Complicity Functions for Detecting Organized Crime Rings

E. Vicente, A. Mateos[(✉)], and A. Jiménez-Martín

Decision Analysis and Statistics Group, Departamento de Inteligencia Artificial,
Universidad Politécnica de Madrid, Madrid, Spain
{e.vicentecestero,alfonso.mateos,antonio.jimenez}@upm.es

Abstract. Graph theory is an evident paradigm for analyzing social networks, which are the main tool for collective behavior research, addressing the interrelations between members of a more or less well-defined community. Particularly, social network analysis has important implications in the fight against organized crime, business associations with fraudulent purposes or terrorism.

Classic *centrality functions* for graphs are able to identify the key players of a network or their intermediaries. However, these functions provide little information in large and heterogeneous graphs. Often the most central elements of the network (usually too many) are not related to a collective of actors of interest, such as be a group of drug traffickers or fraudsters. Instead, its high centrality is due to the good relations of these central elements with other honorable actors.

In this paper we introduce *complicity functions*, which are capable of identifying the intermediaries in a group of actors, avoiding core elements that have nothing to do with this group. These functions can classify a group of criminals according to the strength of their relationships with other actors to facilitate the detection of organized crime rings.

The proposed approach is illustrated by a real example provided by the Spanish Tax Agency, including a network of 835 companies, of which eight were fraudulent.

1 Introduction

Graph theory is able to represent the relationships between all kinds of objects, such as human relationships, probabilistic relationships between events, electronic circuit components, computer networks, atomic networks... The analysis of these networks can be useful for valuable tasks such as detecting business associations with fraudulent purposes, counterterrorism investigation or political communication.

A *graph* [20] is a pair $G = (V, E)$, where V is the set of *vertices* or *nodes* and set E includes the *edges* or *arcs* of the graph. We denote a vertex or node by $v \in V$, and an arc by a pair of (not necessarily different) nodes (u, v). In that case, both nodes, u and v, are *neighboring nodes*. If the arc (u, v) is different to (v, u), then the graph is directed (a *digraph*).

We define the *arc-node incidence* of v in an undirected graph as the number of arcs incident to or from node v, i.e., the number of arcs starting or ending at v. If the graph is a digraph then we define the *indegree* of a node v as the number of arcs ending at (or incident to) v and the *outdegree* as the number of arcs starting at v. Therefore, the incidence degree is the sum of both.

The arcs of a graph can be assigned a weight, which denotes the intensity of the relation between the endpoint nodes of the arc. In this case, the graph is called a *weighted graph*.

The *adjacency matrix* of a given graph G with n nodes is an $n \times n$ matrix $A_G = (a_{u,v}^G)$, where $a_{u,v}^G = 1$ if $(u,v) \in E$ and $a_{u,v}^G = 0$ otherwise. In a weighted graph, this value will be the weight of the arc (u,v).

A *path* from u to v in a graph is a sequence of arcs, starting at node u and ending at node v. If such a path exists, u and v are *connected*. A *geodesic path* between two nodes of the graph is the shortest path between both nodes and the *geodesic distance* is the length of the geodesic path.

A graph is *connected* when there is a path between each pair of nodes and *complete* when all pairs of nodes are connected by an arc.

An important aspect in *social network analysis* is its *visualization*. A graph can be displayed in different ways. Classic visualization algorithms are studied in [4, 8–10, 19]. Secondly, the detection of communities, i.e., groups of nodes that are clearly differentiated in the graph [6, 11, 17], is interesting in social network analysis. Finally, another key feature of social network analysis is to identify different roles depending on the position of each actor in the network. For example, a social network may have key players, communication or action leaders that attract many other actors. The detection of these leaders can be critical in the development of information campaigns. We can also observe intermediate actors connecting different communities or other key players. All these actors can be identified by means of *centrality and intermediation indicators*.

The first studies on centrality in graphs date back to the 1950s and were conducted at [7] the Massachusetts Institute of Technology Group Networks Laboratory, in the field of sociology. Several works [1, 16, 21] report research into the the centrality characteristics of a group and the efficiency in the development of several more or less cooperative tasks. But the centrality concept in networks was later proven to be useful for explaining and analyzing geographical [18], political [2], economics or business [3] questions.

