Graph Comparison and Artificial Models for Simulating Real Criminal Networks

Lucia Cavallaro[1(✉)], Annamaria Ficara[2], Francesco Curreri[2], Giacomo Fiumara[3], Pasquale De Meo[4], Ovidiu Bagdasar[1], and Antonio Liotta[5]

[1] School of Computing and Engineering, University of Derby, Kedleston Road, Derby DE22 1GB, UK
{l.cavallaro,o.bagdasar}@derby.ac.uk
[2] DMI Department, University of Palermo, via Archirafi 34, 90123 Palermo, Italy
{aficara,fcurreri}@unime.it
[3] MIFT Department, University of Messina, Viale Ferdinando Stagno d'Alcontres 31, 98166 Messina, Italy
gfiumara@unime.it
[4] DICAM Department, University of Messina, Viale Giovanni Palatuci 13, 98168 Messina, Italy
pdemeo@unime.it
[5] Faculty of Computer Science, Free University of Bozen-Bolzano, Piazza Domenicani 3, 39100 Bolzano, Italy
antonio.liotta@unibz.it

Abstract. Network Science is an active research field, with numerous applications in areas like computer science, economics, or sociology. Criminal networks, in particular, possess specific topologies which allow them to exhibit strong resilience to disruption. Starting from a dataset related to meetings between members of a Mafia organization which operated in Sicily during 2000s, we here aim to create artificial models with similar properties. To this end, we use specific tools of Social Network Analysis, including network models (Barabási-Albert identified to be the most promising) and metrics which allow us to quantify the similarity between two networks. To the best of our knowledge, the DeltaCon and spectral distances have never been applied in this context. The construction of artificial, but realistic models can be a very useful tool for Law Enforcement Agencies, who could reconstruct and simulate the evolution and structure of criminal networks based on the information available.

Keywords: Criminal networks · Complex networks · Social network analysis · Graph theory · Graph comparison · Graph similarity · Graph matching

1 Introduction

Criminal organizations [16] often profit from providing illicit goods and services in public demand, or by offering legal goods and services in an illicit manner. One of the most renowned criminal organisations (i.e., clans, gangs, syndicates) is the

R. M. Benito et al. (Eds.): COMPLEX NETWORKS 2020, SCI 944, pp. 286–297, 2021.
https://doi.org/10.1007/978-3-030-65351-4_23

Sicilian Mafia. This organisation was analysed in Gambetta's classic work on its economics and dynamics [17], where it is referred to as the original "Mafia". In a more recent work [23], Letizia Paoli provided a clinically accurate portrait of mafia behavior, motivations, and structure in Italy, relying on previously undisclosed confessions of former mafia members now cooperating with the police.

The analysis of the Sicilian Mafia syndicates social structure generated great scientific interest [20]. Currently, scholars and practitioners alike are increasingly adopting a network science perspective to explore criminal phenomena [6].

Social Network Analysis (SNA) has emerged as an important component in the study of criminal networks and in criminal intelligence analysis. This tool is used to describe the structure and functioning of a criminal organisation, to construct crime prevention systems [5] or to identify leaders within a criminal organisation [19]. Indeed, some studies had the unique opportunity to examine real datasets and to use the data sources to build networks and to examine them by means of classical SNA tools [5,8,11,15,25,26,30].

Law Enforcement Agencies (LEAs) increasingly employ SNA in the study of criminal networks, as well as to analyse the relations amongst criminals based on calls, meetings and other events derived from investigations [1,14,15]. When dealing with practical networks, missing data may refer to *nodes* and/or *edges*. Often, criminal networks are incomplete, incorrect, and inconsistent, either due to deliberate deception on the part of criminals, or to limited resources or unintentional errors by LEAs [1,4,5,9,14]. SNA is also used to evaluate LEA interventions aimed at dismantling and disrupting criminal networks [8,11].

Another interesting application of SNA and graph theory is to develop random graph models which mimic the structure and behaviour of real criminal networks. Indeed, even if the growing mechanism of this criminal network remains largely unknown, growth and preferential attachment mechanisms are most probably at the core of the affiliation process. In this respect, comparing an artificial model network to a real network is not only plausible, but even fruitful in terms of useful insights about the structure and behaviour of the real network. The growth of available data and number of network models [22,24,28], has led researchers to face the problem of comparing networks, i.e., finding and quantifying similarities and differences between them.

