Graph and Network Theory for the Analysis of Criminal Networks

Lucia Cavallaro, Ovidiu Bagdasar, Pasquale De Meo, Giacomo Fiumara, and Antonio Liotta

Abstract Social Network Analysis is the use of Network and Graph Theory to study social phenomena, which was found to be highly relevant in areas like Criminology. This chapter provides an overview of key methods and tools that may be used for the analysis of criminal networks, which are presented in a real-world case study. Starting from available juridical acts, we have extracted data on the interactions among suspects within two Sicilian Mafia clans, obtaining two weighted undirected graphs. Then, we have investigated the roles of these weights on the criminal networks properties, focusing on two key features: weight distribution and shortest path length. We also present an experiment that aims to construct an artificial network which mirrors criminal behaviours. To this end, we have conducted a comparative degree distribution analysis between the real criminal networks, using some of the most popular artificial network models: Watts-Strogats, Erdős-Rényi, and Barabási-Albert, with some topology variations. This chapter will be a valuable tool for researchers who wish to employ social network analysis within their own area of interest.

L. Cavallaro (✉) · O. Bagdasar
University of Derby, Derby, UK
e-mail: l.cavallaro@derby.ac.uk

O. Bagdasar
e-mail: O.Bagdasar@derby.ac.uk

P. De Meo · G. Fiumara
University of Messina, Messina, Italy
e-mail: pdemeo@unime.it

G. Fiumara
e-mail: gfiumara@unime.it

A. Liotta
Free University of Bozen-Bolzano, Bolzano, Italy
e-mail: Antonio.Liotta@unibz.it

G. Fortino et al. (eds.), *Data Science and Internet of Things*, Internet of Things,
https://doi.org/10.1007/978-3-030-67197-6_8

1 Introduction

Graph Theory is a well established field in mathematics. However, only recently many of its theoretical results started to be used within Social Network Analysis (SNA), an area with significant implications for real world scenarios. For example, one can simulate the behaviour of social networks using strategies like link predictions [1, 2], temporal networks, or spreading of influences [3, 4]. Other practical applications include to deal with large Artificial Neural Networks [5–7] or targeted advertisements to people based on their friends' interests [8] or, on the other side, containing the spread of fake news [9].

Network Science tools may also be used in the investigation of criminal networks. Sometimes the complex social interactions within a clan-based society may help the feature selection process for building machine learning models [10]. Other times, it is Network Science itself that helps conducting better performing investigation from law enforcement agencies. To this end, criminal networks can be encoded as graphs, and various types of analysis and simulations can be carried out for modelling criminal behaviours.

This chapter is to intended as a short tutorial on how Network Science strategies may be used to conduct an in-depth analysis on real criminal networks. Here, the Sicilian Mafia scenario has been considered. Section 4 relates to our previous analysis on this topic. In particular, Sect. 4.4 includes a comparative Degree Distribution analysis between real criminal networks and artificial ones. Indeed, when it is possible to find out a synthetic network reflecting the behaviour of real-world criminal networks, law enforcement agencies (LEAs) and network scientists can recreate those networks and simulate how interconnections among criminal will evolve.

This chapter is structured as follows. Section 2 presents the key theoretical tools (required for understanding the experiments conducted in Sect. 4), and it is divided in two parts: (i) tools, where the basic definitions on network science are provided; and (ii) popular artificial networks description (as the topologies used in Sect. 4.4). Next, in Sect. 3 a brief review on the use of (i) Social Network Analysis, and its implication in (ii) Criminal Networks is defined. Section 4 is a case study summarizing our work on two real criminal networks related to Sicilian Mafia [11, 12]. This section includes four parts: (i) datasets description, based on the data extracted from juridical acts; (ii) weights distribution analysis, which represents an important preliminary study to understand how the interactions among suspected are structured in terms of interaction frequency; (iii) shortest path analysis, which allows to identify trusted affiliates inside the clan who can spread confidential and illegal messages; (iv) comparative degree distribution analysis between real and synthetic networks, to artificially recreate the criminal networks used here, with the purpose of conducting further investigations through them. Finally, the conclusions follow in Sect. 5.

2 Complex Networks

In this section we introduce the main Network Science concepts underpinning Social Network Analysis, which are later exemplified in the criminal network case study (Sect. 4). In particular, in Sect. 2.1 the main definitions required for understanding the mechanics of SNA are provided. All theoretical concepts are derived from [13], which we refer to the reader for further technical details.

2.1 Tools

In this section, we start with some basic definitions of Graph Theory.

Graph

Definition 1 A *graph* denoted by $G = (N, E)$, consists of a set of nodes N and a set of edges $E \subseteq N \times N$ (also called links L). It is a convenient way of representing relationships between pairs of objects.

As an example, *Facebook*® may be viewed as a graph, where the nodes represent users and edges represent the friendship relationship among them. Is it also possible to define a *subgraph* as follows:

Definition 2 A *subgraph* H of the graph G is a graph whose nodes and edges are subsets of the nodes and edges of G.

