UNIVERSITY OF PALERMO

PHD JOINT PROGRAM:
UNIVERSITY OF CATANIA - UNIVERSITY OF MESSINA
XXXIV CYCLE

DOCTORAL THESIS

Social network analysis approaches to study crime

Author:
Annamaria FICARA

Supervisor:
Prof. Giacomo FIUMARA

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in

Mathematics and Computational Sciences

February 28, 2022

Declaration of Authorship

I, Annamaria FICARA, declare that this thesis titled, "Social network analysis approaches to study crime" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: Annamaria Ficara

Date: 28/02/2022

"Ignorance is the mother of all crimes. Crime is first of all foolishness."

Honoré de Balzac

"When it comes to anything you want to do in your life, you have to be passionate. Success may come, but in the end, the most important thing is that you are doing what you really want to do."

Chiara Ferragni

UNIVERSITY OF PALERMO

Abstract

Department of Mathematics and Computer Sciences

Doctor of Philosophy

Social network analysis approaches to study crime

by Annamaria FICARA

Social Network Analysis (SNA) studies groups of individuals and can be applied in a lot of areas such us organizational studies, psychology, economics, information science and criminology. One of the most important results of SNA has been the definition of a set of centrality measures (*e.g.*, degree, closeness, betweenness, or clustering coefficient) which can be used to identify the most influential people with respect to their network of relationships.

The main problem with computing centrality metrics on social networks is the typical big size of the data. From the computational point of view, SNA represents social networks as graphs composed of a set of nodes connected by another set of edges on which the metrics of interest are computed. To overcome the problem of big data, some computationally-light alternatives to the standard measures, such as Game of Thieves or WERW-Kpath, can be studied. In this regard, one of my main research activities was to analyze the correlation among standard and nonstandard centrality measures on network models and real-world networks.

The centrality metrics can greatly contribute to intelligence and criminal investigations allowing to identify, within a covert network, the most central members in terms of connections or information flow. Covert networks are terrorist or criminal networks which are built from the criminal relationships among members of criminal organizations. One of the most renowned criminal organizations is the Sicilian Mafia.

The focal point of my research work was the creation of two real-world criminal networks from the judicial documents of an anti-mafia operation called Montagna conducted by a specialized anti-mafia police unit of the Italian Carabinieri in Messina (*i.e.*, the third largest city on the island of Sicily). One network includes meetings and the other one records telephone calls among suspected criminals of two Sicilian Mafia families. This dataset is unique and it might represent a valuable resource for better understanding complex criminal phenomena from a quantitative standpoint.

Different SNA approaches have been used on these Montagna networks to describe their structure and functioning, to predict missing links, to identify leaders or to evaluate police interventions aimed at dismantling and disrupting the networks. Graph distances have been used to find a network model able to properly mime the structure of a Mafia network and to quantify the impact of incomplete data not only on Mafia networks such as the Montagna ones but also on terrorist and street gangs networks. The two simple Montagna networks have been finally used to build a multilayer network trying to obtain a more nuanced understanding of the network structure and of the strategic position of nodes in the network.

Acknowledgements

I would like to thank my supervisor Prof. Giacomo Fiumara for encouraging me in all the time of my academic research and daily life. He initiated me into a totally new type of research about criminal networks that I deeply love and that I hope to continue in the coming years under his supervision. His continuous support, advice and patience were invaluable during my PhD study.

I would also like to thank Prof. Pasquale De Meo for his treasured support. The shape of the experimental methods and results of my research activities was really influenced by his plentiful experience.

I also appreciate all the technical support I received from Dr. Salvatore Catanese. Thanks to his collaboration, it was possible to access the judicial documents of the Montagna anti-mafia operation from which most of my research works originate.

I would like to express gratitude to Prof. Francesco Oliveri for his mentorship. Without his immense knowledge, I would never learned to know and love computer science.

I would also like to thank Prof. Antonio Liotta for his support and guidance on my study and most of all for introducing me to his brilliant centrality measure called Game of Thieves.

I would like to extend my sincere thanks to Prof. Maria Carmela Lombardo for all the assistance she provided during my PhD study.

I also sincerely thank the reviewers Prof. Matteo Magnani and Prof. Andrea Tagarelli for reading my thesis carefully and giving their valuable comments.

My gratitude extends to DigForAsp for the funding opportunity to attend two International Schools in Lillehammer (Norway) and Budapest (Hungary) which were very interesting, instructive and suggestive. In particular, I would like to thank Prof. Katrin Franke for her precious suggestions about how to perform a presentation.

I would like to thank the colleagues I have met during international conferences and schools and all the speakers who provided me new ideas for my research activity.

My appreciation also goes out to my research team in Messina, Bolzano and Derby. They made my study and life a wonderful time thanks to their kind help and support.

Finally, I would like to express my gratitude to my parents, my family and my friends. It would not possible for me to complete my study without their encouragement and understanding in the past few years.

Contents

List of Figures

List of Tables

List of Publications

1. Ficara, A., Cavallaro, L., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., and Liotta, A. (2020). "Social Network Analysis of Sicilian Mafia Interconnections". In: *Complex Networks and Their Applications VIII*. ed. by H. Cherifi, S. Gaito, J. F. Mendes, E. Moro, and L. M. Rocha. Cham: Springer International Publishing, pp. 440–450. DOI: 10.1007/978-3-030-36683-4_36
2. Calderoni, F., Catanese, S., De Meo, P., Ficara, A., and Fiumara, G. (2020). "Robust link prediction in criminal networks: A case study of the Sicilian Mafia". In: *Expert Systems with Applications* 161, p. 113666. DOI: 10.1016/j.eswa.2020.113666
3. Cavallaro, L., Ficara, A., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Song, W., and Liotta, A. (2020b). "Disrupting resilient criminal networks through data analysis: The case of Sicilian Mafia". In: *Plos One* 15.8, pp. 1–22. DOI: 10.1371/journal.pone.0236476
4. Cavallaro, L., Ficara, A., Curreri, F., Fiumara, G., De Meo, P., Bagdasar, O., and Liotta, A. (2021). "Graph Comparison and Artificial Models for Simulating Real Criminal Networks". In: *Complex Networks & Their Applications IX*. ed. by R. Benito, C. Cherifi, H. Cherifi, E. Moro, L. Rocha, and M. Sales-Pardo. Cham: Springer International Publishing, pp. 286–297. DOI: 10.1007/978-3-030-65351-4_23
5. Ficara, A., Fiumara, G., De Meo, P., and Liotta, A. (2021b). "Correlations Among Game of Thieves and Other Centrality Measures in Complex Networks". In: *Data Science and Internet of Things: Research and Applications at the Intersection of DS and IoT*. ed. by G. Fortino, A. Liotta, R. Gravina, and A. Longheu. Cham: Springer International Publishing, pp. 43–62. DOI: 10.1007/978-3-030-67197-6_3
6. Ficara, A., Fiumara, G., De Meo, P., and Catanese, S. (2021e). "Multilayer Network Analysis: The Identification of Key Actors in a Sicilian Mafia Operation". In: *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*. Ed. by D. Perakovic and L. Knapcikova. Cham: Springer International Publishing, pp. 120–134. DOI: 10.1007/978-3-030-78459-1_9
7. Ficara, A., Saitta, R., Fiumara, G., De Meo, P., and Liotta, A. (2021d). "Game of Thieves and WERW-Kpath: Two Novel Measures of Node and Edge Centrality for Mafia Networks". In: *Complex Networks XII*. ed. by A. Teixeira, D. Pacheco, M. Oliveira, H. Barbosa, B. Gonçalves, and R. Menezes. Cham: Springer International Publishing, pp. 12–23. DOI: 10.1007/978-3-030-81854-8_2
8. Ficara, A., Fiumara, G., De Meo, P., and Liotta, A. (2021a). "Correlation analysis of node and edge centrality measures in artificial complex networks". In: *Proceedings of Sixth International Congress on Information and Communication*

Technology. Ed. by X.-S. Yang, S. Sherratt, N. Dey, and A. Joshi. Cham: Springer International Publishing. DOI: 10.1007/978-3-030-81854-8_2

9. Ficara, A., Cavallaro, L., Curreri, F., Fiumara, G., De Meo, P., Bagdasar, O., Song, W., and Liotta, A. (2021c). "Criminal networks analysis in missing data scenarios through graph distances". In: *PLOS ONE* 16.8, pp. 1–18. DOI: 10.1371/journal.pone.0255067

