

一种欺诈团伙的识别方法和装置

技术领域

[01]本公开涉及互联网技术领域，特别涉及一种欺诈团伙的识别方法和装置。

背景技术

5 [02]近年来，互联网欺诈犯罪的气焰越来越嚣张，特别是团伙犯罪。诈骗犯罪团伙可以利用互联网平台招揽客户，采取各种方式实施诈骗，欺诈者可以更换新身份，注册新账号，或者利用多个身份，注册不同账号，将欺诈行为分散到不同账号，使反欺诈系统更难识别。在这个背景下，为了对欺诈的防控开展卓有成效的工作，对于欺诈团伙的识别，
10 可以基于关系网络开发用于挖掘犯罪团伙的团伙识别模型，以在识别到团伙后进行有力的打击。

发明内容

[03]有鉴于此，本说明书一个或多个实施例提供一种欺诈团伙的识别方法和装置，以提高团伙识别的准确度。

[04]具体地，本说明书一个或多个实施例是通过如下技术方案实现的：

15 [05]第一方面，提供一种欺诈团伙的识别方法，所述方法包括：

[06]构建包括多个节点的关系网络；

[07]基于所述关系网络进行聚类发现，得到所述关系网络包括的至少一个欺诈团伙，每一个所述欺诈团伙包括多个所述节点；

20 [08]由所述欺诈团伙包括的节点中确定弱节点，所述弱节点是与所述欺诈团伙的关联符合弱关联条件的节点；

[09]将所述欺诈团伙中的所述弱节点去除，识别得到最终的目标欺诈团伙。

[10]第二方面，提供一种欺诈团伙的识别装置，所述装置包括：

[11]网络构建模块，用于构建包括多个节点的关系网络；

25 [12]聚类处理模块，用于基于所述关系网络进行聚类发现，得到所述关系网络包括的至少一个欺诈团伙，每一个所述欺诈团伙包括多个所述节点；

- [13]节点确定模块，用于由所述欺诈团伙包括的节点中确定弱节点，所述弱节点是与所述欺诈团伙的关联符合弱关联条件的节点；
- [14]剪枝处理模块，用于将所述欺诈团伙中的所述弱节点去除，识别得到最终的目标欺诈团伙。
- 5 [15]第三方面，提供一种欺诈团伙的识别设备，所述设备包括存储器、处理器，以及存储在存储器上并可在处理器上运行的计算机指令，所述处理器执行指令时实现以下步骤：
- [16]构建包括多个节点的关系网络；
- [17]基于所述关系网络进行聚类发现，得到所述关系网络包括的至少一个欺诈团伙，每一个所述欺诈团伙包括多个所述节点；
- 10 [18]由所述欺诈团伙包括的节点中确定弱节点，所述弱节点是与所述欺诈团伙的关联符合弱关联条件的节点；
- [19]将所述欺诈团伙中的所述弱节点去除，识别得到最终的目标欺诈团伙。
- [20]本说明书一个或多个实施例的欺诈团伙的识别方法和装置，通过将团伙中的弱节点去除，将团伙中一些联系较弱的节点去掉，优化了团伙识别的精度，并且也优化了团伙
- 15 的大小，有助于提高团伙识别的准确度。

附图说明

- [21]为了更清楚地说明本说明书一个或多个实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书一个或多个实施例中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。
- 20 [22]图 1 为本说明书一个或多个实施例提供的欺诈团伙的识别方法的流程图；
- [23]图 2 为本说明书一个或多个实施例提供的关系网络示意图；
- [24]图 3 为本说明书一个或多个实施例提供的团伙去除链接边的示意图；
- [25]图 4 为本说明书一个或多个实施例提供的弱节点去除的示意图；
- 25 [26]图 5 为本说明书一个或多个实施例提供的弱节点去除的示意图；
- [27]图 6 为本说明书一个或多个实施例提供的团伙细分的示意图；

[28]图 7 为本说明书一个或多个实施例提供的一种欺诈团伙的识别装置的结构;