Furthermore, graphs may be either *weighted*, or *unweighted*:

Definition 3 A *weighted graph* $G = (N, E, W)$ is a triplet consisting of a finite set of nodes N, a set of edges E, and a set of weights $W : E \to \mathbb{R}$ defined on each edge. If all edges weights are equal to one, then the graph is called *unweighted*.

Degree

Definition 4 The *degree* of a node n_i, denoted $deg(i)$ or k_i, is the number of incident edges to n_i. The sum of the degrees of all nodes is equal to the double of the number of edges E:

$$\sum_{n \in N} k_n = 2E. \tag{1}$$

Definition 5 In weighted networks, the *weighted degree* (also known as *strength* [14, 15]) is the sum of the edges weights w incident on n_i:

$$k_i = \sum_{(i,j) \in E} w_{ij}, \tag{2}$$

where the summation spans over all edges (i, j) in the network, linked to node n_i.

Definition 6 For undirected networks, the *average degree* is defined as

$$\langle k \rangle = \frac{1}{N} \sum_{i=1}^{N} k_i = \frac{2L}{N}, \tag{3}$$

where N is the total number of nodes, k_i is the degree of a generic node i, and L represents the total number of links, or edges E, within the network.

Small-World

The Small World phenomenon [16, 17] is based on the concept of the six degrees of separations, according to which two random people in the world may be connected each other via a few acquaintances (i.e., it is estimated that there are six people in the middle between the source and the destination). In Network Science, it translates into a "short" distance between two randomly chosen nodes within a network, that is

$$\langle d \rangle \approx \frac{\ln N}{\ln \langle k \rangle}, \tag{4}$$

where N is the total number of nodes in the graph, $\langle k \rangle$ is the network average degree, and $\langle d \rangle$ the average distance within the network. The denominator implies that the denser the network, the smaller the distance between the nodes is. In conclusion, the average path length or the diameter depends logarithmically on the system size.

Degree Distribution

The *degree distribution* p_k provides the probability that a randomly selected node in the network has degree k. Since p_k is a probability, it must be normalized; i.e.,

$$\sum_{i=1}^{\infty} p_k = 1. \tag{5}$$

For a network made of N nodes, the degree distribution is the normalized histogram given by:

$$p_k = \frac{N_k}{N}, \tag{6}$$

where N_k is the number of nodes having degree k.

The degree distribution has assumed a central role in network theory following the discovery of scale-free networks (See "Scale-Free Property" paragraph); moreover, p_k determines many network phenomena, from network robustness to the spread of viruses.

Weight Distribution

The degree distribution can be extended to weighted networks considering the weighted degree (strength) distribution $P(s)$, defined as the probability that a node may have weighted degree (strength) equal to s. Based on [15], this is

$$P(s) \sim s^{-\gamma}, \tag{7}$$

where γ is a constant typical of the network.

Clustering Coefficient

Clustering is used to quantify the relationship among nodes' neighbours. Indeed, the degree only considers the number of direct links between nodes. The *clustering coefficient* C_i measures the edge density in the immediate neighbourhood of a node. $C_i \in [0, 1]$ represents the clustering coefficient of a generic node n_i:

$$\begin{cases} \text{if } C_i = 0, & \text{there are no edges among the node's neighbours} \\ \text{if } C_i = 1, & \text{each node's neighbour is connected with the others} \end{cases}$$

The local clustering coefficient is computed as follow:

$$C_i = \frac{2L_i}{k_i(k_i - 1)}, \tag{8}$$

where k_i is the degree of the generic node n_i, and L_i represents the number of links (i.e., edges) between the k_i neighbours of n_i.

Average Clustering Coefficient

The average $\langle C \rangle$ of $C_i \in i = 1, \ldots, N$ in the whole network is given by

$$\langle C \rangle = \frac{1}{N} \sum_{i=1}^{N} C_i. \tag{9}$$

Adjacency Matrix

A common way to represent relationships among nodes is the *adjacency matrix* A.

Definition 7 The *Adjacency Matrix* $A[i, j]$ holds node degree (weighted or unweighted) to the edge (n_i, n_j) if it exists, where n_i is the node with index i and n_j is the node with index j. If there is no such edge, then $A[i, j] = None$.

For undirected graphs A is symmetric (i.e., $A[i, j] = A[j, i] \, \forall n_i, n_j \in N$).

Path

Definition 8 A *path* is a sequence of alternating nodes and edges that flow from a starting node to an ending one such that each edge is incident to its predecessor and successor node. A path is called *simple* if each node in the path is distinct.

More formally, a path can be defined as a sequence of nodes

$$P = (n_1, n_2, \ldots, n_m) \in N \times N \times \cdots \times N,$$

such that n_i is adjacent to n_{i+1} for $1 \leq i \leq m - 1$. Such a path P is called a path of length $m - 1$ from n_1 to n_m.

Measures based on paths strategies are the **shortest path length analysis**.