Network comparison requires measures for the distance between graphs [29]. This is a non-trivial task, which involves a set of features that are often sensitive to the specific application domain such as: the results' effectiveness, the interpretability, and the computational efficiency. There is some debate about the weakness of this technique, principally due to cospectrality issues, but there is evidence that the fraction of cospectral graphs is 21% for networks composed of 10 nodes and is less for 11 nodes [34]. We may, therefore, expect that cospectrality becomes negligible for larger graphs. Granted the reliability of these techniques, we selected the simplest and yet effective among the various metrics.

The literature on this topic is abundant, but the classification of best methods for specific situations (including the comparison of real-world networks) remains an open field. A few critical reviews of the literature on this subject have already

been compiled [10,12,27]. Wills and Meyer [33] compared commonly used graph metrics and distance measures, and demonstrate their ability to discern between common topological features found in both random graph models and real world networks. They put forward a multi-scale picture of graph structure wherein they studied the effect of global and local structures on changes in distance measures. The number of useful graph comparison techniques [2] drastically reduces when one requires an algorithm which runs in reasonable time on large graphs.

In recent years, many random graph models emulating features of real-world graphs [3,31] have been developed. An accurate probabilistic study of the application of graph distances to these random models is difficult, as they are often defined in terms of their generative process. For this reason, most researchers restrict their attention to very simple random models such as that of Erdös and Rényi [13]. Even so, rigorous probabilistic analysis can be difficult. A possible solution is the one proposed by Wills and Meyer [33], that is a numerical approach where a sample is taken from random graph distributions and the empirical performance of various distance measures is observed.

Despite the growing scholarly attention to network comparison, to the best of our knowledge, there is no previous research aiming to identify best measures for the distance between graphs related to real criminal networks. Filling this gap is a first step towards comparing and generating artificial networks which mirror the topology and functionality of real criminal networks. Far more important, LEAs could considerably benefit from such a discovery. A surrogate network on which to conduct their investigations could predict the evolution of new connections between criminals or, on the other side, break those links by arresting one (or more) of the suspects, based on the network topology.

To this end, we borrow some of the distance techniques proposed by [33]. We first generate data using popular artificial network models like Erdös and Rényi (ER), Watts-Strogatz [31] (WS), and different configurations of Barabási-Albert (BA) [3]. This is compared against real criminal network dataset named *Meetings* network from our earlier works [5,8,15], whose datasets are publicly available on Zenodo [7]. This captures the physical meetings among suspects in an anti-mafia investigation called "Montagna Operation", concluded in 2007 by the Public Prosecutor's Office of Messina (Sicily).

2 Materials and Methods

This section shows the standard definitions used in this work, as well as a brief description of the real dataset used to compare the artificial networks, along with the method followed to pursue the experiments.

2.1 Background

In this paper we deal with *unweighted undirected graphs*.

An *unweighted graph* $G = \langle N, E \rangle$ consists of a finite set N of n nodes (also called vertices/actors) and a set $E \subseteq N \times N$ of m edges (or links/ ties). A graph

is *undirected* when all the edges between nodes are bidirectional, as opposed to a *directed graph*, where the edges actually point to a direction.

The *adjacency matrix* of graph G defined over the set of nodes $N = \{1, \ldots, n\}$, is a $n \times n$ square matrix denoted by $A = (a_{ij})$, $1 \leq i, j \leq n$, where $a_{ij} = 1$ if there exists an edge joining vertices i and j, and $a_{ij} = 0$ otherwise. In the case of an *undirected graph*, its *adjacency matrix* is symmetric, i.e., $a_{ij} = a_{ji}$. Such a matrix, along with the *Laplacian* and *Normalized Laplacian* matrices, are the most common representation matrices for a graph.