According to Freeman [7], it is difficult to define a centrality notion for graphs that accounts for different situations and interests. Instead the central elements are inspected to check that they have an intuitively evident set of properties. These properties are as follows:

1. The elements of a network with a higher adjacency degree, i.e., nodes that are more related with others nodes, are its central elements.
2. The elements of a network belonging to the highest possible number of geodesics between any two nodes of the network, are its central elements. These nodes are good intermediaries because they have to be traversed along the shortest path from one node to another.

3. The elements of a network closest to the other nodes, i.e., nodes that minimize the sum of geodesic distances to the other nodes, are its central elements.

Thus, the centrality function with the best trade-off between these three, not necessarily conflicting but not strictly correlated, properties will be the best, as we shall see later.

The first centrality functions in the literature were, predictably, functions that primarily satisfied the first of the three properties. However, the adjacency degree of the node it is not, by itself, a good centrality indicator. Consequently, centrality measures should be collective, where the centrality of a node depends not only on the local individual structure of the node, but also on the neighborhood structure, i.e., the centrality of a node is a function not only of the number of nodes connected to it, but also of the centrality of these nodes. This idea directly leads to two major centrality indicators: *eigenvector centrality* [14] and the *PageRank coefficient* [15], which is the basis of the Google engine search.

Besides, *hub/authority centrality* is based on the correlation between nodes with a high indegree (*authority nodes*) and nodes with a high outdegree (*hub nodes*). The HITS (*Hiperlink-Induced Topic Search*) [13] algorithm computes a membership value from each node to each one of these classes.

In this paper we propose a five-phases procedure for organized crime ring detection. The first phase computes the complicity of each actor with each fraudulent actor. Section 2 introduces the concept of complicity or suspicion of collaboration between one actor and another previously identified as fraudulent. Section 3 defines the strength of attraction between fraudulent actors, shown as the set of fraudulent nodes projected using multidimensional scaling in a plane (phase 3). These points are then grouped according to the DBSCAN algorithm (phase 4). Finally each identified actor is added to the group of fraudulent actors that maximizes its complicity (phase 5). Section 4 illustrates our approach with a real example including 835 Spanish companies, eight of which are fraudulent. Finally, some conclusions are provided in Sect. 5.

2 Dangerous Liaisons

The classic centrality measures are designed for graphs representing uniform collectives. However, the fight against organized crime requires an analysis that goes beyond the study of closed groups of individuals with common interests. In our society, honest and fraudster people are interrelated, and the fraudster take advantage of this circumstance and to commit crimes without being caught. Fraudulent companies take advantage of good faith of honorable companies to conceal fraudulent activities. Terrorists mix with citizens, and drug traffickers often have the appearance of respectable business entrepreneurs, who pay taxes and create jobs, etc. A good example are the so-called *carousel fraud plots*, in which a group of companies cooperates to commit value added tax fraud. This network of companies usually forges relationships with legitimate companies, which are unaware of the fraudulent activity of their partners, suppliers and clients.

The good news is that countries have increasingly improved technologies, capable of saving and monitoring networks of taxpayers, consumers, citizens, businessmen..., and these networks include both the honest and the fraudster subject. However, the above centrality functions do not work in these hetero-geneous networks. For example, given a wide collective of companies, some of which have committed carousel fraud, the question is which other companies have a good relation with the companies implicated in fraud? In other words, which companies are suspicious of aiding and abetting the carousel fraud? Cen-trality measures are unable to identify these suspected companies, since they make computations on the basis of the relations with all nodes, irrespective of whether or not they are fraudsters.

2.1 Complicity Functions

We propose the concept of *complicity* or *suspicion of collaboration* between one actor and another previously marked as toxic (fraudulent), rather than centrality functions. In the following, we assume that the graph G is undirected, and we consider a set of *toxic* nodes in G, $\mathcal{F} \subset V$. Our aim is to study the relation between the nodes in $V - \mathcal{F}$ and the toxic nodes and assign a complicity value to those nodes depending on their relations.

The complicity function must satisfy the following three properties:

1. Nodes directly or indirectly connected to toxic nodes should have higher com-plicity values than nodes not related to toxic nodes. In fact, nodes without a direct or indirect connection to toxic nodes should be assigned zero complicity.
2. Distance should be penalized, i.e., the complicity of nodes that are closer to toxic nodes is greater.
3. Node connection to toxic nodes should be considered, i.e., the complicity nodes that are connected to a high number of toxic nodes is higher.

