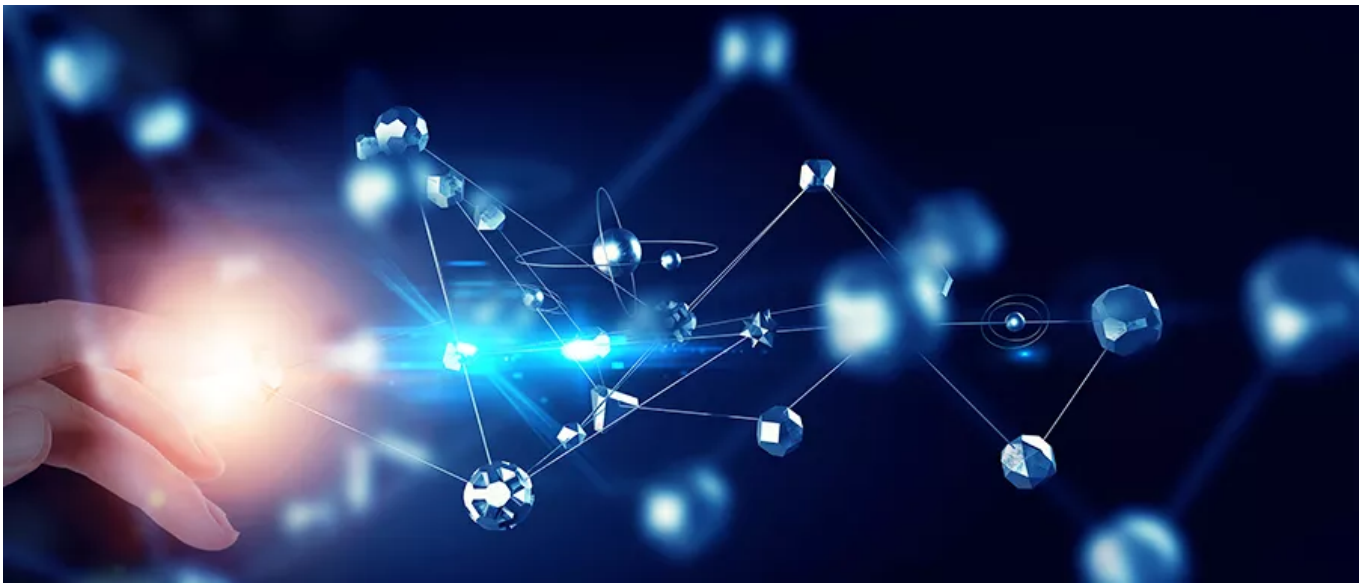
关系图谱在反欺诈场景中的应用及实践

互联网安全实务 1月17日

文章转载自公众号 鲲鱼科技，作者 鲲鱼科技



01 关系图谱概要

随着近几年互联网金融的发展，玲琅满目的信贷产品早已被羊毛党盯上，层出不穷的营销活动更是让欺诈分子有了可乘之机，伪造资料、恶意注册大量虚假账号、团伙包装、刷单、抢红包、套返利等等，他们的欺诈技术手段也越来越高明（群控、云控），成本也越来越低。为了限制这些欺诈用户，信贷机构通过建立反欺诈团队和风控防范体系，使用专家规则和预测模型来拦截欺诈份子。但是道高一尺魔高一丈，再严密的规则也难免有漏洞，被钻空子，传统的反欺诈工具就显得势单力薄。因此关系图谱就有了用武之地。

关系图谱本质就是语义网络，是一种基于图的数据结构，由节点(Point)（“实体”）和边(Edge)（“关系”）组成。把所有不同种类的信息连接在一起而得到的一个关系网络，从“关系”的角度去分析问题，解决问题。目前已被广泛应用于智能搜索、智能问答、个性化推荐、精准营销、风控反欺诈、金融风险预测等领域。具体的关系图谱基础概念本文不再详述，本文重点介绍关系图谱在鲲鱼反欺诈场景中的应用及实践。

02 反欺诈场景中的应用

构建关系图谱的前提就是要把需要的数据从不同的数据源抽取出来存入到图数据库里，所以信息抽取是构建关系图谱的基础。一种是以关系型数据库存储的结构化数据，例如：IP地址、经纬度、设备指纹等，另一种是爬虫采集的非机构化数据，例如行为记录、网上的浏览记录，鲲鱼关系图谱利用机器学习、自然语言处理技术把这些数据变成结构化数据也存入到图谱里。