The *spectrum* of a graph consists of the set of sorted (increasing or decreasing) eigenvalues of one of its representation matrices. It is used to characterise graph properties and extract information from its structure. The spectra derived from each representation matrix may reveal different properties of the graph. The largest eigenvalue (in absolute value) of the graph is called the graph's *spectral radius*. In the case of the adjacency matrix A, if λ_k is its k^{th} eigenvalue, the spectrum is given by their descending order as $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$.

The *spectral distance* [34] between two graphs G and G' of size n, is the Euclidean distance between their spectra, i.e., the set of eigenvalues λ_i and λ_i' (according to the chosen representation matrix). In case of the adjacency matrix, the *Adjacency Spectral Distance* is

$$\mathrm{d}(\mathrm{G}, \mathrm{G}') = \sqrt{\sum_{i=1}^{n} (\lambda_i - \lambda_i')^2}; \tag{1}$$

If the two spectra have different sizes, the smaller graph (of size $k \leq n$) is brought to the same cardinality of the other by adding zero values to its spectrum. In such case, only the first k eigenvalues are compared, which for the Adjacency Spectral Distance d are the largest k eigenvalues. Comparing the higher eigenvalues allows to focus more on global features. Another class of graph distances is the *matrix distance* [33]. A matrix of pairwise distances $\delta(v, w)$ between graph nodes is constructed for each graph, where δ is the shortest path connecting the nodes v and w. Such matrices provide a signature of each graph characteristics and carry important structural information. Given two graphs defined on the same set of nodes, their respective matrices of pairwise distances are built and then the distance between the two matrices is computed with any of the many available norms. In this work we adopt the DeltaCon distance.

This matrix distance method is based on the *Matsusita difference* (also called *root euclidean distance*) $d_{rootED}(G, G')$ between matrices S and S', created from the fast belief propagation method of measuring node affinities [21]. The fast belief propagation matrix is defined as $\mathbf{S} = [\mathbf{I} + \epsilon^2 \mathbf{D} - \epsilon \mathbf{A}]^{-1}$, where $\mathbf{I}$ is the identity matrix. $\mathbf{D}$ is the degree matrix, namely a diagonal matrix whose elements are defined as $d_{ii} = k_i$, k_i being the degree of the ith node, $\mathbf{A}$ is the adjacency matrix and $\epsilon = 1/(1 + \max_i d_{ii})$ [21]. The DeltaCon similarity, with values in the interval $[0, 1]$ is introduced as

$$sim_{DC}(G, G') = \frac{1}{1 + d_{rootED}(G, G')}, \tag{2}$$

where $d_{rootED}(G, G')$ is given by

$$\mathrm{d_{rootED}(G, G')} = \sqrt{\sum_{i,j} \left(\sqrt{S_{i,j}} - \sqrt{S'_{i,j}} \right)^2}. \tag{3}$$

The Matsusita difference is used instead of classical euclidean distance since, as opposed to the latter, it detects even small changes in the graphs.

Random network theory emulates the irregularity and unpredictability of real networks by constructing from scratch and characterizing graphs that are truly random. Some of the most popular random network models are *Erdös-Rényi* (ER), *Watts-Strogatz* (WS) and *Barabási–Albert* (BA).

According to the ER model [13], a network is firstly generated by laying down a number n of isolated nodes. Then each pair is selected and a random number in the interval $[0, 1]$ is generated. If the generated number exceeds a chosen probability p, then the selected nodes are connected. Otherwise they are left disconnected. The procedure is performed for all the $n(n-1)/2$ pairs of nodes. This is the simplest model, also known as the $G(n, p)$ model [18]. A closely related variant is the $G(n, M)$ model, where n labeled nodes are connected with M randomly placed links that is the model we used to conduct our experiments. Even though it is unlikely that real social networks form like this, such models can predict a number of different properties [13].

While the ER model may exhibit a small clustering coefficient along with a small average shortest path length, the WS model [31] can produce graphs with *small-world* properties, which are highly clustered but with small characteristic path lengths. Most nodes are not neighbors, but the neighbors of a node are likely to be connected and most nodes can be reached from every other one by a small number of steps (also called *Six Deegree of Separation* property) [31].

In a small-world network, if L is the distance in steps between two randomly chosen nodes, it grows proportionally to the logarithm of the number of nodes n: $L \propto \log(n)$.