The above properties can be stated using the following expression, which represents the complicity of v with respect to the set of toxic nodes $\mathcal{F}$:

$$C(v) = \frac{1}{|\mathcal{F}|} \sum_{u \in \mathcal{F}} L(g(v, u)),$$

where L is a decreasing function and $g(v, u)$ is the geodesic distance between u and v. L can be an exponential or hyperbolic tangent function, as follows:

$$C(v) = \frac{1}{|\mathcal{F}|} \sum_{u \in \mathcal{F}} e^{r(1-g(v,u))} \text{(exponential) or}$$

$$C(v) = \frac{1}{|\mathcal{F}|} \sum_{u \in \mathcal{F}} \frac{1}{2} \left[\frac{e^{r-rg(u,v)} - e^{rg(u,v)-r}}{e^{rg(u,v)-r} + e^{r-rg(u,v)}} + 1 \right] \text{(hyperbolic tangent)},$$

where $g(v, u)$ is the geodesic distance from v to u without passing through any toxic node and r is a constant that models the differences. These complicity functions satisfy the above properties and output values within [0,1].

The reason why we used geodesics that do not traverse the other toxic nodes to compute each summand of the above expression is that the connection with a toxic node could be overestimated if a toxic node is connected to other toxic nodes, which is commonplace. If an actor is connected to a toxic node which is in turn connected to other toxic nodes, then the actor is also connected to the latter, but this would not be an indicator of complicity. However, if the actor is connected repeatedly to the set of toxic nodes, then it is an accomplice.

These functions are suitable when the graph is connected. However, when the graph is formed by two or more disconnected subgraphs (two or more *connected components*), then the distance between two nodes belonging to different subgraphs is ∞, and the complicity of a node with respect to a fraudster in another connected component is zero. Besides, complicity is also zero for a node in the same component as, but at a large distance from, the fraudster. It is critical for the classification model to be able to deal with these two situations; otherwise disconnected plots would not be distinguishable from sets of nodes that are very far apart within the same component. One possibility would be to smooth the decrease by controlling parameter r, but this method does not yield good results in practice since complicity would have to be negligible as of some value of the geodesic distance. In this situation, a finite distance is the same as an infinite distance, which does not solve the problem. To overcome this drawback, we have to substitute a straight line ($y = k > 0$) (small) for the horizontal asymptote at infinity within the hyperbolic tangent model and *put a step in the infinity*, i.e., we control the parameters α and β rather than parameter r in the expression:

$$C(v) = \frac{1}{|\mathcal{F}|} \sum_{u \in \mathcal{F}} \alpha \left[\frac{e^{r - rg(u,v)} - e^{rg(u,v) - r}}{e^{rg(u,v) - r} + e^{r - rg(u,v)}} + \beta \right],$$

such that

$$\lim_{x \to \infty} \alpha \left[\frac{e^{r - rx} - e^{rx - r}}{e^{rx - r} + e^{r - x}} + \beta \right] = \alpha(\beta - 1) = k \text{ and}$$

$$\lim_{x \to -\infty} \alpha \left[\frac{e^{r - rx} - e^{rx - r}}{e^{rx - r} + e^{r - x}} + \beta \right] = \alpha(\beta + 1) = 1, \text{ i.e., } \beta = \frac{1 + k}{1 - k} \text{ and } \alpha = \frac{1 - k}{2}.$$

2.2 Markov Chain-Based Approach

Markov chains are widely used to compute some classic centrality measures. Markov chains can simulate dynamic systems with a set of possible states where it is possible to pass from one state to another with certain probability.

In the above *PageRank algorithm*, given an adjacency matrix $A = (a_{ij})$, where $a_{ij} = 1$ if there is an arc between u_i and u_j and $a_{ij} = 0$ otherwise. If each row is divided by the sum of its elements, then we have a stochastic matrix $T = (t_{ij})$ (where each row is a probability distribution). This matrix is called a *transition matrix* since each element t_{ij} represents the probability of passing from node u_i to node u_j. In fact, matrix $T^n = \left(t_{ij}^{(n)} \right)$ represents the probability

of reaching node u_j in a path of length n starting at u_i. This probability will be higher if the number of paths connecting both nodes increase.

