AI风控落地：同盾科技复杂网络4.0重磅发布 多项创新加码团伙欺诈分析

2018年03月07日14:21　　来源：中国网

原标题：AI风控落地：同盾科技复杂网络4.0重磅发布，多项创新加码团伙欺诈分析

团伙欺诈的泛滥，给传统风控方式带来挑战。同盾科技复杂网络4.0提供实时可视化关联分析，通过更深层信息挖掘和推理，提供动态分析和监测。在反欺诈领域，如实时团伙检测、催收号码识别等，以及客户价值挖掘等均有广泛应用。其中，百亿级金融图数据库（几百万团伙及其成员）、风险传播算法及知识表示学习系首次发布。

一、欺诈趋势：团伙欺诈成顽疾

“穷则变、变则通、通则久”

1.欺诈产业化成新趋势

近年来，传统金融机构业务逐渐互联网化，新金融模式也层出不穷，但金融的本质未变，风控依然是核心。传统金融风险在互联网金融领域依然存在。同时，追求速度的互联网金融也打开了“潘多拉”盒子，“快”意味着效率，也意味着缺陷和额外的风险，事实证明，随着互联网金融的普及，金融欺诈也随之普

及，并大有西风压倒东风之势，让从业者闻“欺诈”色变。

“苟富贵，勿相忘”和“逐利性”，让一部分先“富”起来的人，带动其他人共同“致富”，并逐渐形成了有组织、有纪律和分工明确的欺诈上下游产业链，如专业的技术开发产业、身份信用包装和虚假身份提供产业、业务漏洞发现和欺诈方法传授产业。据不完全统计，仅2017年，中国的网络欺诈导致的损失近5000亿元。“谁割肉，谁痛苦，谁改变”，因此，金融机构团伙反欺诈的需求强烈而迫切，自是不言而喻的。

2.团伙欺诈案例

如下选取三个真实的团伙欺诈案例，相关企业及人名已作模糊化处理。

*案例一：银行信用卡养卡套现

“某团伙在某村庄以招工的名义大量收取村民的身份证，并申请信用卡，然后刷卡透支，让村民背负银行债务。此时，银行按照过往经验便会判定该村地址为欺诈地址，使该村村民抹上信用污点。”风控难点：银行卡套现风险。

*案例二：汽车金融“零首付”中间团伙骗贷

“某团伙打出‘零首付购车’广告，垫付首付款和代办贷款，购车人不花钱即可拿到车。于是，购车人购买价值25万的本田，团伙垫付10万的首付款后，要求先将车开走用于抵押办理高额度信用卡，再从信用卡中取走垫付的首付款。当把车开走后便杳无音信，购车人不仅未拿到车，每月得还6000多元的银行贷款。”风控难

点：中间人团伙骗贷已成为汽车金融风险最高的风险类型。

*案例三：娱乐直播羊毛党薅羊毛

“某团伙利用某直播平台业务拓展需要，利用大量的新用户身份信息注册、登录平台领取红包，成功薅羊毛数百万”。风控难点：快速识别注册、登录或营销场景下，注册手机号或设备风险。

其他如信贷行业、第三方支付、电商、保险等领域的团伙欺诈也犹如雨后春笋般层出叠见，本文不再一一详述。

3.团伙欺诈识别的难点&挑战点

商场如战场，金融领域竞争激烈，若比竞争对手审核快1s或风控正确率多1%，则市场份额会发生根本改变。“知彼知己”是制胜良策，同盾科技作为智能风控服务商，在分析大量真实团伙欺诈案例基础上，化繁为简、归纳总结出团伙欺诈的特点、共性和作案手段，如技术更新快、组织基本稳定、关联关系强，以及为节省成本，通常会重复利用信息、设备和账号等（如图1所示），最终“拨开云雾见月明”，揪出“狐狸尾巴”。