Thus, the model is constructed as follows. Starting from a ring of nodes, each node is connected to their previous and next neighbours. Each link is then rewired with probability p to a randomly chosen node. For small values of p, the network maintains high clustering but the random long-range links can drastically decrease the distances between the nodes. When $p = 1$, all links are rewired, so the network turns into a random ER network [31].

The BA model [3] exploits a preferential attachment mechanism to develop a *scale-free network*, i.e., the degree distribution follows a power law. The algorithm starts from a network with m_0 nodes, whose links are chosen arbitrarily, as long as each node has at least one link. At each step, a new node with $m \leq m_0$ links is added. The preferential attachment ensures that the probability p_i that the new node is connected to a node i depends on the degree d_i of the latter as follows:

$$p_i = \frac{d_i}{\sum_j d_j}. \tag{4}$$

So the new node prefers to attach itself to already heavily linked nodes, called *hubs*, that tend to accumulate even more links at each step, while nodes with only few links are unlikely to be chosen [3].

2.2 Dataset

Our dataset is available on Zenodo [7] and was discussed in detail in our earlier studies [5,8,15]. Derived from the pre-trial detention order issued by the Court of Messina's preliminary investigation judge on March 14, 2007, was towards the end of the major anti-mafia effort referred to as "Montagna Operation", concluded in 2007 by the Public Prosecutor's Office of Messina (Sicily) and conducted by the Special Operations Unit of the Italian Police (the R.O.S. Reparto Operativo Speciale of the Carabinieri is specialising in anti-Mafia investigations). This prominent operation focused on two Mafia clans, known as the "Mistretta" family and the "Batanesi clan". From 2003 to 2007, these families were found to have infiltrated several economic activities including major infrastructure works, through a cartel of entrepreneurs close to the Sicilian Mafia. We created two networks, capturing phone calls and physical meetings, respectively. Herein, we focus on the Meetings network which accounts for the physical meetings among suspected (police stakeout), which is composed of 101 nodes and 256 edges.

2.3 Methodology

The main question we want to address in this paper is to measure how well an artificial network may catch some real network features. In this respect we first computed the sim_{DC} similarity and the $\mathrm{d}_{\mathrm{rootED}}$ distance (see Eqs. 2 and 3).

Thus, we have compared three network models (ER, WS and BA) with several BA configurations (BA2, BA3, and EBA), reaching a total of five networks, with the Meetings dataset. We have chosen BA because in [15] we have discovered that the criminal network under scrutiny follows a scale-free power law [15]. Furthermore, while not being the main focus of this study, there are reasons to believe that criminals follow specific criteria for recruiting new affiliates (growing and preferential attachment dynamics) [32]; however, this behaviour cannot be identified by a single network snapshot, as the real network herein investigated is. Moreover, in order to have a yardstick, we have also selected the ER and WS models. In particular, WS is not a totally unrealistic model because it is characterised by a short diameter and distance between nodes. The models have been created by using NetworkX libraries and the source code has been developed in Python. Table 1 summarises the input parameters required and the values we assigned to them. The number of nodes n is defined a priori in all the models considered, whereas the number of edges m is set only in ER model.

In WS, $\langle k \rangle$ represents the average degree. This has been set equal to 6, in order to obtain a final configuration as close as possible to the real criminal network in terms of number of total links. The same has been done for the input parameters of all the BA models chosen herein.

Indeed, three different flavours have been selected: BA2 and BA3, in which the number of edges added at each iteration m_i is equal to two and three, respectively, and the extended BA version (EBA) in which two more parameters are required: (i) p, the probability that m already existing pairs of nodes may be connected by a link, and (ii) q, the probability that an already existing link may be rewired. Thus, instead of creating a new link, an old one is reconnected between another pair of nodes; however, we set $q = 0$ to avoid injecting more randomness into the network building process.

Table 1. Artificial models configurations.