实体主要包括：IP地址、经纬度、设备指纹、账户、联系人、逾期黑名单等相关信息，关系包括： 从属关系、紧急联系人、互通电话、同一网络等等；整个实体和关系构建了鲲鱼反欺诈的图谱体系。

用户信息交叉校验

校验用户信息可以用来判断借款人是否疑似存在欺诈风险，使用关系图谱做交叉校验，虽然不能保证百分之百的准确，但是它在人工审核时是一个有力的参考依据。例如：比如借款人张三和借款人李四填写的是同一个公司电话，但张三填写的公司名和李四填写的公司名完全不一样，这就是一个可疑点，需要审核人员格外的注意。我们将关系图谱数据可视化，可以很直观的发现两者的矛盾，可以判断他们二人至少有一人存在欺诈行为。再结合用户其他行为数据，如果张三的行为是一个正常用户，那么可以判定李四存在欺诈风险。

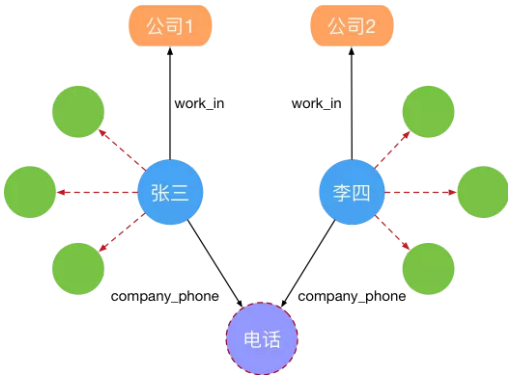


图1 用户信息交叉检验图

团伙欺诈分析

团伙欺诈相对于信息造假、撸羊毛等行为造成的损失更加严重，发现团伙的难度也更大，为了发现团伙，我们通常需要分析多层级的数据，一度关联、二度关联、三度关联，甚至是更多维度关联。通过共享实体找出强连通图，可以帮助我们有效快速的发现隐藏的共同特征。也可以通过一些概率统计的方法，比如：社区挖掘、标签传播、聚类等技术，从图中找出一些社区。

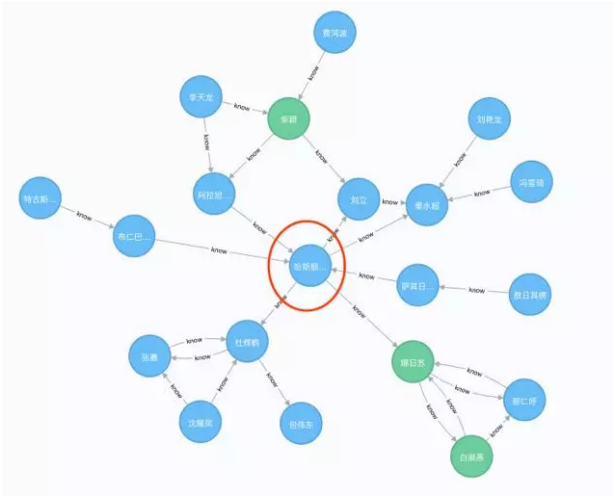


图2 团伙欺诈分析图

失联客户管理

通过用户的注册信息，我们无法联系到借款用户，可能用户已跑路。对于催收人员来说，这个时候根本联系不到用户，甚至是用户填写的联系人也消失的无影无踪。这个时我们可以利用关系图谱去发现失联用户的潜在联系人，提高我们的催收成功率。例如张三是失联用户，李四是张三的联系人，李四也失联了，张三的联系人全部失去联系了，这时我们可以看李四的联系人是否可以与张三有关联，或者查看与张三使用相同设备的用户，在同一个区域的用户等。

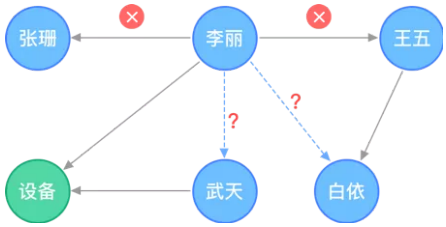


图3 失联客户关系图

03 关系图谱在反欺诈中的实践

关系图谱区别于其他数据存储类型的最重要特征在于其关系可视化，也带来了良好的可解释性。因此，在数以亿计的节点和更庞大的边集合下，将图谱可视化特性充分发挥出来将决定图谱的实际应用价值。鲲鱼科技在关系图谱的实践过程中，对图谱由简单到复杂的结构如何表达做了不同的尝试。