The complicity of a toxic node v_j with another node u_i can be computed as:

$$c(v_j, u_i) = \sum_{n=1}^{\infty} \alpha^n t_{ij}^{j(n)},$$

where $\alpha \in (0, 1)$ penalizes the distance between the nodes and $t_{ij}^{j(n)}$ are elements of $(T^j)^n$, where T^j is the transition matrix accounting for all nodes except toxic nodes different to v_j.

This function is similar to Katz centrality [12], except that we use the transition rather than the adjacency matrix and it is constrained to the toxic node v_j with respect to the node u_i. In other words, we are interested in the communication channels between toxic nodes and other nodes rather than the relations between all nodes in the graph, whereas Katz centrality sums all these values and outputs a single value for each node using the adjacency matrix.

In practice, it is sufficient to define a limit value, such as the graph *diameter* (length of the longest geodesic in the graph), δ, and compute the powers $T^j, (T^j)2, ..., (T^j)^\delta$ for each $v_j \in \mathcal{F}$. If we take the row in matrix $C^j = \alpha T^j + \alpha^2 (T^j)^2 + ... + \alpha^\delta (T^j)^\delta$ corresponding to the toxic node v_j and remove the element corresponding to that toxic node v_j, then we have a transposed vector denoted by c^j.

Now, let C be the rectangular matrix whose rows are the above transposed vectors c^j for the different toxic nodes, i.e. $\forall v_j \in \mathcal{F}$. Then, the total complicity of each non-toxic node can be computed as the sum of the elements in the column in C associated to that non-toxic node, and the complicity mean by dividing the above amount by the number of toxic nodes:

$$c(u_i) = \frac{1}{|\mathcal{F}|} \sum_{v_j \in \mathcal{F}} c(v_j, u_i) = \frac{1}{|\mathcal{F}|} \sum_{v_j \in \mathcal{F}} \sum_{n=1}^{\delta} \alpha^n t_{ij}^{(n)}.$$

2.3 Detection of Suspects of Complicity

The complicity function is useful for fighting against organized crime, identifying all actors represented by nodes that are highly related to a list of toxic nodes. To do this, we propose Algorithm 1, which accounts for a minimum number $s \in \mathbb{N}$ (for example, $s = 1$) of toxic nodes to which the actor should be related in order to be suspected of complicity. The higher the number is, the more suspect the actor will be. Besides, we consider a percentile $p \in (0, 100)$ as of which complicity is significantly high. To do this, we look at the distribution of the complicity values in the graph, considering the relation between the number of toxic and non-toxic nodes.

Algorithm 1. Detection of partners in crime

Input: (G undirected graph, $\mathcal{F}$ list of toxic nodes, $s \in \mathbb{N}$ minimum number of connected toxic nodes with the suspect node, $p \in (0, 100)$ value for the complicity percentile).

1. For each $w \in V$, compute the number $s(w)$ of elements of $\mathcal{F}$ connected to w without passing through other toxic actors.
2. For each element $v \in \mathcal{F}$:
3.   Remove all nodes $u \in \mathcal{F}$ such that $u \neq v$ from V.
4. $\forall w \in V$ such that $s(w) > s$ calculate $c(w, v) = e^{r(1 - g(v,u))}$.
5. For each $w \in V$:
6.   Compute $C(w) = \frac{1}{|\mathcal{F}|} \sum_{v \in \mathcal{F}} c(w, v)$.
7. Compute the percentile of order p from the vector C.
8. Save and rank all nodes with a complicity value above percentile p.

---

3   Detection of Organized Crime Rings

Each toxic node $v_i \in \mathcal{F}$ is associated with a vector $\overrightarrow{v_i} = (v_{i1}, ..., v_{ir})$ where $v_{ij} = c(v_i, u_j)$ is the complicity of the toxic node v_i with the actor u_j.

We define the *strength of attraction* between the toxic nodes v_i and v_k by $f_{ik} = \overrightarrow{v_i} \cdot \overrightarrow{v_k} = \sum_{j=1}^{r} v_{ij}v_{kj}$, which can be normalized as follows: $f_{ik} = \frac{\overrightarrow{v_i} \cdot \overrightarrow{v_k}}{|\overrightarrow{v_i}||\overrightarrow{v_k}|}$, representing the cosine of the angle defined by vectors $\overrightarrow{v_i}$ and $\overrightarrow{v_k}$.