Distance

Definition 9 The *distance* from a node n_i to a node n_j in G, denoted $d(n_i, n_j)$ is the length of a **shortest path** from n_i to n_j (if such a path exists).

$$d_{ij} = min\left(\Gamma(i, j)\right),$$

where $\Gamma(i, j)$ is the set of paths connecting i and j.

Connectedness

Definition 10 A graph G is *connected* if, for any two nodes, there is a path between them.

Definition 11 If G is not connected, its maximal connected subgraphs are called the *connected components* of G.

Definition 12 If a network consists of two components, a properly placed link can connect them, making the network connected. Such a link is called *bridge*.

Scale-Free Property

The majority of real networks, such as the World Wide Web, are called *scale-free networks* and follow the definition:

Definition 13 A scale-free network is a network whose degree distribution follows a power law.

The *power-law distribution* has the following form

$$p_k \sim k^{-\gamma}, \tag{10}$$

where the exponent γ is its *degree exponent*.

Some artificial network models such as the **Barabási-Albert (BA) Model** successfully exhibit this feature.

2.2 Artificial Networks

The need for scientists to create Artificial, or Synthetic Networks has been born from the aim to reproduce real network properties in a controlled environment. For this reason, several typologies of Artificial Networks have been formulated.

Three models in particular have found special popularity within the scientific community: The Erdős-Rényi (ER, also known as Random Network) Model, the

Watts-Strogats Model (WS; i.e., a Random Network variation), and the Barabási-Albert (BA) Model. This last one tries to capture two important properties of real network: the growth and the preferential attachment. Further details on those models are provided in the following paragraphs.

Random Network Model

A random network consists of N nodes where each node pair $(n_i, n_j), \forall i, j \in N$ is connected with probability p. To construct a random network one needs to

1.Start with N isolated nodes,
2.Select a node pair (n_i, n_j) and generate a random number $rand \in [0, 1]$:

$$\begin{cases} \text{if} \, rand > p, & \text{connect the selected node pair with a link} \\ \text{otherwise,} & \text{leave them disconnected} \end{cases}$$

3.Repeat the previous step for all pairs of distinct nodes $(n_i, n_j) \in N \times N$.

The network obtained after this procedure is called a *random graph* or a *random network*. There are two definitions of a random network: the definition provided in the Erdős-Rényi Model, and the one of the Gilbert Model.

Erdős-Rényi Model

Random networks are also called *Erdős-Rényi Networks* from the names of the mathematicians Paul Erdős (1913–1996) and Alfréd Rényi (1921–1970), who studied the properties of these networks. Their model follow the structure

$$G(N, L), \tag{11}$$

where N labeled nodes are connected with L randomly placed links (i.e., edges). Paul Erdős and Alfréd Rényi used this definition in their paper [18].

Gilbert Model

It is a variation of the Erdős-Rényi Model. It has been defined by Edgar Nelson Gilbert (1923–2013) and follows the structure

$$G(N, p), \tag{12}$$

where each pair of N labeled nodes is connected with probability p.

There are two main limits in Random Network Model that had to be overcome over the years by the academic community:

1. The local clustering coefficient in ER model is given by [13]

$$C_i = \frac{\langle k \rangle}{N}.$$

   This behaviour of C_i is contradicted by the local clustering coefficient of real networks.
2. The Poisson distribution that describes the degree distribution of ER networks does not allow large differences between the worst- and best-connected nodes in the network. This implies that hubs, frequently observed in real networks, cannot be found in ER networks. BA model, relying on preferential attachment and growth, successfully reproduces this fundamental feature.

In the following paragraphs those models are described.

Watts-Strogats Model

Two main considerations motivated Duncan J. Watts (1971) and Steven Strogatz (1959) to propose this model: (i) in real networks the average distance between two nodes depends logarithmically on N (See "Small-World" average distance $\langle d \rangle$); (ii) the average clustering coefficient $\langle C \rangle$ of real networks is much higher than expected for a random network of similar N and L (i.e., E).

To construct a random network according to *Watts-Strogats* Model [19]:

1. Start from a ring of N nodes, whereas each node is connected to its immediate previous and next neighbours; hence, each node has $\langle C \rangle = 3/4$, initially.
2. With probability $p \in [0, 1]$ each link is rewired to a randomly chosen node

$$\begin{cases} \text{if } p \simeq 0, & \text{regular lattice} \\ \text{if } 0 < p < 1, & \text{Small-World property} \\ \text{if } p = 1, & \text{Random Network Model (all links rewired).} \end{cases}$$

The Watts-Strogatz model interpolates between a *regular lattice*, which has high clustering (but lacks the Small-World phenomenon), and a *random network*, which has low clustering (but displays the Small-World property). Moreover, high nodes degrees are absent from Watts-Strogatz model.

Barabási-Albert Model

This model was theorized by Albert-László Barabási (1967) and Réka Albert (1972) [20]. It simulates a Scale-Free Network rather than a Random one, by introducing two new concepts to the model: network growth and the preferential attachment. The first concept assumes that real networks continuously increase over time, so new nodes must be considered. The second point argues that random connections defined by a fixed probability do not reflect the behaviour of real networks; in fact, in real scenarios, nodes tend to link to the more connected nodes.