10. Ficara, A., Curreri, F, Cavallaro, L, De Meo, P, Fiumara, G, Bagdasar, O, and Liotta, A. (2021f). "Social network analysis: the use of graph distances to compare artificial and criminal networks". In: *J Smart Environ Green Comput* 1, pp. 159–172. DOI: 10.20517/jsegc.2021.08

11. Ficara, A., Curreri, F., Fiumara, G., De Meo, P., and Liotta, A. (2022a). *Covert Network Constructing, Disruption and Resilience: A survey*. (submitted)

12. Ficara, A., Fiumara, G., Catanese, S., De Meo, P., and Liu, X. (2022c). *The whole is greater than the sum of the parts: a multilayer approach on criminal networks*. (submitted)

13. Ficara, A., Curreri, F., Fiumara, G., and De Meo, P. (2022b). *Human and social capital strategies for Mafia network disruption*. (submitted)

Author Contributions

- Ficara, A., Cavallaro, L., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., and Liotta, A. (2020). "Social Network Analysis of Sicilian Mafia Interconnections". In: *Complex Networks and Their Applications VIII*. ed. by H. Cherifi, S. Gaito, J. F. Mendes, E. Moro, and L. M. Rocha. Cham: Springer International Publishing, pp. 440–450. DOI: 10.1007/978-3-030-36683-4_36
  Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Writing (Original Draft Preparation).

- Calderoni, F., Catanese, S., De Meo, P., Ficara, A., and Fiumara, G. (2020). "Robust link prediction in criminal networks: A case study of the Sicilian Mafia". In: *Expert Systems with Applications* 161, p. 113666. DOI: 10.1016/j.eswa.2020.113666
  Conceptualization, Data Curation, Formal Analysis, Writing (Original Draft Preparation), Writing (Review and Editing).

- Cavallaro, L., Ficara, A., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Song, W., and Liotta, A. (2020b). "Disrupting resilient criminal networks through data analysis: The case of Sicilian Mafia". In: *Plos One* 15.8, pp. 1–22. DOI: 10.1371/journal.pone.0236476
  Formal analysis, Investigation, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation).

- Cavallaro, L., Ficara, A., Curreri, F., Fiumara, G., De Meo, P., Bagdasar, O., and Liotta, A. (2021). "Graph Comparison and Artificial Models for Simulating Real Criminal Networks". In: *Complex Networks & Their Applications IX*. ed. by R. Benito, C. Cherifi, H. Cherifi, E. Moro, L. Rocha, and M. Sales-Pardo. Cham: Springer International Publishing, pp. 286–297. DOI: 10.1007/978-3-030-65351-4_23
  Conceptualization, Data Curation, Formal Analysis, Writing (Original Draft Preparation), Writing (Review and Editing).

- Ficara, A., Fiumara, G., De Meo, P., and Liotta, A. (2021b). "Correlations Among Game of Thieves and Other Centrality Measures in Complex Networks". In: *Data Science and Internet of Things: Research and Applications at the Intersection of DS and IoT*. ed. by G. Fortino, A. Liotta, R. Gravina, and A. Longheu. Cham: Springer International Publishing, pp. 43–62. DOI: 10.1007/978-3-030-67197-6_3
  Conceptualization, Data Curation, Formal Analysis, Funding Acquisition, Investigation, Methodology, Project Administration, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation).

- Ficara, A., Fiumara, G., De Meo, P., and Catanese, S. (2021e). "Multilayer Network Analysis: The Identification of Key Actors in a Sicilian Mafia Operation". In: *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*. Ed. by D. Perakovic and L. Knapcikova. Cham: Springer International Publishing,

pp. 120–134. DOI: 10.1007/978-3-030-78459-1_9
Conceptualization, Data Curation, Formal Analysis, Funding Acquisition, Investigation, Methodology, Project Administration, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation).

- Ficara, A., Saitta, R., Fiumara, G., De Meo, P., and Liotta, A. (2021d). “Game of Thieves and WERW-Kpath: Two Novel Measures of Node and Edge Centrality for Mafia Networks”. In: *Complex Networks XII*. ed. by A. Teixeira, D. Pacheco, M. Oliveira, H. Barbosa, B. Gonçalves, and R. Menezes. Cham: Springer International Publishing, pp. 12–23. DOI: 10.1007/978-3-030-81854-8_2
Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation).

- Ficara, A., Fiumara, G., De Meo, P., and Liotta, A. (2021a). “Correlation analysis of node and edge centrality measures in artificial complex networks”. In: *Proceedings of Sixth International Congress on Information and Communication Technology*. Ed. by X.-S. Yang, S. Sherratt, N. Dey, and A. Joshi. Cham: Springer International Publishing. DOI: 10.1007/978-3-030-81854-8_2
Conceptualization, Data Curation, Formal Analysis, Funding Acquisition, Investigation, Methodology, Project Administration, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation).

- Ficara, A., Cavallaro, L., Curreri, F., Fiumara, G., De Meo, P., Bagdasar, O., Song, W., and Liotta, A. (2021c). “Criminal networks analysis in missing data scenarios through graph distances”. In: *PLOS ONE* 16.8, pp. 1–18. DOI: 10.1371/journal.pone.0255067
Conceptualization, Data Curation, Formal Analysis, Investigation, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation).

- Ficara, A., Curreri, F, Cavallaro, L, De Meo, P, Fiumara, G, Bagdasar, O, and Liotta, A. (2021f). “Social network analysis: the use of graph distances to compare artificial and criminal networks”. In: *J Smart Environ Green Comput* 1, pp. 159–172. DOI: 10.20517/jsegc.2021.08
Conceptualization, Data Curation, Formal Analysis, Project Administration, Resources, Software, Validation, Visualization, Writing (Review and Editing).

- Ficara, A., Curreri, F., Fiumara, G., De Meo, P., and Liotta, A. (2022a). *Covert Network Constructing, Disruption and Resilience: A survey*. (submitted)
Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation), Writing (Review and Editing).

- Ficara, A., Fiumara, G., Catanese, S., De Meo, P., and Liu, X. (2022c). *The whole is greater than the sum of the parts: a multilayer approach on criminal networks*. (submitted)
Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation), Writing (Review and Editing).

- Ficara, A., Curreri, F., Fiumara, G., and De Meo, P. (2022b). *Human and social capital strategies for Mafia network disruption*. (submitted)

Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Resources, Software, Validation, Visualization, Writing (Original Draft Preparation), Writing (Review and Editing).

List of Abbreviations

SNA	**S**ocial **N**etwork **A**nalysis
LEAs	**L**aw **E**nforcement **A**gencie**s**
ER	**E**rdös **R**ényi network
SW	**S**mall **W**orld network
WS	**W**atts **S**trogatz model
NWS	**N**ewman **W**atts **S**trogatz model
SF	**S**cale **F**ree network
PA	**P**referential **A**ttachment
BA	**B**arabási **A**lbert model
EBA	**E**xtended **B**arabási **A**lbert model
MN	Montagna **M**eeti**N**gs network
PC	Montagna **P**hone **C**alls network
SN	Infinito **S**ummits **N**etwork
WR	Oversize **W**iretap **R**ecords network
AW	Oversize **A**rrest **W**arrant network
JU	Oversize **JU**dgment network
SV	**S**ur**V**eillance network
CV	**C**a**V**iar network
ASG	**A**bu **S**ayyaf **G**roup
PK	**P**hilippines **K**idnappers network
DC	**D**egree **C**entrality
BC	**B**etweenness **C**entrality
EBC	**E**dge **B**etweenness **C**entrality
CL	**CL**oseness centrality
CC	**C**lustering **C**oefficient
textbfEC	**E**igenvector **C**entrality
PR	**P**age**R**ank
KC	**K**atz **C**entrality
GoT	**G**ame **o**f **T**hieves
WKP	**W**ERW **K** **P**ath
AS	**A**utonomous **S**ystems
JC	**J**accard **C**oefficient
CN	**C**ommon **N**eighbors
AA	**A**damic-**A**dar coefficient
BFS	**B**readth **F**irst **S**earch
DFS	**D**epth **F**irst **S**earch
PPR	**P**ersonalized **P**age**R**ank
TPR	**T**rue **P**ositive **R**ate
TNR	**T**rue **N**egative **R**ate
AUROC	**A**rea **U**nder the **R**eceiving **O**perating **C**urve
LCC	**L**argest **C**onnected **C**omponent
CI	**C**ollective **I**nfluence

Dedicated to my grandparents

Introduction

My research activity focuses on Social Network Analysis (SNA). SNA studies groups of individuals and can be applied in a lot of areas such us organizational studies, psychology, economics, information science and criminology. Social Network Sites like Facebook, Twitter or Instagram have grown exponentially thus providing new challenges for the application of SNA methods.