[29]图 8 为本说明书一个或多个实施例提供的一种欺诈团伙的识别装置的结构。

具体实施方式

[30]为了使本技术领域的人员更好地理解本说明书一个或多个实施例中的技术方案，下面将结合本说明书一个或多个实施例中的附图，对本说明书一个或多个实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书一个或多个实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本公开保护的范围。

[31]本说明书一个或多个实施例的欺诈团伙的识别方法，可以应用于识别欺诈团伙，例如，基于互联网平台实施诈骗犯罪的团伙组织。

[32]图 1 示例了该欺诈团伙的识别方法的流程图，可以包括：

[33]在步骤 100 中，构建包括多个节点的关系网络。

[34]本步骤中，关系网络中的节点，例如可以是用户账户，或者是用户设备，还可以是其他类型的节点。所述的节点可以作为一个团伙犯罪中的犯罪个体。

[35]以用户账户为例，可以将不同用户各自的转账账户作为节点。不同的节点之间，如果节点间存在账户间共享的介质，例如，该共享介质可以是账户之间在转账交易时使用的共同的设备、指纹、证件号、关联账户、Wifi、LBS 等，若两个节点间存在至少一个共享介质，则可以在这两个节点之间连接一条边，称为节点间的链接边。

[36]请参见图 2 示例的关系网络，该网络中可以包括 15 个节点，其中，存在共享介质的节点之间具有链接边。这些节点和链接边组成了关系网络。

[37]此外，需要说明的是，在该关系网络中的各个节点，可以是至少存在欺诈风险的节点。比如，可以是其中一部分节点是已经确认为欺诈的节点，发生过欺诈交易，还有一部分节点是与该确认欺诈的节点有过共享介质，但尚未确认发生过欺诈交易的节点，可以将这部分节点认为是存在欺诈风险或者欺诈嫌疑的节点。本例子中，可以由确认欺诈节点或者欺诈嫌疑节点组成的关系网络中，挖掘可能存在的欺诈团伙。

[38]在步骤 102 中，基于关系网络进行聚类发现，得到所述关系网络包括的至少一个欺诈团伙，每一个所述欺诈团伙包括多个所述节点。

[39]本步骤中，可以基于已经建好的关系网络，挖掘该网络中包括的欺诈团伙。

[40]例如，可以运用标签传播聚类算法，进行社区发现，挖掘关系网络中包括的欺诈团伙。以图 2 为例，经过聚类发现，其中的节点 1 至节点 11 可以聚成一个团伙，节点 12 至节点 15 可以聚成另一个团伙。

- 5 [41]团伙的发现，可以是团伙中包括的各个节点之间的关联性比较强，比如，这些节点之间存在比较多的共享介质，或者发生过多次的转账交易。

[42]在步骤 104 中，由所述欺诈团伙包括的节点中确定弱节点，所述弱节点是与所述欺诈团伙的关联符合弱关联条件的节点。

- 10 [43]例如，可以使用“弱关联条件”来限定何种节点是弱节点。该条件可以根据业务实际情况来自主确定。如下列举两个弱节点的例子，但实际实施中并不局限于此。

[44]在一个例子中，“弱关联条件”可以是“与欺诈团伙中其他节点之间的链接边的数量，少于预设的边数量阈值”。根据该条件，在关系网络挖掘出的团伙中，若一个节点与所述欺诈团伙中其他节点之间的链接边的数量，少于预设的边数量阈值，则可以确定所述节点是符合弱关联条件的弱节点。

- 15 [45]请继续参见图 2 的例子，节点 11 与所在团伙之间的链接边只有“11-10”这一条边，而假设边数量阈值是 1，且将链接边数量小于等于 1 的节点作为弱节点，那么节点 11 符合上述的弱关联条件。可以确定节点 11 是弱节点。