ER	*WS*	*BA2*	*BA3*	*EBA*
$\begin{cases} n = 101 \\ m = 256 \end{cases}$	$\begin{cases} n = 101 \\ \langle k \rangle = 6 \\ p = 0.6 \end{cases}$	$\begin{cases} n = 101 \\ m_i = 2 \end{cases}$	$\begin{cases} n = 101 \\ m_i = 3 \end{cases}$	$\begin{cases} n = 101 \\ m = 2 \\ p = 0.225 \\ q = 0 \end{cases}$

Afterwards, we first computed the DeltaCon distance as it can be used to compare two graphs with different numbers of nodes and/or edges. Unfortunately, the results this metric provide did not allow to determine which network model is closer to the real network. For this reason, we have also computed the spectral distance by using the adjacency matrix A, which undoubtedly identified the BA models to be the best ones to catch some real network features among the ones herein analysed.

The last refinement concerned the number of edges: as BA2 and BA3 produced networks with a number of edges different from the real network, we decided to further investigate whether the spectral distance could be reduced increasing (resp., decreasing) the number of edges of BA2 (resp., BA3).

The experiments consisted of adding an edge to the BA2 (resp., removing an edge from the BA3) network and computing the spectral distance. This procedure would eventually end when the number of edges reaches the number of edges in the real network. We devised two strategies to add (resp., remove) edges: (i) the preferential attachment selection, according to which the edge is created (removed) between the most attractive nodes and (ii) the random selection, in which the pair of nodes is selected in a purely random way.

In order to have statistically sound results, 1000 artificial networks of each type (ER, WA, EBA, BA2, BA3) have been produced, from which the average values have been computed.

3 Results

This section shows the main findings obtained from our comparative investigation between artificial and real networks. As stated in Sect. 2.3, our study starts

from the computation of S, the fast belief propagation matrix that is required to compute the Matsusita difference whose outcomes are commented in Sect. 3.1. Next, the spectral distance previously described is discussed in Sect. 3.2.

3.1 Matrix Distance

The discovery of an artificial network that almost mirrors the topology of the Meetings network begins by using the DeltaCon distance. As shown in Table 2, the largest differences emerge for the ER and WS models, whereas all the BA tests have slight differences between each other. However, there is no distance that sticks out among them. Thus, this metric is insufficient on its own to point out a model with significantly better performances in terms of emulating a criminal network topology. Even the values of sim_{DC} do not allow to conclude which artificial model network is more similar to the real network. As expected, the values of sim_{DC} lie in the interval $[0, 1]$, and there is little to no difference among the various artificial model networks. It could be interesting to investigate the similarity among them, but this lies outside the scopes of this work. For these reasons we have opted to also use the spectral distance.

Table 2. DeltaCon distance and similarity between the Meetings dataset and the artificial models.

Model	m	*Dist. S*	sim_{DC}
ER	256	2.2 ± 0.2	0.317
WS	202	2.5 ± 0.2	0.287
EBA	246	1.31 ± 0.08	0.433
BA2	198	1.28 ± 0.08	0.438
BA3	294	1.27 ± 0.07	0.441

3.2 Spectral Distance

The spectral distances are computed for the Adjacency matrix A. Table 3 confirms the ER and WS to perform worst, however we still cannot identify the best BA configuration because of the significant error range led to an overlapping outcome cross all BA tests. Thus, we have adjusted these configurations by adding (resp., deleting) links from the BA2 (resp., BA3) model following two options: first, choose the pair of nodes through preferential attachment (resp., detachment); second, pick those pairs among which adding (resp., deleting) links randomly. The resulting graph in Fig. 1 suggests that by adjusting the number of edges, the distance is reduced without a preferable BA configuration.

Table 3. Degree distribution variation between the Meetings dataset and the artificial models computed by the spectral distance.