Matrix f is a symmetrical, nonnegatively defined matrix such that the maximum value in the i-th row, $f_{ii} = 1$, is located on the diagonal, i.e., it is a normalized similarity function, in which completely different nodes are in different components, i.e., $f_{ij} = 0$ if and only if $g(u_i, u_j) = \infty$.

It is possible to derive a distance metric in [0,1] from the similarity function S as follows: $d(u, v) = \sqrt{S(u, u) - 2S(u, v) + S(v, v)}$. In our case, $d(u, v) = \sqrt{2 - 2f(u, v)}$. We can use this distance to project all the nodes using multidimensional scaling to represent fraudsters in $[0,1]^2$ with a maximum distance $\sqrt{2}$, which matches the maximum reachable distance by d when $f(u, v) = 0$. If a larger area is required, then a nonnormalized distance could be used, $d' = a \cdot d$.

Multidimensional scaling (MDS) [22] is a visualization algorithm of high-dimensional data arranged in a plane or 3D space. Data are represented by means of points whose distance is proportional to the differences between the data that they represent. The classic example illustrating this procedure is to plot a geographic map in a plane where the only available information is the distance between a set of cities.

Torgerson [22] proves that a matrix with the features of f (symmetrical and nonnegatively defined) can be decomposed as $f = U \Lambda U^t$, where U is the normalized eigenvector matrix and Λ is the eigenvalue diagonal matrix. If we denote $Y = U \Lambda^{1/2}$, then $YY^t = U \Lambda^{1/2} \Lambda^{1/2} U^t = RR^t$.

If two matrices from two different bases have the same matrix of scalar products, then one is the transform of the other by a change of basis. Then, Y is the matrix R in the basis of proper vectors, i.e., each row of Y is the strength vector from a fraudster in the basis of proper vectors.

Now, since $Y = U\Lambda^{1/2}$, if the first p eigenvalues are somewhat larger than the others, we can consider an approximation $\hat{X}$ of the initial fraudster matrix, which can be represented in p dimensions. If $p = 2$, fraudsters can be represented by points in a plane where their distances are proportional to the complicity differences of their related nodes.

Therefore, the percentage of the sum of the first two eigenvalues over the sum of all eigenvalues is a measure of how good the visualization is, i.e., the visualization is more realistic and better represents the differences, the greater the difference is between the sum of the first two eigenvalues and the sum of all eigenvalues.

We proceed to group the nodes according to the distances from the MDS projection on the plane of the set of toxic nodes. A simple and useful algorithm for this purpose is the *density-based spatial clustering of applications with noise* (DBSCAN) [5], which assesses the density of each region of the plane by computing the numbers of points that are within spheres with radius *eps* of each element in the population. Accordingly, the density of a neighborhood is satisfactory if the number of points in this neighborhood is equal to or greater than a prefixed value *MinPt*. The initial parameters of the DBSCAN then are the radius *eps* and the minimum density value *MinPt*. Note that the choice of these values is a critical decision because if *eps* is very small, then the spheres only have one point, whereas if they are too big, all points could belong to the sphere.

In summary, the procedure for ring detection is:

1. Compute the complicity of each node with each toxic node.
2. Compute the strength of attraction f between toxic nodes.
3. Project the set of toxic nodes using multidimensional scaling in a plane in such a way that the distance between nodes are proportional to $\sqrt{2 - 2f}$.
4. Group the points of the projection according to the DBSCAN algorithm.
5. Add each non-toxic node to the group of toxic nodes that maximizes its complicity.

After performing this assignment we can tune the algorithm considering connecting paths connecting partners in crime and toxic nodes.

4 An Illustrative Example

This section illustrates the ring detection procedure with a real example including 835 linked companies, of which eight are fraudulent. Data was provided by the Spanish Tax Agency. These are missing trade companies that are suspicious of belonging to carousel fraud plots (EU VAT plots) for the year 2013. These companies should have paid the full amount of VAT charged on an intra-Community acquisition of goods (a commodity purchase by a EU member country destined for a domestic market) to the national tax authorities. However, the company disappeared after selling the commodity without making this payment.