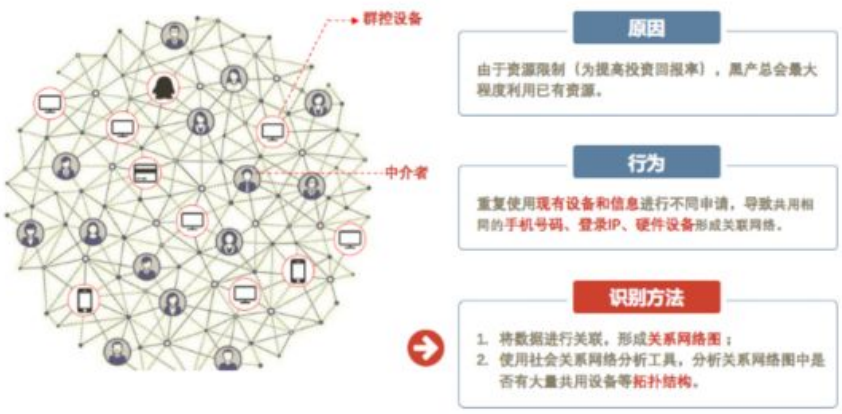

图1：团伙欺诈的特点

团伙欺诈导致风控难度急剧上升，基于线性模型的传统风控，未评估关联关系对风险的影响。“穷则思变”，单纯依靠“增加产品审核流程、全方位的人工调查比对”导致成本居高不下且往往事倍功半，行业迫切需要更多数据源、自动化团伙分析和决策模型。但数据和技术的高门槛让人望而却步，非一朝一夕所能解决。

正所谓“当此困顿之局，唯破局者可立”，同盾科技基于”智能诚信网络”理念、技术的持续创新以及新场景的战略部署，在数据、技术、场景和计算能力方面积累了丰富的实战经验，早在2015年即部署复杂网络技术应对团伙欺诈挑战，经过3年调优，已迭代至复杂网络4.0。

二、破局：同盾科技复杂网络的创新性应用

“工欲善其事，必先利其器”

【知识储备：人类最擅长的思维方式是将点和线关联，并由点及面、抽丝剥茧，逐步理清逻其中的辑推理关系。世间万物是错综复杂的关系网，但无论形式多么复杂，其本质都是简单的三元组，即：实体-关系-实体。】

1.复杂网络产品

（1）复杂网络定义

从概念评述：复杂网络能针对复杂对象的关联关系进行非线性建模，由节点（实体）和节点之间错综复杂的关系（实体之间关系）构成拓扑网络，当异常关系聚集出现时，即可识别欺诈行为。拓展了风险识别的边界和维度，解决了金融场景数据量大、数据复杂和数据不

完整的基本问题，帮助金融机构减少风险，降低风控成本，提高决策效率。

从产品评述：复杂网络是同盾科技核心产品和技术之一，融合同盾大数据和外部数据，提供实时可视化关联分析，将规则、关系及变量通过关系网络表现，通过更深层信息挖掘和推理，提供动态分析和监测。在反欺诈领域，如实时团伙检测、催收号码识别等，以及客户价值挖掘等均有广泛应用

（2）复杂网络技术原理

“打铁还需自身硬”，数据和技术是关键。同盾科技打通跨行业数据及外部数据，结合文本、图片等非结构化数据抽取技术，完成结构化与非结构化信息融合，将时空大数据编织成“实体-关系-实体”的拓扑关系网，当输入“种子数据/线索”，则由点及面、抽丝剥茧，最终顺藤摸瓜找到与之有关联的所有信息，并通过图计算、知识表示和机器学习等技术进行黑中介团伙等的智能化挖掘分析。

图2：同盾科技复杂网技术原理

“知易行难”，同盾科技在复杂网络和知识图谱领域做了深入探索，在关系网络分析中融合组合、数值和

统计思维，积累了一些经验和技巧。在可扩展性算法方面：如局部网络推理、高斯-马尔可夫随机场中取样、稀疏化、图分割、拉普拉斯范式等。数据可视化方面：使用仿真力学模型替代传统的拓扑图关系可视化算法。通过持续的实践-反馈-实践，不断提升复杂网络的精准度。