Definition 14 The *Preferential Attachment* is the probability $\Pi(k)$ that a link of the new node n_j connects to node n_i depends on the degree k_i through the formula

$$\Pi(k_i) = \frac{k_i}{\sum_j k_j}. \tag{13}$$

To construct an artificial network with the Barabási-Albert model, the steps are:

1. Start with a set of N_0 nodes, the links between which are chosen arbitrarily, as long as each node has at least one link.
2. **Growth** – At each timestep a new node n_j with l links (with $l \le l_0$) that connects the new node to nodes already in the network is added.
3. The connections between the new node with the older nodes are defined by the **Preferential Attachment** probability.

3 Social Network Analysis in Criminal Networks

In this section we provide an overview of state-of-the-art of Social Network Analysis applied to Criminal Networks. We also consider the most relevant studies concerning specifically the Sicilian Mafia criminal topologies.

3.1 Criminal Networks Analysis

Through SNA, LEAs are able to analyze criminal networks and investigate the relations among criminals. For this reason, nowadays there is a growing interest in the application of Graph and Network Science onto criminal networks. For instance, SNA has been used in [21] to build crime prevention systems. However, due to the lack of data availability on those kind of networks, there are difficulties in finding relevant quantitative studies. Such examples are those conducted by Szymanski [22] and Berlusconi [23], on the problem of community detection and link prediction.

3.2 Sicilian Mafia Networks

Sicilian Mafia has a particular structure that differs from common criminal networks (such as the terrorist nets), whereby it is a common practice for criminals to come together to achieve a common goal and then fall apart. By contrast, in Sicilian Mafia this behaviour does not occur. Indeed, the affiliates are bound by blind loyalty and they still pursue further goals even after achieving a previous one. Moreover, Families last for several generations. They also tend to diversify their objectives: from controlling entire economic sectors (e.g., by giving "protection" to small traders and taking control of larger factories), to influencing countries political life (e.g., by interfering in the results of electoral competitions). Sicilian Mafia originated in Sicily, and has now spread worldwide [24–26]. The blind loyalty of affiliates makes it even more difficult to obtain reliable information about those criminal networks topologies: important information about such criminal network is likely to be missing or hidden, due to the covert and stealthy nature of criminal actions [27–30].

4 Case Study: The Sicilian Mafia

This section describes firstly the real criminal datasets we used for our tests, followed by a brief summary on the strategies conducted jointly with the results obtained so far as an example on Network Science strength, and how it can be used to significantly help LEAs. In particular, the experiments relate to: (i) weight distribution, (ii) shortest path length, and (iii) degree distribution.

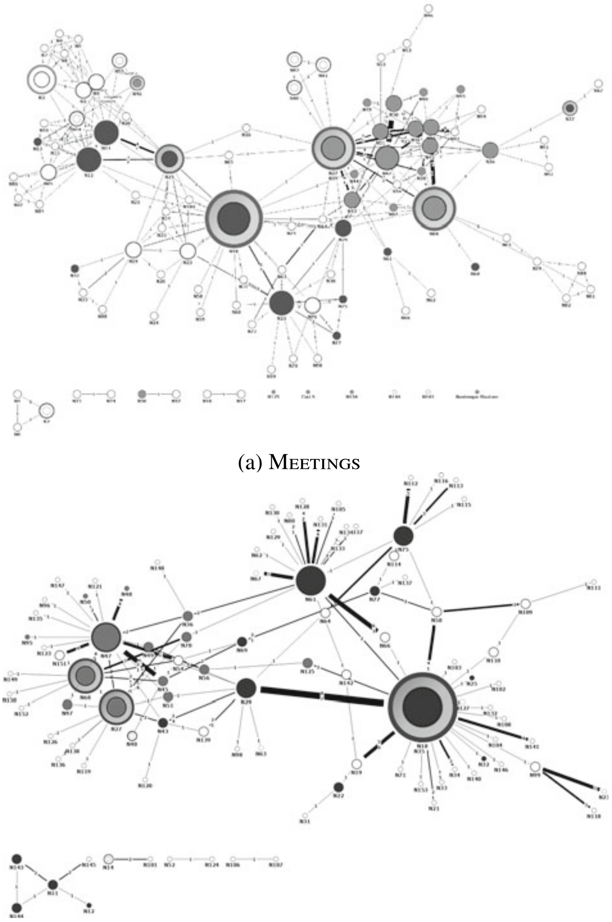
4.1 Dataset Description

The case study example relates to two real-world datasets [31] we built from juridical acts[1] [12]: (i) the *Meetings* dataset represents the physical meetings among criminals obtained through LEA evensdropping; (ii) the *Phone Calls* dataset refers to phone calls between individuals obtained through LEA interceptions.

This particular investigation was a prominent operation conducted during the first decade of the 2000s and focused on two Mafia clans known as the "Mistretta" family, and the "Batanesi" clan [11, 12, 32].

