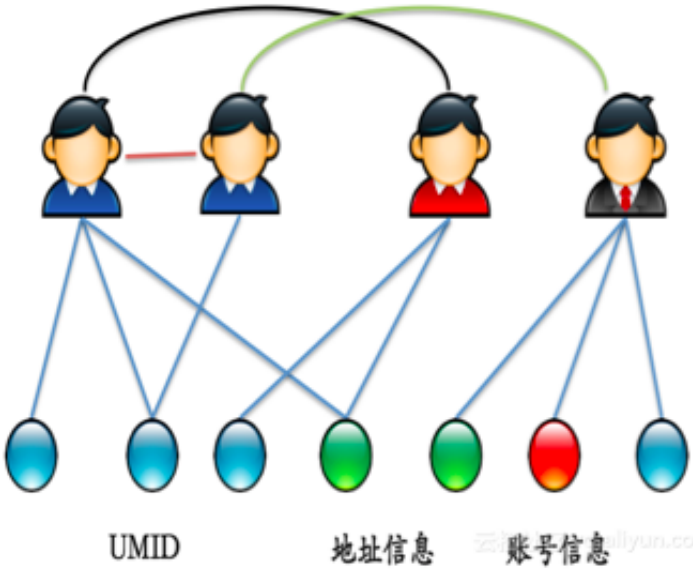
3.数据流图模型：在大规模数据流上挖掘频繁子图，利用数据流挖掘我们在资金流网络中首次发现了由“僵尸账号”通过炒信行为产生的“坍缩网络”，同时构建了一套“转账首活网络”能有效识别这些炒信用户，准确率达到了99.9%；

4.大规模图链接模型：在大规模图数据基础上做排序和权重挖掘，通过这种图链接方法我们有效地发现了重复运单和虚假运单的行为；我们的图算法能并行处理1亿以上节点5亿条边的图数据。在 3千万个节点，2.2亿条边的图数据上调用图链接算法时间仅需要14分钟。同时整个算法框架也包含了实时计算模块，使得对时效性要求高的业务场景下（比如双11）部分算法识别可以实现0秒延迟并可以每15分钟动态调整并跟新所有其他的模型。

三、大数据全链路反作弊示例

淘宝反作弊最核心的部分就是搭建了一个将“账号网、交易网、资金网、物流网”四网合一的全链路大数据的天罗地网，做到全方位无死角的监控和识别任一种作弊行为。

＊账号网：主要是从各种注册信息或登陆信息中来全方位真实了解账号的真实性和平台特性，通过挖掘用户行为的变化情况来有效发现账号行为的异常性（见图3）；


UMID
地址信息
账号信息

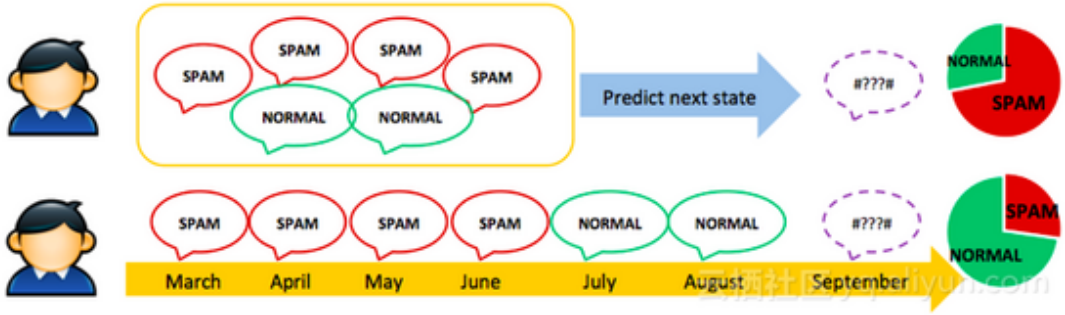

SPAM
SPAM
SPAM
SPAM
NORMAL
NORMAL
Predict next state
#???#
NORMAL
SPAM
SPAM
SPAM
SPAM
SPAM
NORMAL
NORMAL
#???#
March
April
May
June
July
August
September
SPAM
NORMAL

图2、大数据全链路反作弊识别－账号网

＊交易网：主要通过挖掘用户具体的购买行为路径来跟踪是否有异常，这涉及到“售前”（搜索词，点击浏览，详情页等）－“售中”（收藏夹，购物车，支付等）－“售后”（物流，评论，退货等）（见图3）；