One of the most important results of SNA has been the definition of a set of measures that describe the role of single individuals with respect to their network of relationships. These so-called centrality measures are of great practical relevance since, *e.g.*, they can be used to identify influential people with the potential of controlling the information flow inside communication networks. The main standard centrality metrics, *i.e.*, degree, closeness, betweenness, and clustering coefficient, are fundamental to increase our understanding of a network.

Centrality measures are also used in the more general field of complex network analysis for applications such as studying landscape connectivity to understand the movement of organisms, analyzing proteins and gene networks, studying the propagation of diseases, or planning urban streets for optimal efficiency. These metrics can greatly contribute to intelligence and criminal investigations allowing to identify, within a covert network, the most central members in terms of connections or information flow (Calderoni and Superchi, 2019). Covert networks are terrorist or criminal networks which are built from the criminal relationships among members of criminal organizations. Different terms can be adopted to refer to a criminal organization, like syndicates, crews, gangs, firms or mafia. Mafia was defined by Gambetta (1996) as a "territorially based criminal organization that attempts to govern territories and markets"; he particularly calls *original Mafia* the criminal group located in Sicily.

The starting point of my research work was the creation of two real-world criminal networks from the judicial documents of an anti-mafia operation called Montagna conducted by a specialized anti-mafia police unit of the Italian Carabinieri in Messina (*i.e.*, the third largest city on the island of Sicily) (Ficara et al., 2020). One network includes meetings and the other one records telephone calls among suspected criminals of two Mafia families. This dataset is unique and it might represent a valuable resource for better understanding complex criminal phenomena from a quantitative standpoint.

The main problem with computing centrality metrics on complex networks is the typical size of the data. The large size of current social networks makes their quantitative analysis challenging. From the computational point of view, SNA represents social networks as graphs on which the metrics of interest are computed. Graphs are defined as a set of nodes or actors with edges or links between them and with no edges connecting a node to itself.

To overcome the problem of big data, some computationally-light alternatives to the standard centrality measures should be found. De Meo et al. (2012, 2013, 2014) presented a novel measure called the K-path to compute link centrality. The advantage of using this metric is that it can be computed with a near-linear time algorithm called Weighted Edge Random Walks – K Path (WERW-Kpath). More recently, Mocanu, Exarchakos, and Liotta (2018) developed an algorithm called Game of Thieves which is able to compute actors and links centrality in a polylogarithmic time.

We explored the correlation among standard and nonstandard measures on network models and real-world freely available networks (Ficara et al., 2021a,b) and then on real-world Mafia networks extracted from three different anti-mafia operations (Ficara et al., 2021d).

The identification of the most central actors in a covert network and their removal belongs to one of the two disruption strategies in which we can categorize criminal network disruption: the social capital approach and the human capital approach. A third strategy comes from the combination of the other two: the mixed approach. We reviewed and classified network disruption methods in Ficara et al. (2022a). We also used a social capital approach to disrupt the Montagna networks simulating different intervention procedures: sequential and block node removal (Cavallaro et al., 2020b). The first one refers to those scenarios in which police arrest one criminal at a time. The second strategy simulates police raids.

Information on a covert network is often likely to be missing or hidden. These networks are usually incomplete, incorrect and inconsistent. Law Enforcement Agencies (LEAs) may in fact have limited resources or make unintentional errors. Investigations often encounter individuals unrelated to the criminal organization (*e.g.*, friends, relatives, and other frequent contacts). Moreover, some members of the criminal organization actively attempt to avoid detection (*e.g.*, by refraining from the use of telephone, using intermediaries, and coding messages). In criminal network analysis, missing data can refer to missing nodes and/or missing edges. LEAs plan to get reliable results from the application of link prediction algorithms to address the problem of missing edges which is a critical impediment to understand network boundaries and topology. In particular, we tackled the problem of estimating the robustness of link prediction algorithms in the Montagna networks (Calderoni et al., 2020). First, we applied several link prediction algorithms and observed that link prediction algorithms leveraging the full graph topology provide very accurate results even on very sparse networks. Second, we carried out extensive simulations to investigate how the noisy and incomplete nature of criminal networks may affect the accuracy of link prediction algorithms.

We also faced the missing data problem in covert networks of different nature (*i.e.*, Mafia, terrorist and street gang networks) from a different prospective (Ficara et al., 2021c). We first used random edge and node removal strategies. Edge removal simulates the scenario in which LEAs fail to intercept some calls or to spot sporadic meetings among suspects. Node removal models the situation in which some suspects cannot be intercepted or investigated. Then, we used graph distances to compare the complete and the pruned networks. This comparison allows to quantify the impact of incomplete data and to determine which network type is most affected by it.

Graph distances have also been used to compare a Mafia network with several network models with the aim to identify the model able to properly mime the structure and behavior of a covert network (Cavallaro et al., 2021; Ficara et al., 2021f). Artificial but realistic models can, in fact, represent a useful tool for LEAs to simulate and study the structure, evolution and faults of criminal networks. LEAs could create models which replicate criminal networks starting from the investigation data, even if they are affected by noise or missing information. Network models could be used to predict and prevent the creation of relationship ties between criminals or to break those ties by arresting one or more of the suspects.

SNA studies have led to an improvement and to a generalization of existing tools to networks with multiple subsystems and layers of connectivity. These kind of networks are usually called multilayer networks. Some networked systems can be better modeled by multilayer structures where the individual nodes develop relationships in multiple layers. For this reason, we built a multilayer network from the single-layer Montagna networks and we focused on the identification of key actors using different approaches with and without considering the layered structure (Ficara et al., 2021e). The analysis of multiple layers within a criminal network provides a complete picture of the network structure identifying actors with strategic positions whose centrality does not emerge from the analysis of the single-layer networks.

This dissertation is structured as follows. Chap. 1 contains the description of data management issues, including the methods that may be used to collect and validate data and those to transform the original criminal information into graphs. All the network models and real criminal networks used in our studies are also introduced. Chap. 2 regards the leader identification problem including the explanation of standard and nonstandard centrality measures and the correlation analysis among them. Chap. 3 is about the use of graph distances to compare artificial and real criminal networks. Chap. 4 describes the problem of missing data in covert networks that we faced, at first, using link prediction algorithms in the Montagna networks and, then, using graph distances in several covert networks. Chap. 5 explains the three main disruption strategies. It also describes the concept of resilience and the characteristics of resilient covert networks. Then, it focuses on our approach to disrupt the Montagna networks. Chap. 6 is about the use of a multilayer approach on the Montagna dataset.

Chapter 1

Covert networks

Organized crime is a category of groups operating covertly and illegally outside the boundaries of the law that could potentially have devastating effects on both the social and economic order (Everton, 2012; Xu and Chen, 2008). Criminal relationships can be studied in terms of network theory as covert or dark networks, which usually include terrorist and criminal networks.

A criminal network can be represented as a simple graph composed by a set of nodes or actors connected by another set of edges or links supporting in some way or other the commission of illegal actions.

Criminal networks are the result of large number of different pieces of information. In particular, physical and/or audio surveillance stakeouts are usually used together with documents from criminal prosecutions (Morselli, 2008), law enforcement agencies accounts (Malm and Bichler, 2011), interviews with suspects and case studies describing the operation of secret organizations (Erickson, 1981). The elements of a criminal network are the individuals appearing in the records, after a judicious screening removed those not involved in criminal activities (*e.g.*, family, friends, legitimate business partners and suppliers) (Faust and Tita, 2019). Communications, meetings, financial transactions and trading of illicit goods are modeled using edges (Faust and Tita, 2019).

Access to data related to criminal organizations, and in particular records from wiretapping activities (Berlusconi et al., 2016), is difficult. This may explain why most studies in this sector rely on a limited number of case studies involving only one source of information. Criminal networks are covert and most of the information is not publicly available. This leads to small datasets available for analysis, and most importantly severely limits the range of applicability of the findings (Jupp, 2012).