- 20 [46]在另一个例子中，“弱关联条件”还可以是“与欺诈团伙中其他节点之间的链接边的边权重，低于预设的权重阈值”。根据该条件，在关系网络挖掘出的团伙中，若一个节点与所述欺诈团伙中其他节点之间的链接边的边权重，该边权重例如可以是多条权重的平均值或者总和值，低于预设的权重阈值，则可以确定所述节点是符合弱关联条件的弱节点

- 25 [47]仍以图 2 为例，即使一个节点在团伙中与其他各节点之间存在多条链接边，但是该多条链接边的边权重低于预设的权重阈值，也将被确认为弱节点。例如，节点 6 分别与节点 7、节点 8 和节点 5 之间存在链接边，每一条链接边都可以具有对应的边权重，该边权重可以根据节点之间的共享介质的数量，或者转账交易的次数等因素综合确定，一条链接边的边权重可以用于衡量该链接边对应的两个节点之间的联系频繁度、关联的强弱等。例如，可以将这三条链接边的边权重求取平均值，或者将这三条链接边的边权重进行加和，得到的平均值或者加和值可以称为节点 6 对应的边权重。一个节点对应的

边权重若低于预设的权重阈值，则可以认为节点符合弱关联条件，可以确认为弱节点。

- [48]此外，在确认弱节点前，可以将由关系网络挖掘得到的至少一个欺诈团伙中，将不同团伙之间的团伙链接边去除。例如，以图 2 为例，假设节点 1 至节点 11 可以聚成一个团伙，节点 12 至节点 15 可以聚成另一个团伙，可以将节点 9 与节点 13 之间的链接边(可以称为团伙链接边，即该团伙链接边连接的两个节点分别属于不同的团伙)去除，并将节点 2 与节点 12 之间的团伙链接边去除。请参见图 3 的示例，在去除团伙链接边后，得到了两个独立的团伙。

[49]在步骤 106 中，将所述欺诈团伙中的所述弱节点去除，识别得到最终的目标欺诈团伙。

- 10 [50]本步骤中，分别在每一个团伙中，去除掉步骤 104 中确定的弱节点。并且，弱节点的去除可以采用循环去除的方式。

- [51]例如，参见图 4 和图 5 的示例，首先，在图 4 中，可以根据弱关联条件，去除了节点 9 与节点 1 之间的链接边，相当于将节点 9 由团伙中去除，还去除了节点 11 与节点 10 之间的链接边，相当于将节点 11 由团伙中去除。接着，在图 5 中，继续根据弱关联条件进行判定，将节点 10 又确定为弱节点，因为该节点 10 也是只具有一条链接边，那么在图 5 中可以将节点 10 与节点 5 之间的链接边去除。去除了节点 9、节点 11 和节点 10 后，剩余的节点具有的链接边的数量都大于 1，不是弱节点。

- [52]此外，采用上述的循环去除弱节点的方式，可以将每一个欺诈团伙中的全部弱节点去除。实际实施中，也可以只去除部分弱节点，比如，如图 4 的示例，将节点 11 和节点 9 去除，但是可以保留节点 10。部分弱节点的去除在一定程度上也可以提高团伙识别的精度，具体去除多少弱节点，可以根据业务情况设定，例如，可以预设设定待去除的弱节点的数量上限。

- [53]本例子的欺诈团伙的识别方法，通过将团伙中的弱节点去除，将团伙中一些联系较弱的节点去掉，优化了团伙识别的精度，并且也优化了团伙的大小，有助于提高团伙识别的准确度。

[54]此外，在去除了团伙中的弱节点之后，如果去除所述弱节点后的欺诈团伙仍然符合团伙细分条件，则可以继续对去除弱节点后的欺诈团伙进行聚类发现，即继续对团伙进行细分。

[55]例如，团伙细分条件包括但不限于如下两种，既可以将如下列举的两种条件分别考

虑,也可以将两种条件综合考虑:

[56]若欺诈团伙中包括的节点数量大于节点数量阈值,则继续细分该团伙;