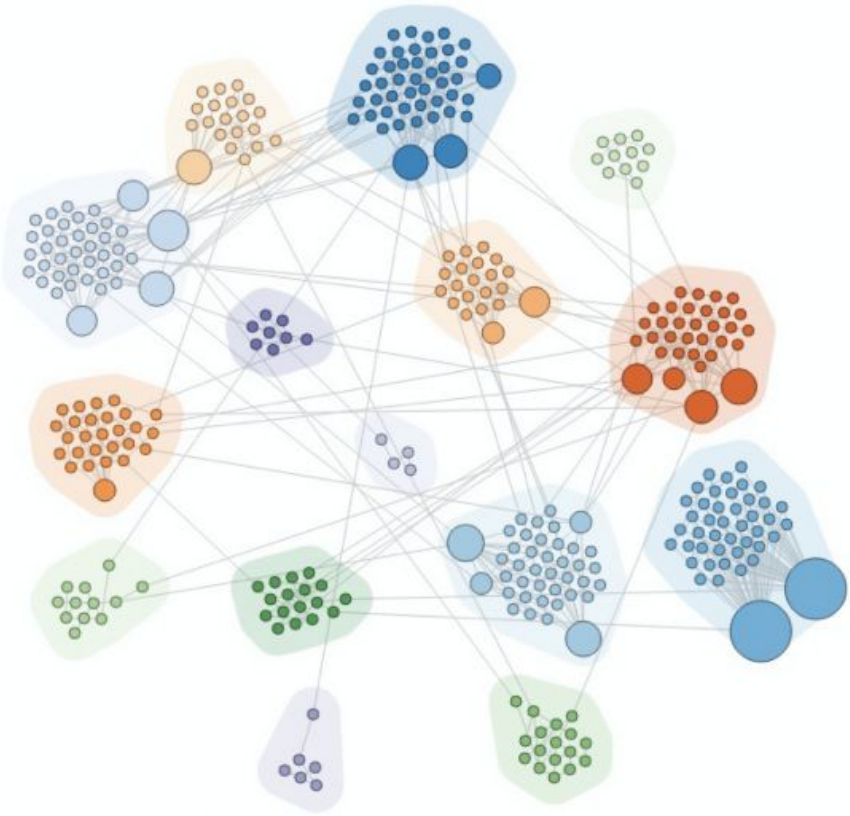

图3：复杂网络图分割探索优化

（3）复杂网络功能

复杂网络在应用上，既可作为产品输出，也可作为技术能力输出。

实时风险群体分析、可视化工作台及风险群体报告是复杂网络作为产品输出的呈现，分别在事前、事中和事后支持欺诈团伙的智能化分析。实时风险群体分析支持灵活的策略配置，可毫秒级返回分析结果（见下图），如：关联风险分、丰富的量化指标、关系图和建

议，直观呈现欺诈团伙的组织形式、核心成员、地址及时间特性。可视化工作台可进行数据动态关联分析，如分析人员聚类、时间聚类、地址聚类等。风险群体报告则可针对批量数据进行团伙风险分析。