Also terrorist social networks can be represented as graphs where nodes in the network represent actors or groups, and the links between the nodes demonstrate their relationship with each other. An edge among terrorists or groups of terrorists can exist if they communicated with each other or if they were present on the location of the same attack.

The main difference between terrorism and organized crime lies in their purpose. While terrorism is carried out in order to achieve a political aim, organized crime is usually perpetrated for material gain, financial or otherwise. For terrorist groups, the illicit acquisition or sale of goods and services is most often viewed as a means to achieve their political or ideological goals, rather than the goal itself. By contrast, for organized criminal groups, the illicit acquisition or sale of goods and services is the goal.

Morselli, Giguère, and Petit (2007) compared the structure of criminal and terrorist organizations, explaining the connection between time-to-task (*i.e.*, the interplay between time and action), and their vulnerability. Terrorist organizations are characterized by a limited time-to-task and a particularly efficient communication system at the core. In these way, actions take place as quickly as possible, and the probability to be detected is considerably reduced. A terrorist organization, in fact, might accomplish its intents by one single but successful terrorist attack. Criminal organizations are characterized by a longer time-to-task, and a less efficient communication system at the core. Actions may be delayed for an extended period during which criminals can operate within secure settings. These organizations try to stand flexible and agile adapting quickly to external shocks (Kleemans and van de Bunt, 1999; Raab, 2003).

1.1 Network constructing

1.1.1 Data collection and incompleteness

SNA is based on the adoption of real datasets as sources: this allows to construct the networks that are then analytically studied (Calderoni et al., 2020; Cavallaro et al., 2020b; Duijn, Kashirin, and Sloot, 2014; Ficara et al., 2020; Robinson and Scogings, 2018; Rostami and Mondani, 2015b; Villani, Mosca, and Castiello, 2019). Anyhow, the acquisition of complete network data that is able to describe the whole structure and all of the activities of a criminal group in its entirety is theoretically impossible to attain (Rothenberg, 2002).

During investigations, the suspected criminals will indeed always try to conceal sensible information. For this reason, LEAs have to adopt alternative methods by exercising particular inquiring powers in order to collect evidence surreptitiously. So, the information available for successive studies can be collected from sources like phone taps and surveillance (Natarajan, 2000), archives (Morselli and Roy, 2008; Tremblay, Talon, and Hurley, 2001), informants, interrogations to the people involved such as witnesses and suspects (McGloin, 2005; Natarajan and Belanger, 1998), but even from infiltration operations by police.

Yet, in spite of providing significant advantages, the above sources come with an amount of drawbacks as well. For example, if the subjects under investigation become conscious of being phone-tapped, they get inclined to avoid speaking openly about what could turn into self-incriminating evidence (Natarajan, 2000). Phone-taps transcripts themselves are usually sampled and do not include all of the conversations occurred. The transcripts available to researchers come from different kinds of court records, that are the original wiretap records, police reports, arrest warrants, and sentences (Campana and Varese, 2012). In police reports, all relevant conversations are transcribed to be made available to the prosecutor and the judge. This means that anything deemed unrelated to criminal activities, such as conversations about personal or unrelated matters, is not included, which risks introducing misinterpretations by LEAs.

The arrest warrants typically include an even more sampled part of the whole transcripts, along with other relevant information that could come from other investigative sources. Finally, only a fraction of these data are reported in the final sentence, along with other evidences. This means that the amount of electronic surveillance data decreases moving from the original records up to the final sentence (see Fig. 1.1), and it becomes more likely to lose relevant portions of these data. For this reason, it is suggested to avoid using the sentence documentation as a data source for statistical analysis, since the data sampled at that stage is likely to be partial and biased, which may lead to unreliable results (Berlusconi, 2013; Campana and Varese, 2012).

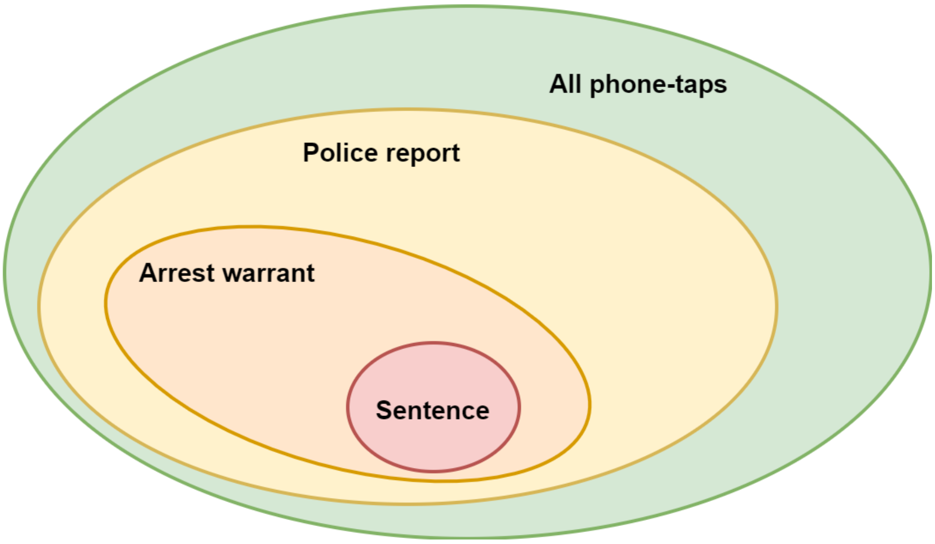

FIGURE 1.1: Sampled phone-tapped conversations between criminals in court records.

Another issue is represented by the fact that different phones and telephone lines are used in criminal communications, making it difficult for the police to phone-tap all of them (Baker and Faulkner, 1993). This can result in either missing links or missing nodes. In the latter case, we may end up missing some surveillance targets, who will not appear in the graphs, risking to miss out on figures holding a central role in the organizations (Morselli, 2008).

Longer-lasting investigations can minimize such problems, since these will reduce the amount of missing data. Interceptions and monitoring of a criminal group going on for months or years will lower the chances for some skilled criminal to avoid detection (Calderoni, 2012; Morselli, 2008). However, these prolonged investigations lead to datasets (and networks) that change over time, due to the dynamic nature of criminal roles and activities. Typically, actors come and go, social relations are built and dismantled, and criminal opportunities change alongside the social context (Charette and Papachristos, 2017; Duijn, Kashirin, and Sloot, 2014).

It is worth noticing that the analysis of networks is based on their particular composition, considered at a given point in time. Yet, since the network changes and evolves over time, different data collection methods may be required in order to cover more time spans (Sparrow, 1991). While investigations are proceeding, the list of suspects tends to evolve as time goes by, not only because of the dynamic nature of such covert networks, but also as a function of strategic decisions by the police. In fact, LEAs normally start their investigations from some key subjects and, then, keep expanding their range by adding further subjects. This approach is close to snowball sampling (Goodman, 1961), that is shown to be better suited for network analysis, as opposed to a random sampling approach. It is indeed shown that the latter holds very high chances of generating distorted inferences on network structures (Robins, 2015). For this reason, it is not adopted.

This snowball-like sampling data collection technique is indeed mixed with purposive sampling (Goodman, 1961), so that LEA decisions have a great impact at the point of being a valuable strategy. Sampling based on human insights is, however, also a possible source of biases. In practice, it may not be possible to monitor all the individuals that appear connected to the central ones. This may be due to lack of resources, which makes it impossible to monitor all active criminals. The investigation is often focused on those individuals for whom it is easier to gather evidence. These constraints lead to partial data collection, with some groups operating under the police sight, while others are left out.

Another source of error arises from the possibility that LEAs misunderstand or misjudge the relevance of specific nodes. There is also the case in which the police omits information, *e.g.*, when undercover agents have not yet been disclosed.

An important data source is represented by other open sources such as public registries (Morselli and Roy, 2008). The case records prosecuted in the criminal courts are publicly available, and may be used for research purposes, but only after case closure. For instance, American LEAs fill crime statistics using some defined standards, and their archives are available online. Nevertheless, as noted above for the case of sampled phone-taps, the information coming from prosecutorial transcripts and criminal investigation files (in general from closed cases) may still present limitations in terms of data accuracy and completeness (Baker and Faulkner, 1993; Berlusconi, 2013).