Both datasets led to undirected and weighted graphs; thus, edge weights w are available and represent the number of times any given pair had a meeting in the *Meetings* dataset, and the number of times two individuals called each other in *Phone Calls* dataset. In SNA, those coefficients are also known as the strength of the tie binding two individuals [11]. In Fig. 1, the graphs obtained as well as the description of what each element represents (i.e., nodes, colours, edges weight, nodes and edges size, etc.) is shown. The main characteristics of the datasets are summarized in Table 1.

[1] Source code are available at https://github.com/lcucav/criminal-nets.



(a) Meetings

(b) Phone Calls

Fig. 1 Dataset Description. The colours represent different clans: darker nodes are the "Mistretta" family; in grey the "Batanesi" clan is drawn; white and light gray circled nodes and for two others Mafia families not directly involved in the current investigation. All *circled* nodes represent the *bosses*. Lastly, white nodes represent other subjects not classifiable in any of the previous categories. Edges' width depends on the number of meetings or phone calls, while the nodes size relates with their degree. (Reproduced from Ficara et al. 2020)

4.2 Weight Distribution Analysis

Figure 2 shows the weight distribution of the *Meetings* and the *Phone Calls* networks. As already mentioned, the weights represent the amount of meetings and phone calls exchanged between pairs of individuals in the networks, respectively.

It is noteworthy that in both these networks there are just a few high-weight edges; i.e., nodes incident on those links exhibit an high number of interaction within the

Table 1 Characteristics of *Meetings* and *Phone Calls* networks. (Reproduced from Ficara et al. 2020)

Parameter	Meetings	Phone calls
No. nodes	101	100
No. edges	256	124
Max. weight	10	8
Max. frequency	200	100
Avg. degree	5.07	2.48
Max. shortest path	7	14
Common nodes	47	

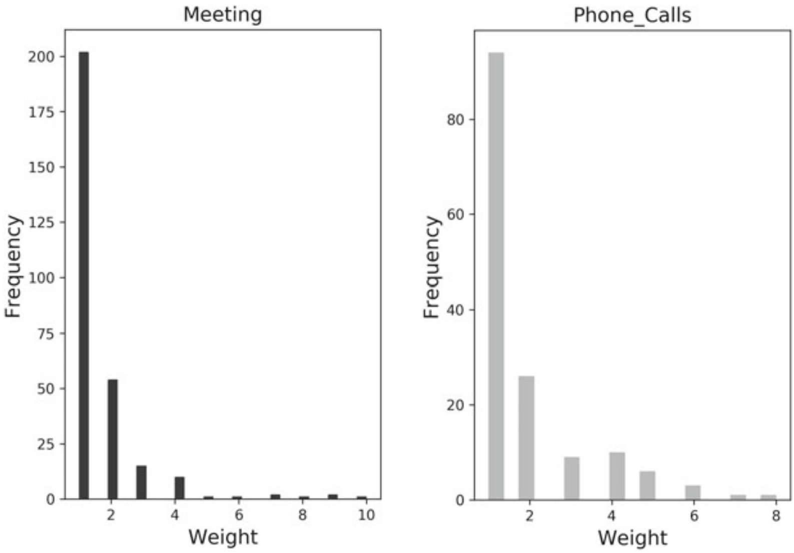
network. In [11], we motivated this behaviour as a necessity from affiliates to focus their efforts in trying to reduce the risk of being intercepted by external people (i.e., LEA, and other people outside the clan). In the *Meetings* network, this trend is even more accentuated; moreover, the maximum interactions weight (i.e., $w = 10$) is greater than its counterpart in the *Phone Calls* network (i.e., $w = 8$).

Our explanation is that mobsters prefer to communicate by face-to-face meetings, rather than calling each other, to reduce interception risks. Furthermore, bosses often have to participate to public events to pursue their power inside a clan, including: funerals of other affiliates, and other solemn religious demonstrations (masses, processions, etc.). It is a well known practice that, during those kinds of events, bosses pass messages to their closest subordinate affiliates.

4.3 Shortest Path Length Analysis

The shortest path length distribution in Fig. 3 is closely related to dynamic properties such as velocity of messages spreading process within the network. Generally speaking, the criminal organizations structure aims to optimize the interaction frequency among members, while reducing as much as possible the interception risks. Thus, trusted members may be discovered by following short interactions paths; indeed, those affiliates may also be acting as a *bridge* (See Sect. 2.1“Connectedness”) to connect distant groups in the network.

In [11] we noticed that both the weighted and the unweighted shortest path length analyses show a higher interaction frequency among affiliates throughout a “balanced” number of intermediates. This means that they do not like to spread their encrypted messages with a too low (resp., high) number of intermediates. This is to avoid, from one side, to overexpose their bosses to police investigations. From the other side, the longer the sequence of intermediates, the higher the chances to be intercepted by people outside the Family.