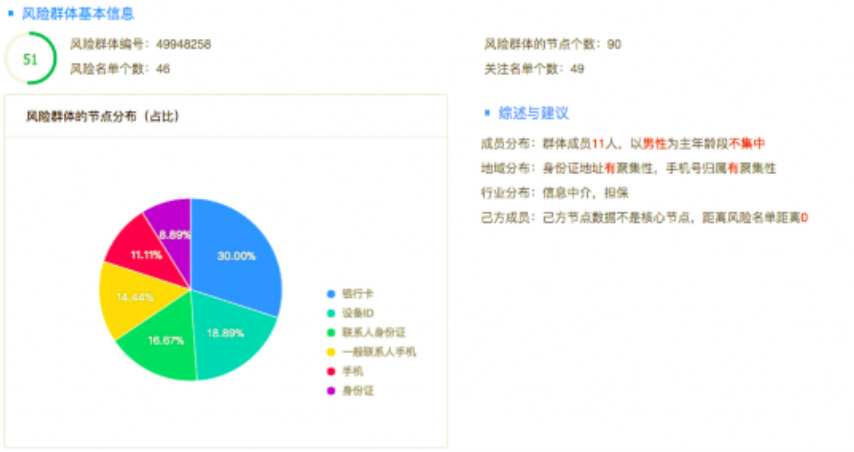

图4：实时风险群体分析结果

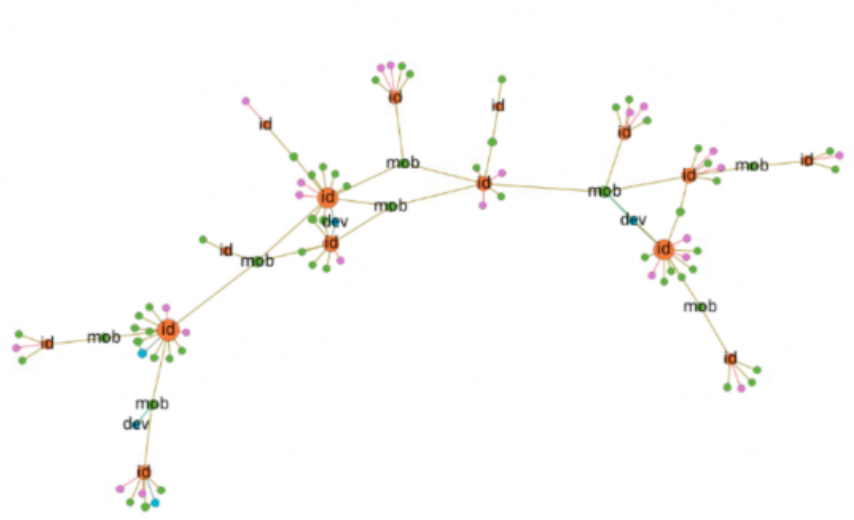

图5：实时风险群体分析分布图（中介团伙分布图，相关详情已脱敏隐去）

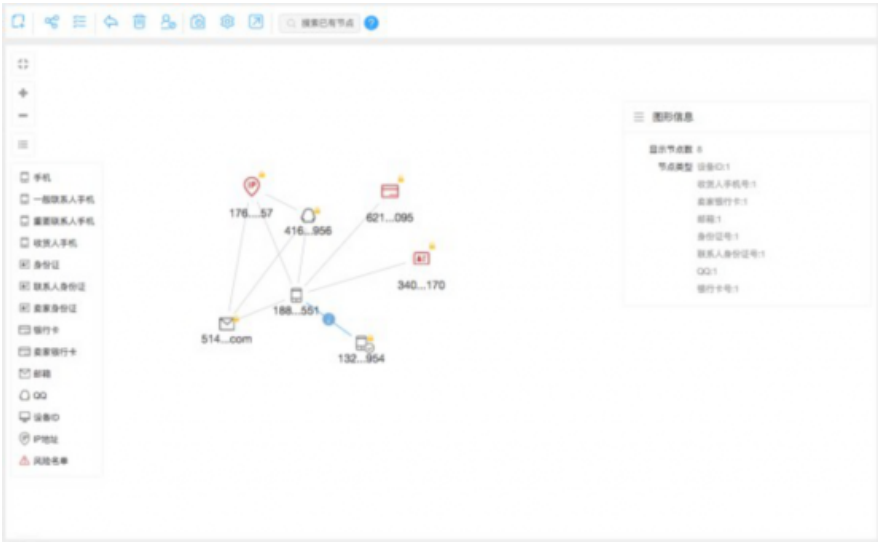

图6：可视化工作台界面

复杂网络作为技术能力输出，在催收号码识别、客户价值挖掘等产品有应用。

（4）复杂网络应用场景

复杂网络支持全场景的实时数据可视化分析，如：银行养卡套现、申请欺诈检测、账户保护、羊毛党识别、恶意刷单作弊等。

2.复杂网络4.0的创新性

“以终为始”，反欺诈效果是关键，创新性体现在三个层面：

其一，数据层面：多源数据融合+NLP，重构金融图数据库。

“数据比技术更重要”是行业共识，有高质量数据，即使简单算法，也能取得好效果。复杂网络4.0融合多来源数据，重构数据清洗、信息抽取和融合方案，使用全新图数据库框架，重构金融图数据库，新图数据库具有分布式、高可扩展性和可维护性，可支持千亿级数据毫秒级实时查询响应。同时，使用NLP技术，将非结