Files on closed criminal investigations are kept by the police for long periods in order to allow the examination of trends in policing as well as in the behaviors and compositions of criminal groups (Spapens, 2011; Tremblay, Talon, and Hurley, 2001). This kind of judicial documents, intelligence reports, or investigation files are the main data source in the case of micro studies. Whereas in the case of macro studies, the main source are intelligence databases collected by LEAs (Heber, 2009; Malm and Bichler, 2011; Malm, Bichler, and Walle, 2010) and databases created through archival analyses (Mastrobuoni, Patacchini, et al., 2010; Papachristos and Smith, 2012).

In light of the above considerations, it is now well-accepted that criminal-related information (and networks) is typically incomplete, or it is just limited to a specific time span. Therefore, it has to be taken for granted that it is not possible to attain complete network data (Rothenberg, 2002). The problem of missing information is particularly relevant in analyzing criminal networks, since it potentially affects the scope and structure of the network (Malm, Bichler, and Walle, 2010; Morselli, 2008; van der Hulst, 2009). Such incompleteness translates into missing nodes and edges, which can create a domino effect that alters the results of the measures, leading to incoherent inference problems (Ianni and Reuss-Ianni, 1990; Sparrow, 1991). However, some studies have showed that networks measures may still be valid under some missing data scenarios (Ficara et al., 2021c; Malm, Bichler, and Walle, 2010; Morselli, 2008; Xu and Chen, 2008).

1.1.2 Data reliability and validity

In addition to the missing data problem, criminal network data suffer also from incorrectness (Rothenberg, 2002). Data validity and reliability are indeed some of the main problems encountered in studies that apply SNA to organized crime.

During investigations, some of the consulted individuals to gain information might be reliable, as opposed to others that might try to deceive the investigations in order to protect themselves or their associates, or just to achieve some specific goal. This means that investigators deal with data of different quality. Since there is not a typical method in SNA to deal with such different gauges of reliability, the subjective judgement of investigators becomes crucial in the analysis and interpretation of the available intelligence data.

The task of determining the information relevance is known as the problem of signal and noise. In such context, relevant information and a considerable volume of irrelevant or unreliable information are merged. In fact, LEAs often face the issue of possessing very large amounts of data, some of which having hardly any importance. When they deal with great amounts of raw data gathered from several sources, the possibility to occur into inconsistencies becomes inevitably greater.

During collection, data can be evaluated according to source reliability and information validity (McDowell, 2008). In a criminal investigation setting, a source can be classified as:

(1) reliable, when it is authentic, competent and trustworthy;

(2) usually reliable;

(3) unreliable;

(4) unknown, if there is no information about it.

On the other hand, information can be:

(1) truthful, if it is shared by other sources as well, making it consistent;

(2) probable;

(3) doubtful;

(4) unknown, if there is no other data it can be compared with.

Information which is doubtful or derives from sources of unknown reliability may include facts, partial truths, false information, or lies and it consequentially has to be used carefully.

An example of reliability problems is given by data collected through surveys or interviews, that suffer from actors lying (Reuter and Haaga, 1989). Information collected from interrogations are also affected by the risk that the interviewees downplay or amplify their real role, and are not representative of the whole group.

In case of data collected through phone-taps, when the actors talk freely on the phone about some incriminating actions, the transcripts can be considered valid. Yet, a double-check is still needed in order to compare data collected from the taps and data collected from other official records relating to the case. Such verification procedure is necessary, since communications among criminals are frequently packed with lies or codes, in order to conceal the real intention of the conversation (Campana and Federico, 2013).

Beside the police seeking to verify the phone-taps, the criminals themselves may also try to validate whether the information received by fellow criminals is accurate. Longer investigations and surveillance tend to eventually expose this kind of lies. Yet, dynamics is another feature of criminal networks that affects the reliability of data since longer investigations lead to data sets changing over time. There is, then, the potential for a network analysis to become out of date in a short time (Burcher and Whelan, 2018). Analytical techniques, adopted by intelligence, must be capable to handle large amounts of information, and to aid at extracting the signal from the noise.

Because of the above reasons, we can say that data, gathered during criminal investigations, are affected by the following weaknesses:

- Incompleteness, that is inevitable given the covert nature of such type of networks.

- Incorrectness, that can be induced either by unintentional errors during data collection or by criminals intentionally deceiving investigations.
- Inconsistency, that may occur when data regarding the same actors end up being collected multiple times, generating inaccuracies. Such misleading information could, for instance, cause the same actor to appear as different individuals in a network.

Because of the described issues, and since sources themselves reflect the perception of LEAs, the data used in literature are all exposed to biases. This is the main reason why data mining and machine learning techniques are often unsuitable in criminal network analysis. These methods would be effective in discovering trends and patterns automatically from large volumes of data, or for making predictions. On the other side, these methods require good quality data, free from biases, errors and missing data (Murphy, 2012). As it turns out, criminal network analysis views social relationships in terms of network theory.

Scholars have indeed reported difficulties at managing such biases, analyzing the possible limitations they can bring (Bouchard and Ouellet, 2011; Calderoni, 2012; Morselli, 2008; Varese, 2006). Nevertheless, researchers attempted to develop automated data mining techniques for LEAs, such as an automatic actors extractor from police reports and actors inconsistency detectors from networks (Chen et al., 2004).

1.1.3 From data to graph transformation

SNA has to deal with another obstacle in the criminal field, which lies into data transformation into actual graphs.

There is no standard method for this task: the process goes through the subjective judgement of the analyst. For instance, it may be difficult for an analyst to decide whom to include or exclude from the network - the boundaries are often prone to ambiguity (Sparrow, 1991). As stated by LEAs, the boundaries of the overall network do not necessarily correspond to the ones of the criminal group; thus, the analysts may identify by themselves the internal boundaries on the basis of personal experience and theoretical or practical considerations (Morselli, 2008). This problem is known as fuzzy boundaries and it is a well-known challenge for practitioners (Athey and Bouchard, 2013; Borgatti, 2006; Burcher and Whelan, 2015; Duijn, Kashirin, and Sloot, 2014). Data conversion turns out to be, indeed, a quite labor-intensive and time-consuming procedure.

A covert network can be mathematically represented by a simple graph which is defined as a tuple $G = (N, E)$ where $N = \{1, 2, ..., n\}$ is the set composed by n nodes and $E = \{1, 2, ..., e\}$, $E \subseteq N \times N$, is the set of e edges, whose generic element l represents the edge existing between a pair of nodes (i, j).

Some basic definitions from network science are described below (Barabási and Pósfai, 2016; Wasserman and Faust, 1994).

Weight and directionality. The type of graph is defined by edge weight and directionality. If all edges are bidirectional, then the graph is called undirected. If edges have directionality, then the graph is called directed. If edges have weights, then the graph is weighted. The weight is just a numerical value attached to each edge.

Density. Graph density is a measure of how many edges between nodes exist compared to how many edges between nodes are possible. For an undirected graph, it is defined as:

$$\delta = \frac{2e}{n(n-1)} . \tag{1.1}$$

Adjacency matrix. The adjacency matrix of a graph, defined over the set of nodes N, is an $n \times n$ square matrix denoted by $A = (a_{ij})$, $1 \leq i, j \leq n$, where the generic element a_{ij} is defined as:

$$a_{ij} = \begin{cases} 1 & \text{if } i \to j \\ 0 & \text{otherwise} . \end{cases} \tag{1.2}$$

In undirected graphs, $a_{ij} = a_{ji}$ for all $i \neq j$ and therefore the adjacency matrix A will be symmetrical: $A = A^T$ (where T is the transpose representation).

Path. A path is a sequence of nodes such that each node is connected to the next node along the path by an edge.

Shortest path. The shortest path (or distance) d_{ij} between two nodes i and j in a graph is the path with the fewest number of edges.

Average path length. The average path length $\langle d \rangle$ is the average distance between all pairs of nodes in a graph. It is defined as:

$$\langle d \rangle = \sum_{i,j \in N} \frac{d_{ij}}{n(n-1)} . \tag{1.3}$$

Connected component. A connected component cc is a subset of nodes in a graph, so that there is a path between any two nodes that belong to the component, but one cannot add any more nodes to it that would have the same property.

Largest connected component. The largest connected component lcc is the biggest one among all the connected components in a graph. Real undirected networks usually have a lcc which contains most of the nodes in the graph. The rest of the graph is divided into a large number of small components disconnected from the others.