Model	*m*	*Dist. A*
ER	256	8.4 ± 0.2
WS	303	9.2 ± 0.2
EBA	255	6.6 ± 0.2
BA2	198	6.9 ± 0.2
BA3	294	7.1 ± 0.2

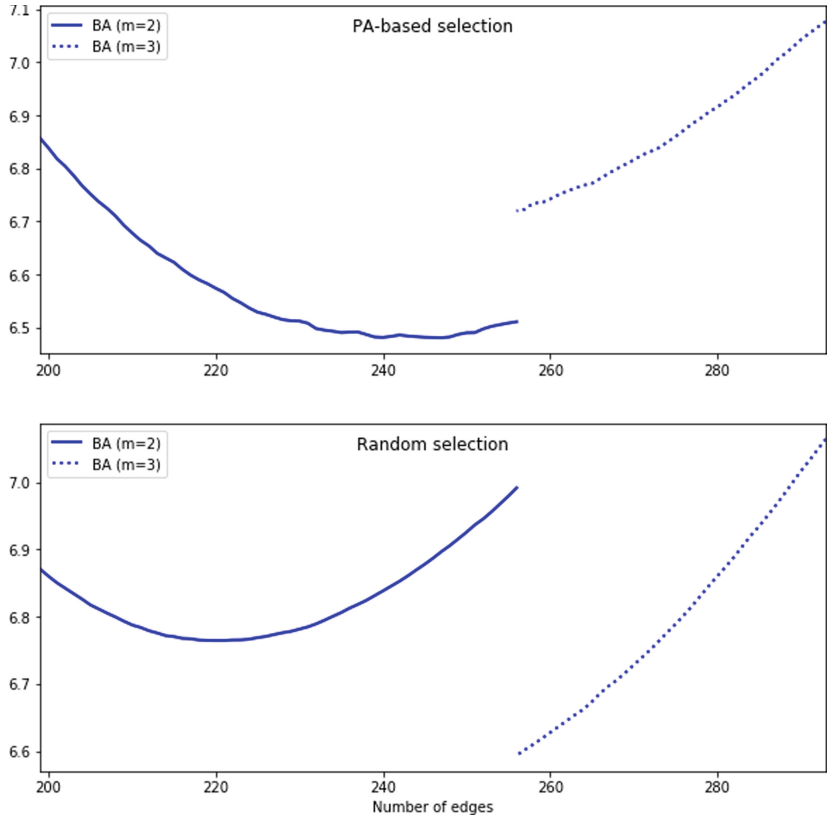

Fig. 1. Spectral distances evolution during the addition/deletion of edges. Upper subplot: spectral distance of the adjacency matrix using the preferential attachment-based selection of edges; Lower subplot: same distance using a random selection of edges.

4 Discussion and Conclusions

This paper paves the way to a new branch of criminal network analysis by providing a new perspective on how SNA methods can help LEAs. We applied tools

from Network Science and Graph Theory on a real criminal network dataset with the aim to discover new ways to use artificial networks on police investigations. The idea is to find a way to replicate the topology of real criminal networks through classical models widely used in the state-of-art for several domains.

Consequently, we computed two distance metrics on different artificial models to find the one which better reproduces the features of a real criminal network topology. To do so, we started by computing the DeltaCon distance on ER, WS, and BA models. This metric is independent from the graphs' size and, from our experiments, it has only suggested which model(s) could be discarded, moving towards the computation of the spectral distance. However, even by using this metric, small differences emerge because the error range overlap some of the models outcomes. Hence, we adjusted the edges' number of the artificial networks, in order to match the real criminal size used as litmus test. The link selection criteria followed is twofold: first, we selected the pair of nodes accordingly with the preferential attachment (resp., detachment) that also takes into account the nodes' degree; second, we opted for a randomly choice of the links that need to be added (resp., removed).

So far the conclusion is that the BA model unveiled to be the closest one to the real dataset considered for the comparison among the ones herein investigated. Performance was not significantly affected by its construction. The results obtained suggest pathways to new scenarios and applications; indeed, the use of an artificial model may significantly help LEAs. Starting from the investigation data (even though affected by *noise* or *missing information*), it could be possible in the future to create a substitute model that replicates, closely enough, the criminal network under scrutiny. Thus, it could be useful for the investigators to make their decisions in terms of how to efficiently spread their resources (i.e., policeman, patrols, etc.): from one side, the artificial model could be able to predict (and prevent) the creation of relationship ties between criminals; on the other side, LEAs could quickly intervene to break the links among them (when already present) by arresting one or more of the suspects.