(a) Meetings

(b) Phone Calls

Fig. 2 Weight distribution in the Meetings dataset (**a**), and the Phone Calls dataset (**b**). (Reproduced from Ficara et al. 2020)

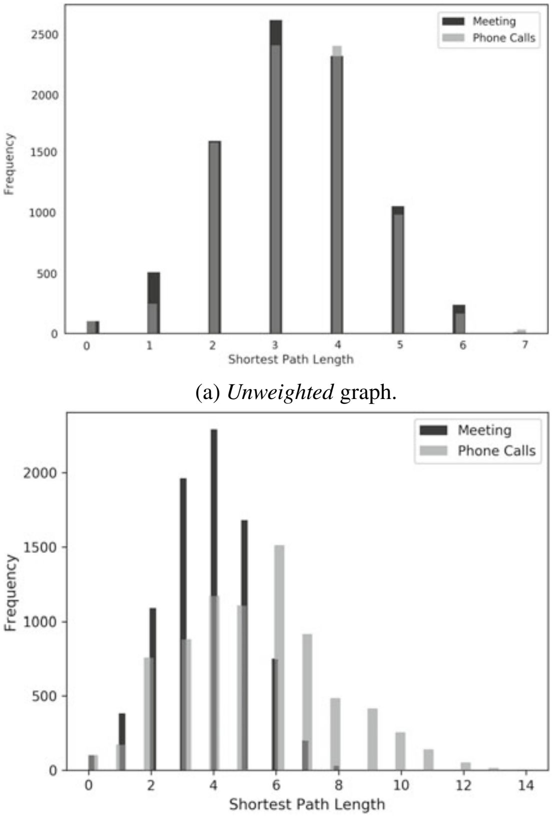
Even through this analysis, as it was for the weights distribution, it emerged that the clan tries to minimize the risk of interceptions, especially to avoid exposing those mobsters who are hierarchically in a higher rank.

4.4 Degree Distribution Analysis

The Degree Distribution Analysis has been conducted in order to discover an appropriate artificial network that would virtually mirror the real-world criminal graphs topology under scrutiny. We previously analysed the weight distribution, but due to lack of libraries available for weighted graphs analysis,[2] we opted for a preliminary analysis on nodes degree distribution. To this end, in Fig. 4 we compared our real criminal networks against five artificial models: (i) the Random Network by Gilbert (G-ER), (ii) Watts-Strogatz (WS), (iii) its variant accordingly with Newmann [33] (N-WS), and (iv) two different configurations of the Barabási-Albert (BA) model in terms of links added at each step; BA2 with $m = 2$, and BA3 with $m = 3$. Tables 2 and 3 summarize the number of edges and average degree obtained with the configurations above described in *Phone Calls* and *Meetings* graphs, respectively.

[2] https://networkx.github.io/documentation/networkx-1.9/reference/generators.html.

Fig. 3 Distribution of shortest path lengths in MEETINGS and PHONE CALLS networks in Unweighted (**a**) and Weighted (**b**) graphs. (Reproduced from Ficara et al. 2020)



(a) *Unweighted* graph.

(b) *Weighted* graph.

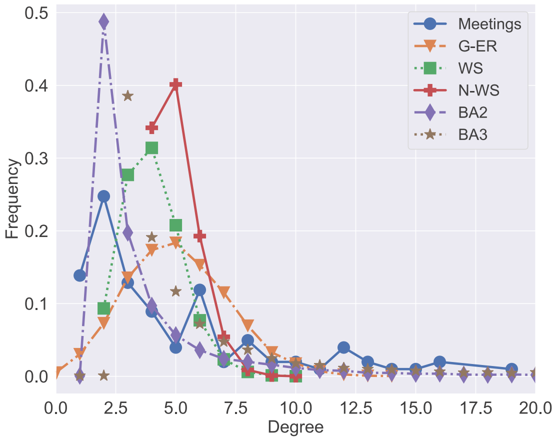
Note that all the results herein shown represent the average results obtained after 100 runs per each synthetic network.

We initially compared the real networks with the Erdős-Rényi (ER) topology, but this model did not allow to customize the number of links. Then, we opted for the Gilbert one, whereby both number of nodes n and links m are defined a priori.

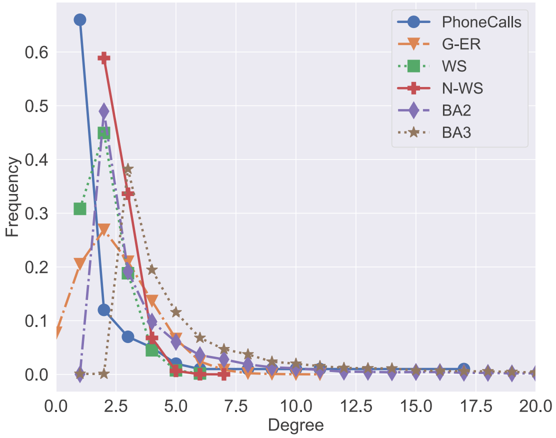
In the WS model, we set $n, k = \frac{2m}{n}$ (that represents the number of nearest neighbors links per node), and the rewiring probability $p = 0.5$, with $p \in [0, 1]$. As previously asserted in Sect. 2.2, if $p = 1$, we turn into a Random Network. The main difference between WS and N-WS models is that in WS, number p is the probability of rewiring each edge; whereas in N-WS, $p = 0.25$ is the probability of adding a new edge for each edge. Indeed, if $p = 1$, then number of edges is doubled.