[57]或者,若欺诈团伙的欺诈案件浓度低于预设的案件浓度阈值,则继续细分该团伙。

所述的欺诈案件浓度例如可以是,该团伙中节点执行的欺诈交易数量占团伙交易总数的

5 比例。

[58]以图 5 为例,假设去除弱节点后,节点 1 至节点 8 的团伙仍然比较大,节点数量大于节点数量阈值,则可以使用标签传播聚类算法,继续该团伙进行挖掘细分,细分后同样可以进行弱节点的去除。例如,经过再细分后,节点 1 至节点 8 的团伙可以被分为两个团伙,参见图 6 所示,一个是节点 1 至节点 4 组成的团伙,另一个是节点 5 至节点 8

10 组成的团伙。

[59]经过对团伙不断的优化,最终识别到的团伙可以称为目标欺诈团伙,该目标欺诈团伙已经具备了很好的精度,可以计算其关联强度、欺诈案件浓度等参数,并推送给欺诈策略团队进行打击,从而提高了团伙打击的准确率。

[60]为了实现上述的欺诈团伙的识别方法,本说明书一个或多个实施例还提供了一种欺诈团伙的识别装置。如图 7 所示,该装置可以包括:网络构建模块 71、聚类处理模块

15 72、节点确定模块 73 和剪枝处理模块 74。

[61]网络构建模块 71,用于构建包括多个节点的关系网络;

[62]聚类处理模块 72,用于基于所述关系网络进行聚类发现,得到所述关系网络包括的至少一个欺诈团伙,每一个所述欺诈团伙包括多个所述节点;

20 [63]节点确定模块 73,用于由所述欺诈团伙包括的节点中确定弱节点,所述弱节点是与所述欺诈团伙的关联符合弱关联条件的节点;

[64]剪枝处理模块 74,用于将所述欺诈团伙中的所述弱节点去除,识别得到最终的目标欺诈团伙。

[65]在一个例子中,节点确定模块 73,具体用于:

25 [66]若所述节点与所述欺诈团伙中其他节点之间的链接边的数量,少于预设的边数量阈值,则确定所述节点是符合弱关联条件的弱节点;

[67]或者,若所述节点与所述欺诈团伙中其他节点之间的链接边的边权重,低于预设的权重阈值,则确定所述节点是符合弱关联条件的弱节点。

[68]在一个例子中，如图 8 所示，该装置还可以包括：团伙细分模块 75，用于在所述剪枝处理模块将所述欺诈团伙中的所述弱节点去除之后，若去除所述弱节点后的欺诈团伙符合团伙细分条件，则继续对去除弱节点后的所述欺诈团伙进行聚类发现。

5 [69]上述实施例阐明的装置或模块，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

10 [70]为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书一个或多个实施例时可以把各模块的功能在同一个或多个软件和/或硬件中实现。

[71]上述图中所示流程中的各个步骤，其执行顺序不限制于流程图中的顺序。此外，各个步骤的描述，可以实现为软件、硬件或者其结合的形式，例如，本领域技术人员可以将其实现为软件代码的形式，可以为能够实现所述步骤对应的逻辑功能的计算机可执行指令。当其以软件的方式实现时，所述的可执行指令可以存储在存储器中，并被设备中的

15 的处理器执行。

[72]例如，对应于上述方法，本说明书一个或多个实施例同时提供一种欺诈团伙的识别设备，该设备可以包括处理器、存储器、以及存储在存储器上并可在处理器上运行的计算机指令，所述处理器通过执行所述指令，用于实现如下步骤：

[73]构建包括多个节点的关系网络；

20 [74]基于所述关系网络进行聚类发现，得到所述关系网络包括的至少一个欺诈团伙，每一个所述欺诈团伙包括多个所述节点；

[75]由所述欺诈团伙包括的节点中确定弱节点，所述弱节点是与所述欺诈团伙的关联符合弱关联条件的节点；

[76]将所述欺诈团伙中的所述弱节点去除，识别得到最终的目标欺诈团伙。

25 [77]还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[78]本领域技术人员应明白，本说明书一个或多个实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[79]本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书一个或多个实施例，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[80]本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于数据处理设备实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[81]上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[82]以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。