As future work, we wish to extend those tests performing them on different spectral distance configurations (such as, choosing the Laplacian, rather than the Adjacency matrix, as the latter appears as the weakest among the matrix representations of a graph [34]) as well as including both of the real criminal networks we modelled (i.e., Meetings and Phone Calls) as they are complementary to each other and a joint analysis may offer a better view on the overall interconnections. As those networks are weighted, we would like to discover whether and how weights influence the performances obtained by the artificial models herein investigated. Another interesting point is to try to answer to another open question that is how to compare through SNA two different real criminal networks in order to unveil whether there are some analogies despite their size.

References

1. Agreste, S., Catanese, S., De Meo, P., Ferrara, E., Fiumara, G.: Network structure and resilience of Mafia syndicates. Inf. Sci. **351**, 30–47 (2016). https://doi.org/10.1016/j.ins.2016.02.027
2. Akoglu, L., Tong, H., Koutra, D.: Graph based anomaly detection and description: a survey. Data Min. Knowl. Discov. **29**(3), 626–688 (2015). https://doi.org/10.1007/s10618-014-0365-y
3. Barabási, A.L., Albert, R.: Emergence of scaling in random networks. Science **286**(5439), 509–512 (1999). https://doi.org/10.1126/science.286.5439.509
4. Berlusconi, G., Calderoni, F., Parolini, N., Verani, M., Piccardi, C.: Link prediction in criminal networks: a tool for criminal intelligence analysis. PLoS ONE **11**(4), 1–21 (2016). https://doi.org/10.1371/journal.pone.0154244
5. Calderoni, F., Catanese, S., De Meo, P., Ficara, A., Fiumara, G.: Robust link prediction in criminal networks: a case study of the Sicilian Mafia. Expert Syst. Appl. **161**, 113–666 (2020). https://doi.org/10.1016/j.eswa.2020.113666
6. Campana, P.: Explaining criminal networks: strategies and potential pitfalls. Methodological Innov. **9**, 205979911562274 (2016). https://doi.org/10.1177/2059799115622748
7. Cavallaro, L., Ficara, A., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Song, W., Liotta, A.: Criminal Network: the Sicilian Mafia. "Montagna Operation" (2020). https://doi.org/10.5281/zenodo.3938818
8. Cavallaro, L., Ficara, A., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Song, W., Liotta, A.: Disrupting resilient criminal networks through data analysis: the case of Sicilian Mafia. PLoS ONE **15**(8), 1–22 (2020). https://doi.org/10.1371/journal.pone.0236476
9. De Moor, S., Vandeviver, C., Vander Beken, T.: Assessing the missing data problem in criminal network analysis using forensic DNA data. Soc. Netw. **61**, 99–106 (2020). https://doi.org/10.1016/j.socnet.2019.09.003
10. Donnat, C., Holmes, S.: Tracking network dynamics: a survey using graph distances. Ann. Appl. Stat. **12**(2), 971–1012 (2018). https://doi.org/10.1214/18-AOAS1176
11. Duijn, P.A.C., Kashirin, V., Sloot, P.M.A.: The relative ineffectiveness of criminal network disruption. Sci. Rep. **4**(1), 4238 (2014). https://doi.org/10.1038/srep04238
12. Emmert-Streib, F., Dehmer, M., Shi, Y.: Fifty years of graph matching, network alignment and network comparison. Inf. Sci. **346–347**, 180–197 (2016). https://doi.org/10.1016/j.ins.2016.01.074
13. Erdös, P., Rényi, A.: On random graphs I. Publicationes Mathematicae **6**, 290–297 (1959)
14. Ferrara, E., De Meo, P., Catanese, S., Fiumara, G.: Detecting criminal organizations in mobile phone networks. Expert Syst. Appl. **41**(13), 5733–5750 (2014). https://doi.org/10.1016/j.eswa.2014.03.024
15. Ficara, A., Cavallaro, L., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Liotta, A.: Social network analysis of sicilian mafia interconnections. In: Complex Networks and Their Applications VIII, pp. 440–450. Springer International Publishing (2020). https://doi.org/10.1007/978-3-030-36683-4_36
16. Finckenauer, J.O.: Problems of definition: what is organized crime? Trends Organized Crime **8**(3), 63–83 (2005). https://doi.org/10.1007/s12117-005-1038-4
17. Gambetta, D.: The Sicilian Mafia: The Business of Private Protection. Harvard University Press, Cambridge (1996)