原始图信息

通过D3重构了图谱展示，不同的颜色表示不同的数据类型。本谱图中已经限定了初始节点展示数量和查询层级。用户可以在此图谱的基础上筛选节点和边，点击节点也可以继续拓展更深维度的关系。

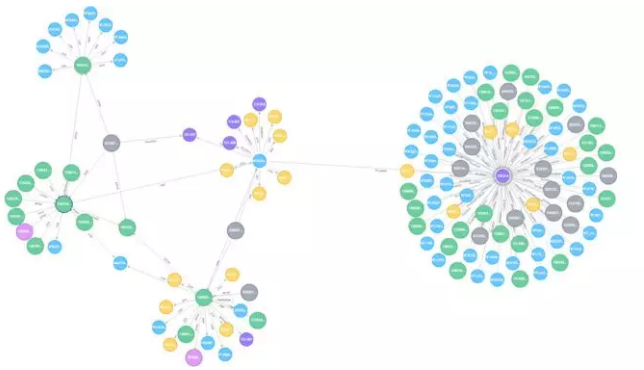


图4 原始图谱信息

黑产简图

在关系图谱运行过程中会不断的尝试去发现并标记恶意用户，以识别欺诈用户和正常用户。这部分被标记的恶意用户具有较高参考价值。恶意群体，往往活跃于不同的平台中，留下他们的足迹，将这些用户记录下来并做重点防护是非常有必要的。同时也对外输出这些欺诈风险用户的核验结果。

A)周边黑产

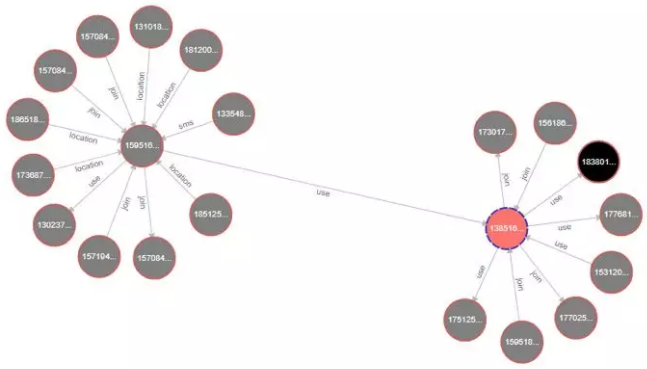


图5 周边黑产图

可以看到，我们提取了待查节点与其周边黑产节点的关联关系并生成简图，给予核查者最初步直观的印象。而图中标记最黑的节点是结合路径长度与路径权重得来的，与待查节点最接近的黑产节点，在核查时相对的会具有更高参考价值。

B)两点关联性查询

无论是通过查看“周边黑产”继而进行后续查询又或者类似于核查“否认交易”的情况，我们都需要拥有一个查询两节点间关联关系的功能。这一功能将展示两节点间所有的关联路径，核查者可以详细分析两者是否具备“强关联”，进而可以通过强关联节点的黑与白来推断待查节点的黑与白。因为两个节点间的关系可能是非常复杂的，因此为方便调查人员使用，在应用的过程中我们将两节点的最短路径及路径中的重要节点单独标记了出来（如下图中的红色节点与红色加粗的边）。图中的节点提供了扩展功能，用户可以根据需要进一步拓展图谱。

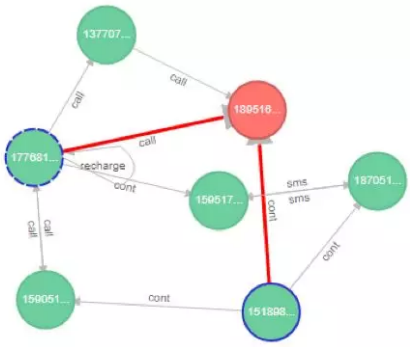


图6 两节点关联关系

社群发现与可疑点挖掘

根据六度空间理论，由单个节点不断向外扩散六度，理想的情况下几乎可以扩展出整个世界。关系图谱中的一些节点，往往可以拓展出数十万甚至百万的关联节点， 即使只是三度以内的连接也可以拓展出上万节点。而如此多的节点是我们所无法直接观察并分析的。同时，虽然有如此多的关联，但是节点往往成团的聚在一起，与其他团之间“弱关联“在一起，提高了调查难度。所以寻找出待查节点所在的真实团体，才能进一步的分析这个团伙。社群在此产生了巨大的价值。