Figure 1 shows a graph describing the relationships between the 835 companies, highlighting the fraudulent companies in green. These relationships refer to any corporate, family, representation, management, authorization and co-ownership bank accounts for the year 2013.
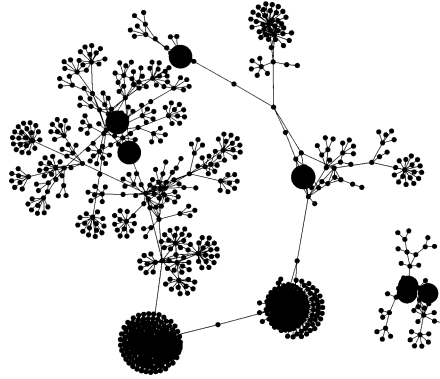
**Fig. 1.** 835 linked companies (Color figure online)

Our goal is to compute the complicity of companies with the fraudsters, group fraudsters depending on their relationship and complicity with each other and, finally, assign each company to a group of fraudsters accounting for average complicity with fraudsters from each ring following the procedure described in Sect. 3.

Figure 2(a) shows the projection by multidimensional scaling of the fraudster group, whereas Fig. 2(b) shows the resulting cluster after applying the DBSCAN algorithm. Four clusters are identified using different colors. Specifically, companies 582 and 579 (in green) constitute a cluster, whereas companies 17, 34 and 58 (in red) form another cluster. Companies 121 and 460 are in the third cluster. Finally company 240 is itself the fourth cluster.

Next, we build a ring for each cluster including the 827 remaining companies. To do this, we compute the average complicity of each company regarding the fraudster companies in each cluster. Thus, the company will be a member of the ring with which it has the highest average complicity. Each company is located in the selected cluster (ring) at a distance from the centroid of the cluster equal to its average complicity. Figure 2(c) shows the rings for the four clusters. The colors in the respective rings are associated with the percentiles of complicity values. Specifically, companies whose average complicity regarding the fraudsters in the corresponding cluster is under percentile 75 are shaded green, companies above percentile 95 are colored red and yellow is used for companies between the above percentiles.

Finally, Fig. 3 illustrates the original graph including the 835 linked companies in this case highlighting the companies with different colors (red, pink, blue and so on) in the different rings with an average complicity above percentile 95. These are the companies that could be considered as being suspicious of taking part in an organized crime ring.

The Spanish Tax Agency is currently using the proposed approach to rank, on the basis of the above average complicities, companies suspicious of fraud for inspection, since the number of inspectors and their availability are limited. This has led to an increment in the success rate.
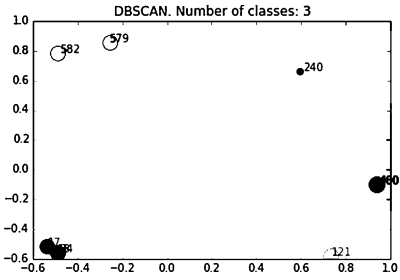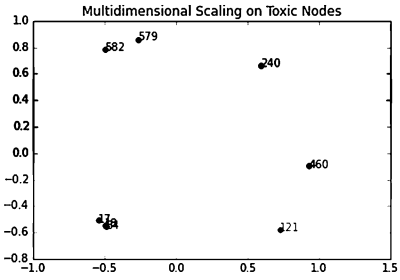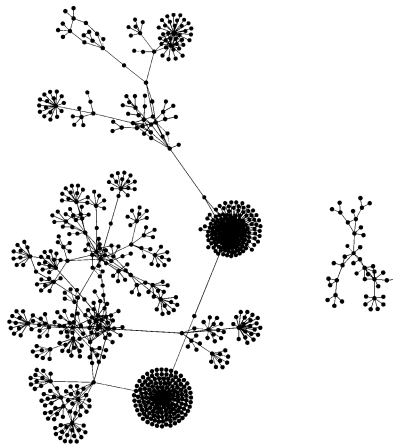
(a) Multidimensional scaling of fraudulent nodes

(b) DBSCAN clustering
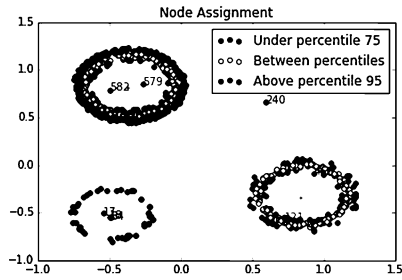
(c) Rings

Fig. 2. Detection of organized crime rings (Color figure online)

Fig. 3. Resulting organized crime rings (Color figure online)

5   Conclusions

Social network analysis has important implications in the fight against organized crime, business associations with fraudulent purposes or terrorism. We have introduced several functions to measure the degree of complicity between the actors in an heterogenous social network with a set of previously identified *toxic* actors, with the aim of detecting the partners of an organized crime plot. This complicity function naturally induces a similarity function between toxic nodes, the *strength of attraction*, which can be transformed into a distance metric.