18. Gilbert, E.N.: Random graphs. Ann. Math. Stat. **30**(4), 1141–1144 (1959). https://doi.org/10.1214/aoms/1177706098
19. Johnsen, J.W., Franke, K.: Identifying central individuals in organised criminal groups and underground marketplaces. In: Shi, Y., Fu, H., Tian, Y., Krzhizhanovskaya, V.V., Lees, M.H., Dongarra, J., Sloot, P.M.A. (eds.) Computational Science – ICCS 2018, pp. 379–386. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-93713-7_31
20. Kleemans, E.R., de Poot, C.J.: Criminal careers in organized crime and social opportunity structure. Eur. J. Criminol. **5**(1), 69–98 (2008). https://doi.org/10.1177/1477370807084225
21. Koutra, D., Vogelstein, J.T., Faloutsos, C.: DeltaCon: A principled massive-graph similarity function. In: Proceedings of the 2013 SIAM International Conference on Data Mining, pp. 162–170 (2013). https://doi.org/10.1137/1.9781611972832.18
22. Newman, M.E.J.: Estimating network structure from unreliable measurements. Phys. Rev. E **98**, 062321 (2018). https://doi.org/10.1103/PhysRevE.98.062321
23. Paoli, L.: Mafia brotherhoods: organized crime, Italian style. Oxford University Press, Oxford Scholarship Online (2008). https://doi.org/10.1093/acprof:oso/9780195157246.001.0001
24. Peixoto, T.P.: Reconstructing networks with unknown and heterogeneous errors. Phys. Rev. X **8**, 041011 (2018). https://doi.org/10.1103/PhysRevX.8.041011
25. Robinson, D., Scogings, C.: The detection of criminal groups in real-world fused data: using the graph-mining algorithm "GraphExtract". Secur. Inform. **7**(1), 2 (2018). https://doi.org/10.1186/s13388-018-0031-9
26. Rostami, A., Mondani, H.: The complexity of crime network data: a case study of its consequences for crime control and the study of networks. PLoS ONE **10**(3), 1–20 (2015). https://doi.org/10.1371/journal.pone.0119309
27. Soundarajan, S., Eliassi-Rad, T., Gallagher, B.: A guide to selecting a network similarity method. In: Proceedings of the 2014 SIAM International Conference on Data Mining, pp. 1037–1045 (2014). https://doi.org/10.1137/1.9781611973440.118
28. Squartini, T., Mastrandrea, R., Garlaschelli, D.: Unbiased sampling of network ensembles. New J. Phys. **17**(2), 023052 (2015). https://doi.org/10.1088/1367-2630/17/2/023052
29. Tantardini, M., Ieva, F., Tajoli, L., Piccardi, C.: Comparing methods for comparing networks. Scientific Rep. **9**(1), 17557 (2019). https://doi.org/10.1038/s41598-019-53708-y
30. Villani, S., Mosca, M., Castiello, M.: A virtuous combination of structural and skill analysis to defeat organized crime. Socio-Econ. Plann. Sci. **65**(C), 51–65 (2019). https://doi.org/10.1016/j.seps.2018.01.002
31. Watts, D.J., Strogatz, S.H.: Collective dynamics of 'small-world' networks. Nature **393**(6684), 440–442 (1998). https://doi.org/10.1038/30918
32. Williams, P.: Transnational criminal networks. Netw. Netwars Future Terror, Crime, Militancy **1382**, 61 (2001)
33. Wills, P., Meyer, F.G.: Metrics for graph comparison: a practitioner's guide. PLoS ONE **15**(2), 1–54 (2020). https://doi.org/10.1371/journal.pone.0228728
34. Wilson, R.C., Zhu, P.: A study of graph spectra for comparing graphs and trees. Pattern Recogn. **41**(9), 2833–2841 (2008). https://doi.org/10.1016/j.patcog.2008.03.011