The actual graphs degree distributions act very differently from one another. In particular, the fluctuations in *Meetings* are justified by the fact that face-to-face encounters have been observed not only between couple of suspects, but also among groups of more than two people at the same time. On the other hand, phone calls have only been considered between individual suspects. The analysis suggests that through

Fig. 4 Degree Distribution in the MEETINGS dataset (**a**), and the PHONE CALLS datasets (**b**). Circles give the actual datasets values. G-ER is the Random Network proposed by Gilbert. WS is the Watts-Strogatz network. N-WS is the Newmann variation of WS. BA2 and BA3 are the Barabási-Albert models with $m = 2$ and $m = 3$, respectively



(a) MEETINGS



(b) PHONE CALLS

Table 2 Characteristics of artificial models in the *Phone Calls* network

Model	No. edges	Avg. degree
G-ER	124	2.48
WS	100	2.00
N-WS	123	2.46
BA2	196	3.92
BA3	291	5.82

Table 3 Characteristics of artificial models in the *Meetings* network

Model	No. edges	Avg. degree
G-ER	256	5.07
WS	202	4.00
N-WS	250	4.95
BA2	198	3.92
BA3	294	5.82

degree distribution it was not possible to identify an appropriate artificial network that best fits the network characteristics of the two real-world datasets considered. This is mainly due to the size of the networks. In fact, artificial networks seem to work better with lager sizes; thus, are quite unstable in the first step of their creation. For example, the emergence of hubs in BA models cannot be highlighted because of the small size of the overall network obtained.

5 Conclusions

This chapter aims to showcase the applicability of Graph Theory in Criminology, during a time when the use of SNA by LEAs is growing substantially. The case study herein reported as an example, explores different approaches on criminal networks analysis by means of network science tools.

In our study we have first created a graph from data extracted from juridical acts; then, we started a twofold preliminary investigation: a weight distribution analysis, and in parallel, a shortest path length analysis. These have been conduced to identify the extent by which weighted graphs are useful in those small networks.

Thus, we conducted a comparative degree distribution analysis between our real-world networks and some models generated by popular artificial networks. The aim was to identify the appropriate synthetic network which could simulate criminal networks artificially, but in an effective manner. The strength of this idea is that we may also be able to understand the patterns followed by criminals to create their internal interconnections among affiliates. Our study has found that the network size is a limitation. Indeed, there are significant fluctuations and through degree distribution comparative analysis it was not possible to find an appropriate artificial network that accurately mirrors the two real criminal networks used in our tests.

To overcome this issue, in future studies we will investigate adjacency matrix structures for both real and synthetic networks to get insights into network topologies.