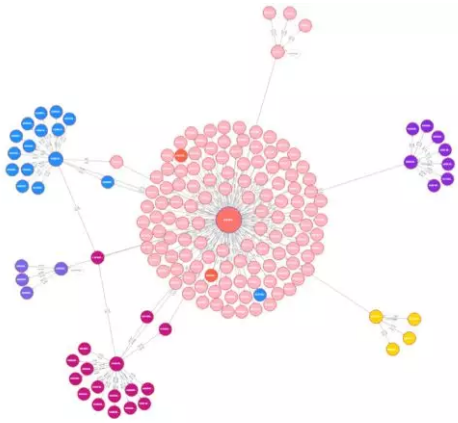


图7 待查接节点三度空间的社群划分图

提取用户直接所在的团，是提供给核查人员分析的基础。如下图所示，我们也可以直观的看到待查节点所在社群中拥有多少黑产节点。

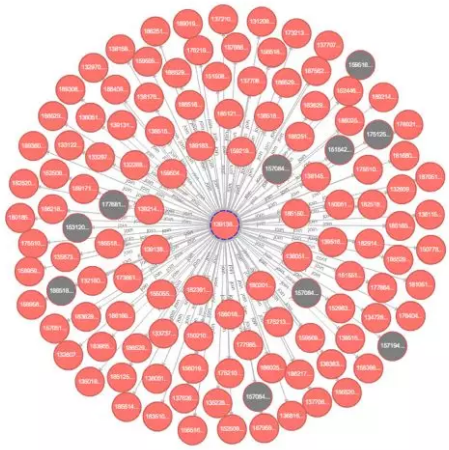


图8 待查接节点所在社群简图

社群算法本身不具备排查恶意节点的能力，即使是基于黑产标记的标签传播算法，在排查恶意节点时也显的有些模棱两可。毕竟，我们的黑产标记不见得全面，黑产节点在巨大的用户群体下，显得及其渺小。如此情况下，单一的占比往往无法提供很好的鉴别能力。因此我们在实践中综合了“社群黑产占比“以及”节点黑产连接度“两项指标来做可疑节点识别。

$$\text{社群黑产占比} = \frac{\textit{黑产节点数量}}{\textit{社群大小}}$$

$$\text{节点黑产连接度 f(node)} = \begin{cases} \sum_{1}^{3} w_i * num_i, & \text{f(node)} < 1 \\ 1, & \text{f(node)} \geq 1 \end{cases}$$

公式中i代表node节点的i层相邻关系，num_i代表在node节点的第i层有num_i个黑产节点；w_i则是第i层黑产节点可以给node节点传染的黑产连接系数。对于黑产连接度，我们统计其周围三度连接内所有黑产节点。认为一度连接的节点可以传播$w_1(0.1)$的值给当前节点，二度连接节点可以传播$w_2(0.05)$的值给当前节点，三度连接节点可以传播$w_3(0.02)$的黑产值给当前节点。那么，如果当前节点的一度相邻中有5个黑产节点，二度有10个黑产节点。这个节点的黑产连接度为1，可疑度较大，我们将该节点标记为灰色。

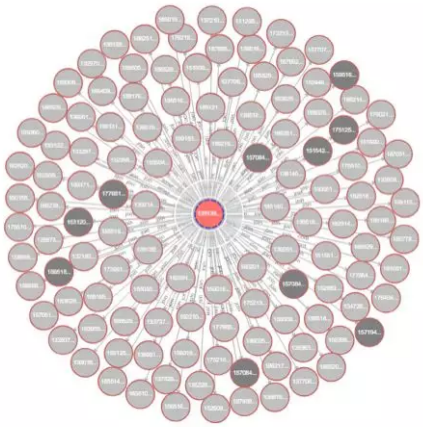


图9 发现社群内可疑节点图

04 总结

1）反欺诈的特点在于行为的隐蔽性、稀释性，群体坏样本量小但聚集度高，对传统方法提出了很多挑战，深度挖掘用户背后复杂的网络关系成为解决团伙欺诈的重中之重。关系图谱技术因为其良好的特征表现方式成为目前反欺诈领域解决团伙欺诈、信息伪造炙手可热的技术。

2）我们对关系图谱初步的尝试和应用也取得了一些成果，成功打击了数百个欺诈、盗刷等黑产团伙，关系图谱的模型也在实战中得到了不断优化。

3）未来我们也将持续利用各种新技术、新手段，新模型、结合互联网风控场景的特征，进一步探索更多行之有效的方法，应用到更多的领域当中。相信在未来2，3年时间里，关系图谱技术会发挥更大的价值。