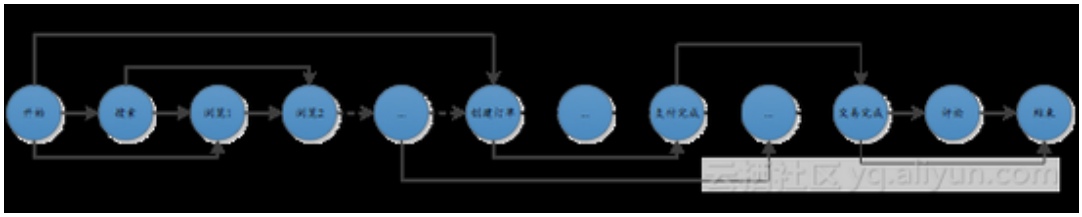


图3、大数据全链路反作弊识别－交易网

＊资金网：主要是通过挖掘资金流的行为来识别一些异常交易

或者洗钱，盗号，套现等高危行为（见图4）；

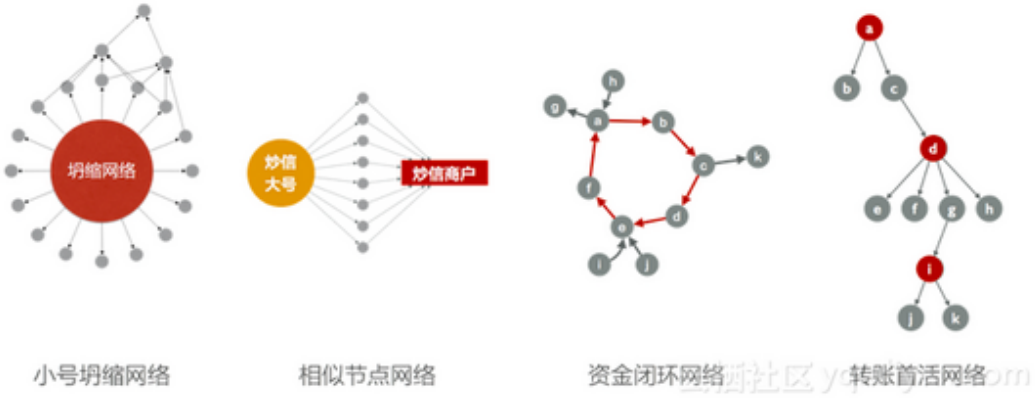


图4、大数据全链路反作弊识别－资金网

＊物流网：主要是通过挖掘交易和物流环节的关联性来识别一些虚假运单和空包等作弊行为（见图5）.

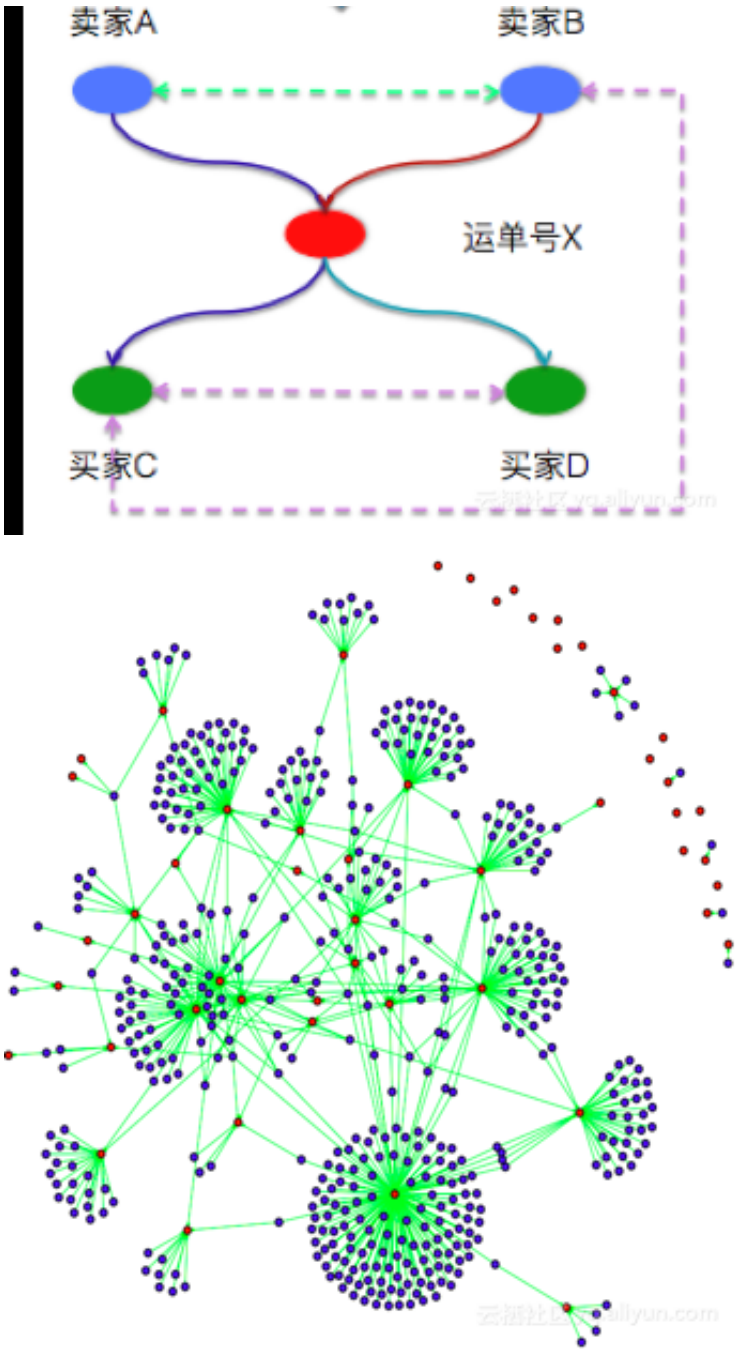


图5、大数据全链路反作弊识别－物流网

四、总结

淘宝反作弊体系已经建立并完善了一套完整的包括“账号网”、“交易网”、“资金网”、“物流网”的大数据分析体系，和覆盖“售前”、“售中”和“售后”的电商全链路的在线学习（Online

Learning）和大规模图挖掘（Graph Mining）算法识别系统。同时还建立了完整的“平台化”风险管控系统-“虫洞”，通过系统监控预警以及在线分析的方式将模型算法和人工运营有效结合起来，不仅能高效识别作弊行为并进行了有效地干预，同时还可以有效控制各种风险。经过日常和大促的洗礼，淘宝反作弊算法体系无论在准确率、覆盖率、反弹率上都能经受任何形式的考验。