构化与结构化数据融合，形成包含100亿节点（实体）、300亿边（关系）的金融图谱。

其二，技术层面：结合风险传播算法、知识表示和机器学习，进行深度挖掘分析，开启AI风控。

风控作为金融平台竞争力的核心，最早依赖于规则架构，后来演化为规则加模型架构，现在趋向于 AI。AI 风控体现在两方面：风险传播算法、知识表示和机器学习。

1.风险传播算法

风险传播算法依据“近朱者赤，近墨者黑“的原理，从已知风险节点角度评估整个网络节点的风险程度。利用网络结构进行风险传播，进而提高风险节点的覆盖度。

2.知识表示和机器学习

构建数据关系网络是“智能分析”的第一步，利用合适方法将数据价值充分发挥，进而挖掘未知的关联才是目的。使用network embedding方法将高维信息映射到低维空间，解决数据稀疏问题，使知识融合和推理的性能显著提升，结合机器学习，利用无监督算法进行风险群体的识别。实际应用中，通过机器学习对图分割算法不断调优，划分不同的团伙和团伙特征，对判断团伙性质有重要决策作用，如"30%的节点为风险名单"、"40%的节点命中疑似垃圾注册风险类型"。

其三，应用层面：行业化+本地化并驾齐驱，复杂网络全方位技术输出。

数据壁垒导致通用关系网无法适应行业特性，在抽取行业特征基础上、消除噪声、构建行业化关系网络势在必行，如：信贷关系网络、汽车金融关系网络、保险关系网络、羊毛党关系网络等，提高反欺诈效果。

针对银行、汽车金融及保险公司，在风控云方案之外，本地化部署也是着力点之一，可解决强监管，数据无法上“云”的问题。由于本地化数据业务闭环属性更强，数据更全面，在标签数据基础上，可深度优化有监督学习模型，取得更精准的效果。但无论本地化数据量级多大，相对于跨行业大数据而言，都是“小数据“。融合本地化数据与同盾大数据，结合监督算法和无监督算法，进一步反哺原有本地化风控规则，完善本地化方案的不足，进而提高反欺诈效果。

复杂网络作为技术能力全方位向同盾各产品线输出，如评估系统性风险的小微企业的担保关系圈、催收号码识别及基于关系网络的客户价值挖掘等。

三、实践：典型案例及应用示例分析

“实践是检验真理的唯一标准”

1.银行信用卡养卡套现

【行业风险点】信用卡非法套现。

【案例分析】案例一，银行可以利用复杂网络，抽取现数据关联性，从关联中分辨出是否使用类似的电话号码、地址以及区域，将关联属性与其他金融数据输入深度学习网络做有监督的训练，在数十万欺诈案例数据上得到一个动态识别模型。