Degree. The degree k of a node i is defined as the number of nodes adjacent to it or as the cardinality of the set of neighbors of that node:

$$k_i = |\mathcal{N}(i)| = |\{j : \exists(i,j) \vee \exists(j,i), j \neq i\}| . \tag{1.4}$$

The degree assumes a discrete value between a minimum of 0 when a node is isolated (*i.e.*, it is not connected to any other node) and a maximum of $n - 1$ if the node is connected to all other nodes in the network. The degree of a node can be calculated by adding the columns (or rows) of the adjacency matrix A:

$$k_i = \sum_{j=1}^{n} a_{ij} = \sum_{i=1}^{n} a_{ij} . \tag{1.5}$$

Average degree. In undirected graphs, the average degree $\langle k \rangle$ is given by twice the total number of edges divided by the total number of nodes:

$$\langle k \rangle = \frac{2e}{n} . \tag{1.6}$$

Degree distribution. The degree distribution p_k provides the probability that a randomly selected node i in the graph has degree k. For a graph with N nodes the degree distribution is a normalized histogram given by:

$$p_k = \frac{n_k}{n} , \tag{1.7}$$

where n_k is the number of nodes with degree equal to k.

Degree matrix. The degree matrix K of a graph is a diagonal matrix where:

$$\mathrm{k_{ij}} = \begin{cases} k_i & \text{if } i = j \\ 0 & \text{otherwise} . \end{cases} \tag{1.8}$$

k_i is the degree of the node i.

Clustering. The average clustering coefficient $\langle CC \rangle$ is the probability that two neighbors of a randomly selected node link to each other. It is defined as:

$$\langle CC \rangle = \frac{1}{N} \sum_{1}^{N} CC(i) , \tag{1.9}$$

where CC_i is the clustering coefficient of a node i which will be deeply explained in Sect. 2.1.

Spectrum. The spectrum of a graph is defined as the set of eigenvalues (sorted in increasing or decreasing order) of one of its representation matrices. It is used to characterize graph properties, and to extract information from its structure. In the case of the adjacency matrix A, if λ_k is its k^{th} eigenvalue, the eigenvalues sorted in descending order $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ compose the spectrum.

1.2 Network models

Graphs are complex networks characterized by non trivial topological features which often occur in networks representing real systems such as criminal networks, social networks, biological networks, brain networks and others. The most studied and well-known classes of complex networks are random graphs, small-world networks, and scale-free networks (see Fig. 1.2).

1.2.1 Random networks

A random network may be simply described by a probability distribution, or by a random process which generates it. The Erdos–Rényi (ER) model is one of two closely related models to generate random networks. There are two variants of the

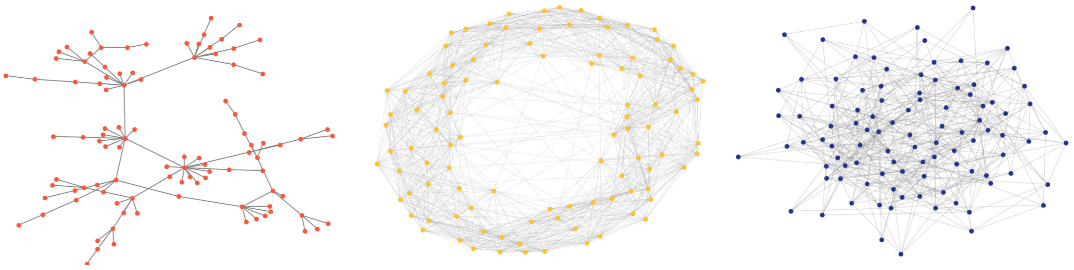

FIGURE 1.2: **Network models.** Scale-free (left column), small-world (middle column) and random graphs (right column).

Erdös Rényi model (Erdös and Rényi, 1959). The first chooses one of all possible networks $G(n, M)$ with n nodes and M edges, where each network has an equal probability. This could be done by choosing M edges from the $\binom{n}{2}$ possible edges. Second variant $G(n, p)$ (Gilbert, 1959) starts with an initial set of n unconnected nodes and includes edges with probability p. It can easily be deduced that each network with n nodes and M edges is equally likely with probability:

$$p^M (1-p)^{\binom{n}{2}-M} . \tag{1.10}$$

1.2.2 Small-world networks

A small-world (SW) network is characterized by a high degree of local clustering (like regular lattices). It also possess short node-node distances. This network model, also called Watts-Strogatz (WS) model, was proposed by Watts and Strogatz (1998). It interpolates between these two extremes by taking a regular lattice, and randomly rewiring some of its edges. Newman and Watts (1999) proposed a real-space renormalization group transformation for the model, and demonstrated that the transformation was exact in the limit of large system size. Given a graph $G(N, E)$, the Newman-Watts-Strogatz small-world model (NWS) is defined as follows:

Step 1 **Ring Creation**. Creation of a ring over n nodes in which each node $i \in N$ is connected with the k closest neighbors. If k is odd, i is connected with the nearest $k-1$ neighbors.

Step 2 **Edge rewiring**. For each edge $(i, j) \in E$, in the underlying n-ring with k nearest neighbors, a new edge (i, x) is added, with randomly-chosen existing node x and probability p.

Compared with the WS model, the random rewiring increases the edges number because new edges are added, and no edges are removed.

1.2.3 Scale-free networks

A scale-free (SF) network is characterized by a degree distribution (see Eq. 1.7) which decays like a power law (Barabási and Albert, 1999). Given a network defined as a graph $G(N, E)$, the scale-free network model of Barabási and Albert (BA) is defined as follows:

Step 1 **Initial condition**. The network consists of n_0 nodes and m_0 edges.

Step 2 **Growth**. One node i with m edges is added at each step. Time t is the number of steps.

Step 3 **Preferential attachment (PA)**. Each edge of i is attached to an existing node j with the following probability:

$$P_i = \frac{k_j}{\sum\limits_{i \in N} k_i} . \tag{1.11}$$

The defined probability is proportional to the degree of node i.

Holme and Kim (Holme and Kim, 2002) proposed a SF network model with two main characteristics: a perfect power-law degree distribution and a high clustering. To incorporate the second one, which is a peculiarity of the SW model, the authors modified the above BA algorithm by adding the following step:

Step 4 **Triad formation**. If an edge (i, j) is added in the PA step, an edge from i to a neighbor of j (chosen randomly) is added. If all neighbors of j are already connected to i (*i.e.*, there are no pair to connect), a PA step is done instead.

Albert and Barabási (2000) also proposed an extension of the standard BA model called Extended Barabási–Albert (EBA) model. Given two probabilities p and q, $p + q < 1$, the model is created according to the following mechanism:

Step 1 With p probability, m new edges are added to the graph, starting from randomly chosen existing nodes and attached preferentially at the other end.

Step 2 With q probability, m existing edges are rewired by randomly choosing an edge, and rewiring one end to a preferentially chosen node.

Step 3 With $(1 - p - q)$ probability, m new nodes are added to the graph with edges attached preferentially.

When $p = q = 0$, the EBA model reduces to the standard BA model.

1.3 Real world networks

Network models, such as those described in Sect. 1.2, are closely similar to real-world networks in terms of network properties. It is easier to perform an analysis on these synthetic networks instead of real-world networks. Moreover, network models can be useful to understand the mathematical basis of real-world networks, and to perform controlled experiments that may not be available to real-world networks.

Most of my research work focused on two real-world criminal networks related to a Mafia operation called Montagna (Calderoni et al., 2020; Cavallaro et al., 2020b, 2021; Ficara et al., 2020, 2021c,d,e).

Then, this research was extended to other seven real-world covert networks. Some of them were also related to two distinct Mafia operations (*i.e.*, Infinito and Oversize), while the others were linked to street gangs and terrorist organizations.

Table 1.1 shows the characterization of the single investigations from which the covert networks were constructed (Ficara et al., 2021c).

TABLE 1.1: Characterization of real-world covert networks.