References

1. Linyuan, L., Zhou, T.: Link prediction in complex networks: a survey. Phys. A Stat. Mech. Appl. **390**(6), 1150–1170 (2011). https://doi.org/10.1016/j.physa.2010.11.027
2. Hasan, M.A., Zaki, M.J.: A survey of link prediction in social networks. In: Aggarwal, C. (ed.) Social Network Data Analytics. Springer, Boston, MA (2011)
3. Tassiulas, L., Katsaros, D., Basaras, P.: Detecting influential spreaders in complex, dynamic networks. Computer **46**(4), 24–29 (2013). https://doi.org/10.1109/MC.2013.75
4. Cavallaro, L., Costantini, S., De Meo, P., Liotta, A., Stilo, G.: Network connectivity under a probabilistic node failure model. In: ArXiv e-print (Jun 2020). arXiv: 2006.13551 [cs.SI]
5. Mocanu, D.C., Mocanu, E., Stone, P., Nguyen, P.H., Gibescu, M., Liotta, A.: Scalable training of artificial neural networks with adaptive sparse connectivity inspired by network science. Nat. Commun. **9**(1), 1–12 (2018)
6. Cavallaro, L., Bagdasar, O., De Meo, P., Fiumara, G., Liotta, A.: Network science strategies for accelerating the training of artificial neural networks. In: Numerical Computations: Theory and Algorithms NUMTA 2019, p. 169 (2019)
7. Cavallaro, L., Bagdasar, O., De Meo, P., Fiumara, G., Liotta, A.: Artificial neural networks training acceleration through network science strategies. In: Sergeyev, Y.D., Kvasov, D.E. (eds.) Numerical Computations: Theory and Algorithms, pp. 330–336. Springer International Publishing, Cham (2020)
8. Bellur, U., Kulkarni, R.: Improved matchmaking algorithm for semantic web services based on bipartite graph matching. In: IEEE International Conference on Web Services (ICWS 2007), Salt Lake City, UT, pp. 86-93 (2007)
9. Zhou, X., Zafarani, R.: Fake news: a survey of research, detection methods, and opportunities. In: ArXiv e-print (Dec 2018). arXiv:1812.00315 [cs.CL]
10. Oluwabunmi, O., Cosma, G., Liotta, A.: Clan-based cultural algorithm for feature selection. In: 2019 International Conference on Data Mining Workshops (ICDMW), pp. 465–472. IEEE (2019)
11. Ficara, A., Cavallaro, L., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Liotta A.: Social network analysis of sicilian mafia interconnections. In: Cherifi, H., Gaito, S., Mendes, J., Moro, E., Rocha, L. (eds.) Complex Networks and Their Applications VIII. COMPLEX NETWORKS 2019. Studies in Computational Intelligence, vol. 882, pp. 440–450. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-36683-4_36
12. 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), e0236476 (2020). https://doi.org/10.1371/journal.pone.0236476
13. Barabási, A.L., Pósfai, M.: Network Science. Cambridge University Press, Cambridge (2016). http://barabasi.com/networksciencebook/
14. Antoniou, Ioannis: E and Tsompa, ET : Statistical analysis of weighted networks. Discret. Dyn. Nat. Soc. **2008** (2008). https://doi.org/10.1155/2008/375452
15. Barthélemy, M., Barrat, A., Pastor-Satorras, R., Vespignani, A.: Characterization and modeling of weighted networks. Phys. A Stat. Mech. Appl. **346**(1–2), 34–43 (2005). https://doi.org/10.1016/j.physa.2004.08.047
16. Travers, J., Milgram, S.: The small world problem. Psychol. Today **1**(1), 61–67 (1967)
17. Milgram, S.: An experimental study of the small world problem. Sociometry **32**(4), 425–443. American Sociological Association (1969). https://doi.org/10.2307/2786545
18. Erdős, P., Rényi, A.: On random graphs I. Publicationes Mathematicae **6** 290–297 (1959)
19. Watts, D.J., Strogatz, S.H.: Collective dynamics of small-world networks. Nature **393**, 440–442 (1998)
20. Barabási, A.L., Albert, R.: Emergence of scaling in random networks. Science **286**, 509–512 (1999)
21. Chen H., Chung W., Xu J., Wang G., Qin Y., Chau M.: Crime data mining: a general framework and some examples. IEEE Comput. **37**, 50–56. IEEE (2004). https://doi.org/10.1109/MC.2004.1297301

22. Bahulkar, A., Szymanski, B.K., Baycik, N.O., Sharkey, T.C.: Community detection with edge augmentation in criminal networks. In: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 1168–1175. IEEE (2018)
23. Berlusconi, G., Calderoni, F., Parolini, N., Verani, M., Piccardi, C.: Link prediction in criminal networks: a tool for criminal intelligence analysis. Public Library of Science. PLoS ONE. **11**(4), 1–21 (2016). https://doi.org/10.1371/journal.pone.0154244
24. Franchetti, L., Sonnino, S.: La Sicilia nel 1876. **1**. Barbèra G. (1877)
25. McGloin, J.M.: Policy and intervention considerations of a network analysis of street gangs. Criminol. Public Policy **4**(3), 607–635 (2005). https://doi.org/10.1111/j.1745-9133.2005.00306.x
26. Mastrobuoni, G., Patacchini, E.: Organized crime networks: an application of network analysis techniques to the American Mafia. Rev. Netw. Econ. **11**(3) (2012). https://doi.org/10.1515/1446-9022.1324
27. Krebs, V.: Mapping networks of terrorist cells. Connections **24**(3), 43–52. INSNA (2002)
28. Xu, J., Chen, H.: Criminal network analysis and visualization. Commun. ACM **48**(6), 100–107. ACM (2005). https://doi.org/10.1145/1064830.1064834
29. Calderoni, F., Morselli, C.: Inside criminal networks. Eur. J. Crim. Policy Res. **16**(1), 69–70 (2010). https://doi.org/10.1007/s10610-010-9118-7
30. Campana, P., Varese. F.: Listening to the wire: criteria and techniques for the quantitative analysis of phone intercepts. Trends Organ. Crime **15**(1), 13–30 (2012). https://doi.org/10.1007/s12117-011-9131-3
31. Cavallaro, L., Ficara, A., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Song, W., Liotta, A.: Criminal Network: The Sicilian Mafia. "Montagna Operation" (Version 0.0.1) [Data set]. Zenodo. (2020). https://doi.org/10.5281/zenodo.3938818
32. Castaldo, F. (ed.): Messina, arrestati il capo ed i sodali della "Famiglia mafiosa di Mistretta". In: Grandangolo, il giornale di Agrigento (Jan. 18th 2019). https://www.grandangoloagrigento.it/mafia/messina-arrestati-il-capo-ed-i-sodali-della-famiglia-mafiosa-di-mistretta
33. Newman, M.E.J., Watts, D.J.: Renormalization group analysis of the small-world network model. Phys. Lett. A **263**(4), 341–346 (1999). https://doi.org/10.1016/S0375-9601(99)00757-4