【复杂网络分析】两个人共用一套信息（手机号和身份证），进而逐步关联，形成链条型关系网络。

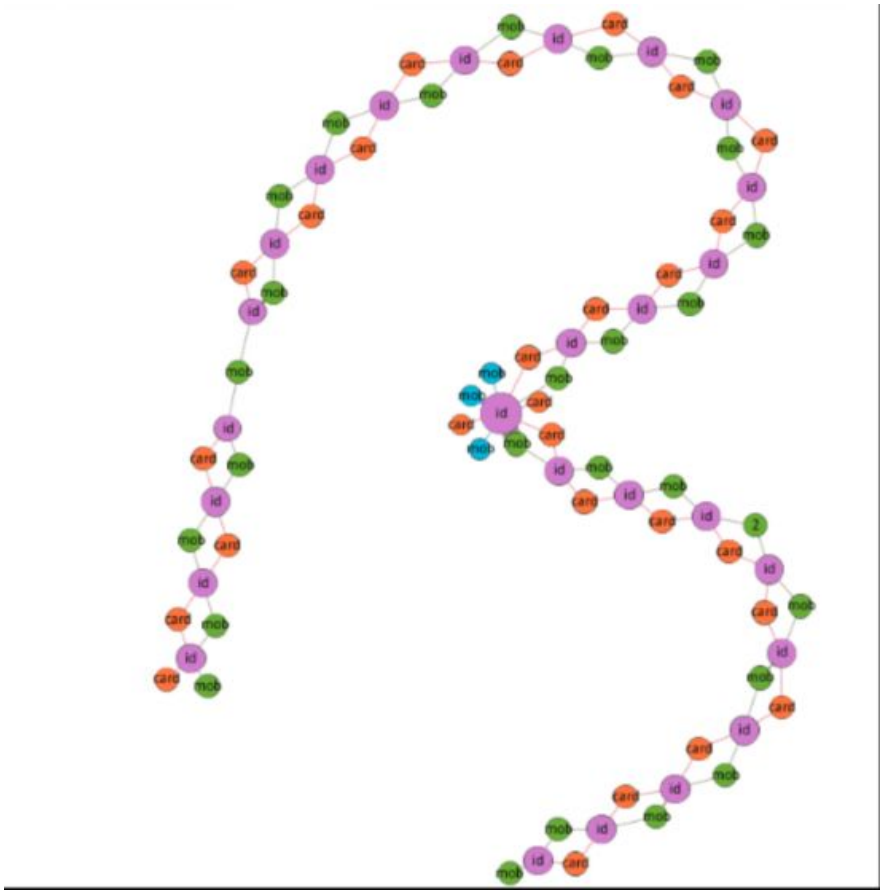

图7：复杂网络分布图（id=身份证，mob=手机号，card=银行卡）

2.汽车金融中介欺诈

【行业风险点】汽车金融是特殊的金融产品，风控难点：如身份伪造、中介欺诈、团伙欺诈、骗车二抵等，二手车金融作为最有潜力的产品之一，其团伙欺诈风险尤其泛滥。

【案例分析】案例二的汽车金融团伙欺诈，具有典型的地域性和组织性。

【复杂网络分析】

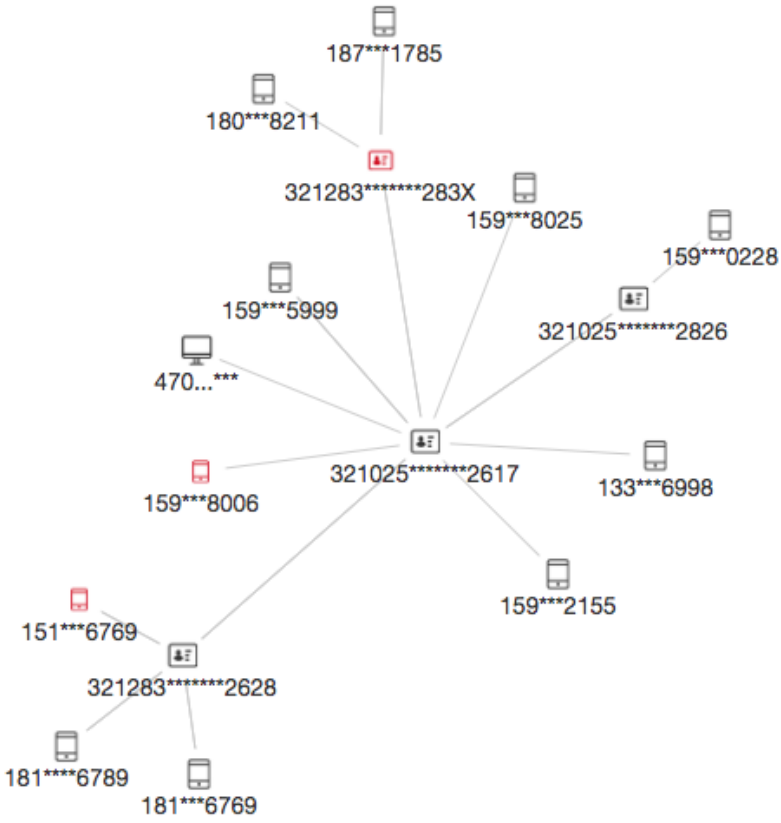

图8：复杂网络分布图

3.直播娱乐羊毛党识别

【行业风险点】消费金融、娱乐直播等行业推出的优惠活动，吸引羊毛党们有组织的参加，逐渐形成了羊毛党“专业化”、“组织化”和“地域化”的发展趋势。

【案例分析】案例三可通过复杂网络识别注册、登录手机号或设备群体风险，找出团伙的核心成员，分析地址聚集性和组织形式等。