Investigation	Network			Source
	Name	Nodes	Edges	
Montagna Operation (Sicilian Mafia) 2003-2007	MN PC	Suspects	Physical Surveillance Audio Surveillance	(Calderoni et al., 2020) (Cavallaro et al., 2020a)
Infinito Operation (Lombardian 'Ndrangheta) 2007-2009	SN	Suspects	Physical and Audio Surveillance	(Calderoni and Piccardi, 2014)
Oversize Operation (Calabrian 'Ndrangheta) 2000-2009	WR AW JU	Suspects	Audio Surveillance Physical Surveillance Audio Surveillance	(Berlusconi et al., 2016) (Piccardi et al., 2016)
Swedish Police Operation (Stockholm Street Gangs) 2000-2009	SV	Gang members	Physical Surveillance	(Rostami and Mondani, 2015b) (Rostami and Mondani, 2015a)
Caviar Project (Montreal Drug Traffickers) 1994-1996	CV	Criminals	Audio Surveillance	(Morselli, 2008)
Abu Sayyaf Group (Philippines Kidnappers) 1991-2011	PK	Kidnappers	Attacks locations	(Gerdes, Ringler, and Autin, 2014)

Fig. 1.3 shows the degree distributions for each criminal network as a normalized histogram (Ficara et al., 2021c). The degree distribution p_k provides the probability that a randomly selected node in each covert network has degree k (see Eq. 1.7). Same colors imply the networks belong to the same police investigation. Networks related to the anti-mafia operations Montagna (*i.e.*, MN and PC) and Oversize (*i.e.*, WR, AW and JU), the Swedish Police Operation (*i.e.*, SV) and the Caviar Project (*i.e.*, CV) have similar degree distributions in which most nodes have a relatively small degree k with values around 0, 1 or 2, while a few nodes have very large degree k, and are connected to many other nodes. The Infinito Mafia network (*i.e.*, SN) and the terrorist network of Philippines Kidnappers (*i.e.*, PK) are the only networks having different degree distributions compared to other criminal networks, as most of their nodes have large degree k. In particular, we note that most nodes in PK are strongly connected and have a degree $k = 57$.

SN is a one-mode projection of the original two-mode network in which are represented the meetings and the suspects attending them. This implies that all suspects taking part in a meeting are assumed to be interacting with each other, which could be somewhat artificial. In fact, in crowded meetings some participants may have had a very limited (if any) interaction with other participants. In such case, assuming that all participants interacted with each other may considerably overestimate the real number of connections. However, it must be added that LEAs were only able to identify the participants to meetings, and not the full extent of their interactions. Similar consideration applies to PK which was built based on the presence of the kidnappers in the same place of a terrorist event. Here as well, the existence of an edge linking two terrorists does not necessarily imply that they have interacted or worked together, despite being in the same place.

1.3.1 Mafia networks

Mafia networks refer to the major native mafia-like organizations which are the Sicilian Mafia (the original “Mafia" or Cosa Nostra) and the Calabrian ‘Ndrangheta. They are loose confederations of about one hundred groups, also called cosche or

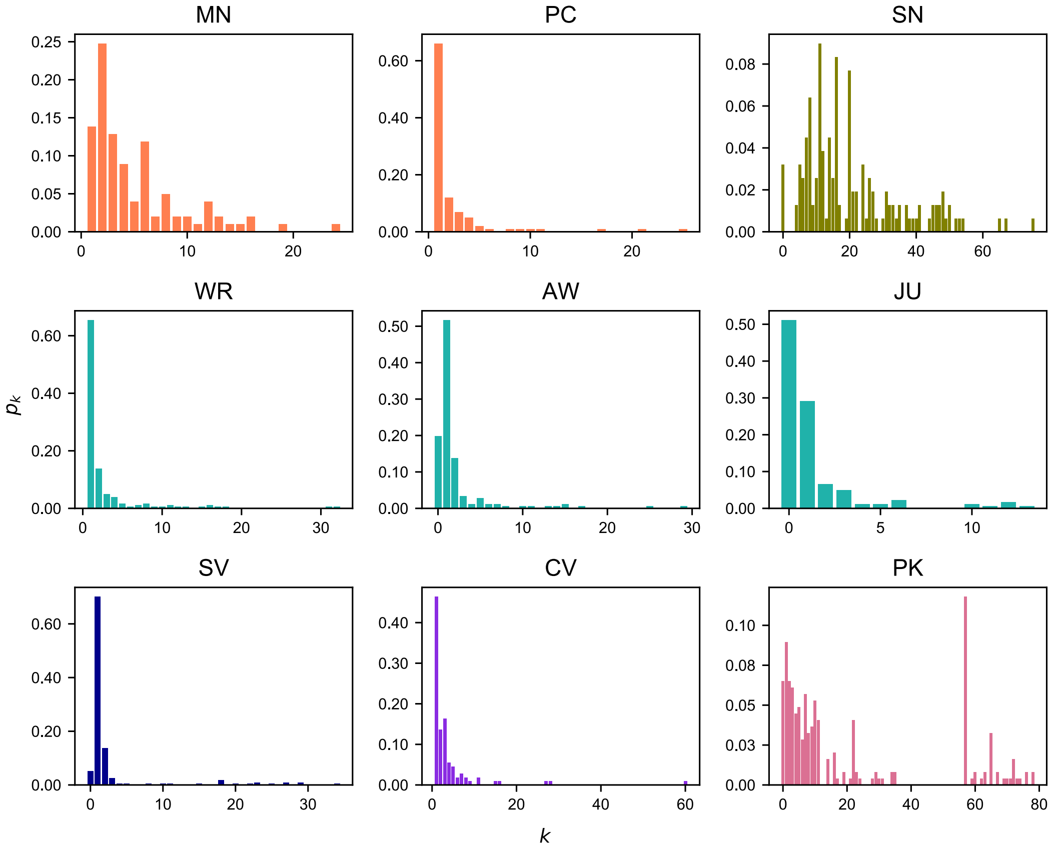

FIGURE 1.3: **Degree distributions of real-world covert networks.** The degree distribution p_k provides the probability that a randomly selected node has degree k in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW), Judgment (JU), Surveillance (SV), Caviar (CV) and Philippines Kidnappers (PK) networks. Same colors imply the networks belong to the same police investigation.

families who affect the social and economic life especially in Southern Italy since at least the 19th century (Paoli, 2004, 2008).

Mafia families have a typical structure (Ficara et al., 2021e) which is shown in Fig. 1.4. On top of the pyramid hierarchical chart is the Boss who makes all the major decisions, controls the Mafia members and resolves any disputes. Usually, the real boss keeps a low-profile hiding his real identity. Just below the boss is the Underboss who is the second in command. He can resolve disputes without involving the boss himself and replaces the boss if he is old or in danger of going to jail. In-between the boss and underboss is the role of the Consigliere who is an advisor to the boss and makes impartial decisions based upon fairness, and for the good of the Mafia. Also in-between there is the Messaggero who is a messenger who functions as liaison between criminal families. He can reduce the need for sit-downs, or meetings, of the mob hierarchy, and thus limits the public exposure of the bosses. Below the underboss is the Caporegime (also called Captain or Capo) who manages his own crew within the criminal family in a designated geographical location. A Capo's career relies heavily on how much money they can bring into the family. How many capos there are in a given family simply depends on how big that family is. Then, there are

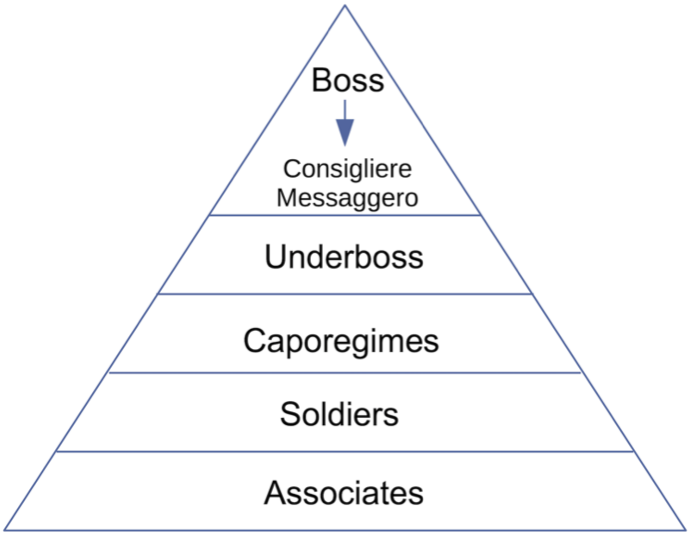

FIGURE 1.4: The structure of a Mafia family.

soldiers who report to their Caporegime. They are street level mobsters who essentially are no more than your average type criminals. Many soldiers can be assigned to one Capo. The final part of a family comes in the shape of associates, who are not actual members of the Mafia, but they work with Mafia soldiers and caporegimes on various criminal enterprises. An associate is simply someone who works with the mob, including anyone from a burglar or drug dealer to a pharmacist, entrepreneur, lawyer, investment banker, police officer or politician.