Then, toxic nodes can be projected as points in a plane where the distances between points are proportional to the original distances between the toxic nodes (multidimensional scaling algorithm). The DBSCAN algorithm then groups the toxic nodes according to different high-density regions, and nodes with higher complicity are assigned to the different rings accounting for the maximization of average complicity.

The methodology has been illustrated by a real example, including 835 companies, of which eight are fraudulent according to the Spanish Tax Agency. The proposed approach detects organized crime rings and computes, for each ring, the complicity level of its actors. The Spanish Tax Agency is currently using the proposed approach to rank suspicious companies for inspection, since the number of inspectors and their availability are limited. This has led to an increment in the success rate.

We propose as a future research line to conduct a comparative analysis between the proposed method and other group detection methods, and between the complicity function and other centrality functions. Besides, further available information about the considered companies could be incorporated into the analysis and artificial intelligence tools, such as machine learning and statistics, could be used to derive a more robust crime ring detection method.

References

1. Bavelas, A., Barret, D.: An experimental approach to organizational communication. Personnel **27**, 366–371 (1951)
2. Cohn, B.S., Marriott, M.: Networks and centers in the integration in Indian civilization. J. Soc. Res. **I**(1), 1–9 (1958)
3. Czepiel, J.A.: Word of mouth processes in the diffusion of a major technological innovation. J. Mark. Res. **I**, 1–9 (1974)
4. Eades, P.: A heuristic for graph drawing. Congressus Numeranti **42**(11), 149–160 (1984)
5. Ester, M., Kriegel, H.-P., Sander, J., Xu, X.: A density-based algorithm for discovering clusters in large spatial databases with noise. In: KDD 1996 Proceedings (1996)
6. Faust, K., Wasserman, S.: Blockmodels: interpretation and evaluation. Soc. Netw. **14**(1–9), 5–61 (1992)

7. Freeman, L.C.: Centrality in social networks conceptual clarification. Soc. Netw. **1**, 215–239 (1978)
8. Fruchterman, T.M.J., Reingold, E.M.: Graph drawing by force-directed placement. Softw. Pract. Experience **21**(11), 1129–1164 (1991)
9. Hu, Y.: Efficient and high quality force-directed graph. Math. J. **10**(1), 37–71 (2005)
10. Kamada, T., Kawai, S.: An algorithm for drawing general undirected graphs. Inf. Process. Lett. **31**(1), 7–15 (1989)
11. Karrer, B., Newman, M.E.J.: Stochastic block models and community structure in networks. Phys. Rev. E **83**(1), 016107 (2011)
12. Katz, L.: A new status index derived from sociometric analysis. Psychometrika **18**(1), 39–43 (1953)
13. Kleinberg, J.: Authoritative sources in a hyperlinked environment. J. ACM **46**(5), 604–632 (1999)
14. Langville, A.N., Meyer, C.D.: A survey of eigenvector methods for web information retrieval. SIAM Rev. **47**(1), 135–161 (2005)
15. Lawrence, P., Sergey, B., Rajeev, M., Terry, W.: The pagerank citation ranking: bringing order to the web. Technical report, Stanford University (1998)
16. Leavit, H.J.: Some effects of certain communication pattern on group performance. Massachusetts Institute of Technology (1949)
17. Peixoto, T.P.: Hierarchical block structures and high-resolution model selection in large networks. Phys. Rev. X **4**(1), 011047 (2014)
18. Pitts, F.R.: A graph theoretic approach to historical geography. Prof. Geogr. **17**, 15–20 (1965)
19. Quigley, A., Eades, P.: FADE: graph drawing, clustering, and visual abstraction. In: Marks, J. (ed.) GD 2000. LNCS, vol. 1984, pp. 197–210. Springer, Heidelberg (2001)
20. Schaeffer, S.E.: Graph clustering. Comput. Sci. Rev. **I**, 27–64 (2007)
21. Smith, S.L.: Communication Pattern and the Adaptability of Task-Oriented Groups: An Experimental Study. Group Networks Laboratory, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge (1950)
22. Torgerson, W.S.: Multidimensional scaling: I. Theory and method. Psychometrika **17**(4), 401–419 (1952)