【复杂网络分析】箭头所指手机号未知风险，单纯通过专家规则无法识别其风险。但通过复杂网络分析可知，该手机号所关联的设备与大量虚假号码关联（羊毛党典型特征），因而可判定箭头所指手机号为虚假号码，为羊毛党所掌控。

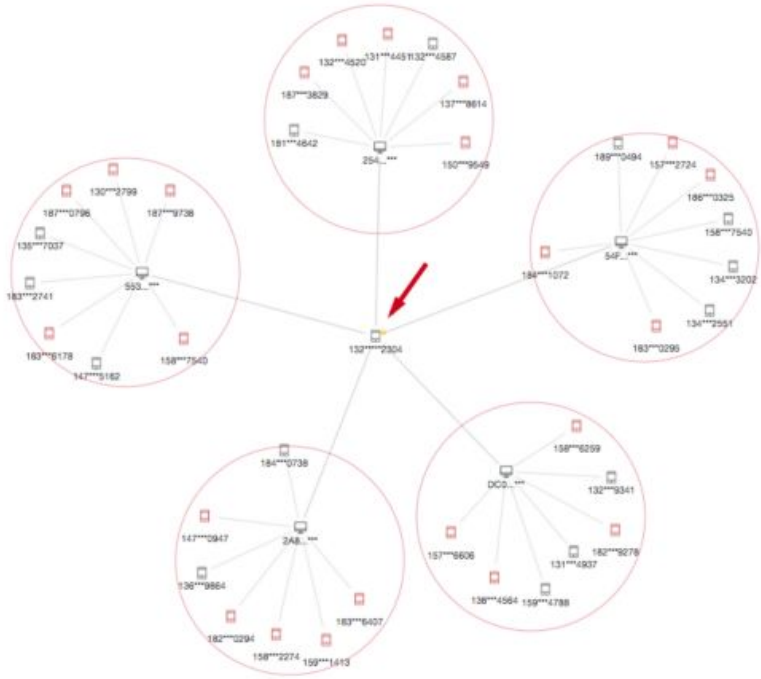

图9：复杂网络分布图

“行百里者半九十”，同盾科技复杂网络4.0是又一个新起点。未来，将不断推陈出新、加快产品技术迭代，如：关系类型深度挖掘推理、资金链关系图等。在应用领域，与银行、汽车金融和保险领域深度融合，如保险领域的理赔反欺诈场景，如车险，医疗险等场景的团伙欺诈分析，进一步提高团伙欺诈风险识别的精准度和效率。

（责编：朱传戈、李昉）

推荐阅读

肖捷：2018年减税降费三管齐下 将提高个人所得税起征点

人民网北京3月7日电　今日上午，十三届全国人大一次会议新闻中心举行记者会，财政部部长肖捷，副部长史耀斌、胡静林就“财税改革和财政工作”相关问题回答中外记者提问。 财政部部长肖捷在会上表示，过去的一年，在以习近平同志为核心的党中央坚强领导…【详细】

产经频道