This hierarchical structure represents a peculiarity of a criminal organization as the Mafia. A custom network model could be constructed to replicate this structure starting from a scale free network (see Subsect. 1.2.3) which is the one with the most similar topology to a Mafia network, as we will explain in detail in Chap. 3.

Moreover, in Ficara et al. (2022b), we tried to create a network model for criminal network disruption using scale free networks with the same number of nodes and edges of our Montagna networks. After identifying, the key role in the hierarchy of a Mafia family or in its criminal activities, it is possible to identify this role in scale free models, and apply a disruption strategy based on the human capital (see Subsect. 5.1.1 for more details) to these models. Specifically, the human capital approach is simulated targeting nodes with the same rank of the caporegimes in our Mafia networks.

Our line of long-term research began with no information about the node role, and only one type of criminal network related to phone calls. Initially, it was natural to use graph theory. The knowledge of roles allows to study alternative approaches by combining new tools such as agent based modeling with more traditional tools like network science methods.

The Montagna Operation

The Montagna operation was one of the most important anti-mafia investigation concluded in 2007 by the Public Prosecutor's Office of Messina, and conducted by the R.O.S. (*Reparto Operativo Speciale*, or Special Operations Group, a specialized anti-mafia police unit of the Italian Carabinieri) (Calderoni et al., 2020). This operation focused in particular on two families known as Mistretta and Batanesi.

From 2003 to 2007, these families had infiltrated several economic activities including the public works in the area, through a cartel of entrepreneurs close to the Sicilian Mafia (Calderoni et al., 2020). The groups engaged in extortion racketeering, and provided illegal protection to achieve illegal profits from the public construction works, with dynamics similar to those described by Gambetta (Gambetta, 1993; Gambetta and Reuter, 1995). Furthermore, the investigation showed that the Mistretta family had taken on the role of mediator between the Mafia families of Palermo and Catania, and the other criminal organizations around Messina. Indeed both the Mistretta and Batanesi families had close connections with other families located in the province of Messina, namely Barcellona and Caltagirone. The charges were upheld by several trials, and the majority of the individuals have been sentenced to long prison terms.

Our main data source was the pre-trial detention order issued on March 14, 2007 by the preliminary investigation judge of the Court of Messina towards the end of the investigation. The order concerned a total of 52 suspects, all charged with the crime of participation in a Mafia clan (Article 416 bis of the Italian Criminal Code) as well as other crimes (*e.g.*, theft, extortion, damaging followed by arson) (Calderoni et al., 2020). According to the Italian Criminal code, the affiliation to a Mafia clan carries a penalty of between ten and fifteen years of imprisonment. The Court ordered the pre-trial detention for 38 individuals, and provided detailed motivations for the decision in a document of more than two hundred pages with an important amount of information about the suspected crimes, activities, meetings, and calls.

Most of the information from judicial documents were about the Mistretta and Batanesi families. From the analysis of legal documents we built two networks: the Meetings (MN) network, in which nodes are uniquely associated with suspected criminals and edges specify meetings among individuals, and the Phone Calls (PC) network, in which nodes are uniquely associated with suspected criminals and edges records phone calls between pairs of individuals (Ficara et al., 2020). Our dataset is publicly available on Zenodo (Cavallaro et al., 2020a).

TABLE 1.2: Properties of Montagna networks.

Parameter	**MN**	**PC**
weights	weighted	weighted
directionality	undirected	undirected
connectedness	false	false
no. of nodes n	101	100
no. of isolated nodes n_i	0	0
no. of edges e	256	124
no. of components $\|cc\|$	5	5
max avg. path length $\langle d \rangle$ for cc	3.309	3.378
max shortest path length d	7	7
density δ	0.051	0.025
avg. degree $\langle k \rangle$	5.07	2.48
max degree k	24	25
avg. clust. coeff. $\langle CC \rangle$	0.656	0.105

MN has 101 nodes and 256 edges while PC has 100 nodes and it contained only 124 edges. There were 47 individuals who jointly belonged to MN and PC. Some statistics about MN and PC are displayed in Table 1.2.

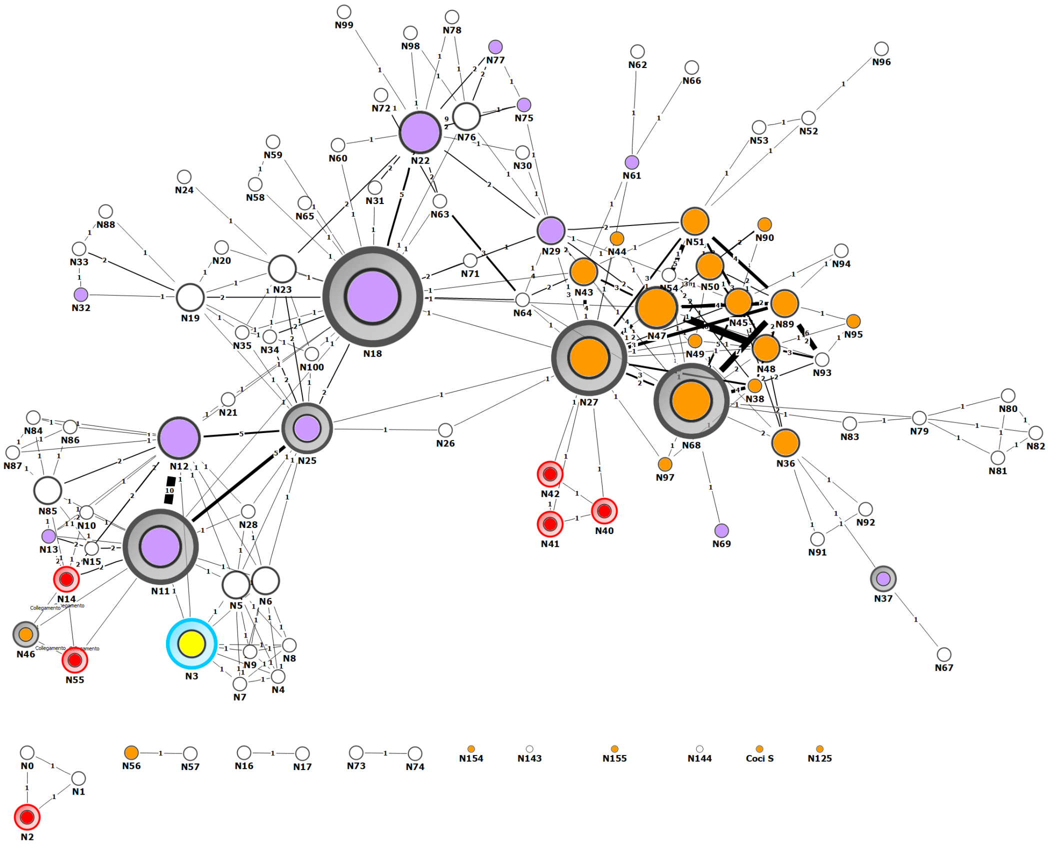

FIGURE 1.5: **The Montagna Meetings network.** The node size is proportional to the node degree, while the edge thickness is proportional to the edge weight. Members of the Mistretta and Batanesi families are respectively colored in purple and orange. Circled nodes correspond to the subjects investigated for having promoted, organized and directed the Mafia association. The red and yellow circled nodes refer to bosses of Mafia families of other districts. The white nodes represent the other subjects considered to be: (i) close to the association and (ii) not classifiable in any of the previous categories, but nevertheless useful for the purposes of the Mafia-type association and the realization of its plans.

Figs 1.5 and 1.6 graphically report MN and PC networks. In these figures, the node size is proportional to the node degree, while the edge thickness is proportional to the edge weight, *i.e.*, the total number of meetings (or telephone calls) recorded between the nodes that edge connects. Members of the Mistretta and Batanesi families are colored in purple and orange, respectively. Circled nodes correspond to the subjects investigated for having promoted, organized and directed the Mafia association. The red and yellow circled nodes refer to bosses of Mafia families of other districts. The white nodes represent the other subjects considered to be: (i) close to the association and (ii) not classifiable in any of the previous categories, but nevertheless useful for the purposes of the Mafia-type association and the realization of its plans (Calderoni et al., 2020).

Fig. 1.7 shows the edge weights distribution in the Montagna MN and PC networks (Ficara et al., 2020). Noticeably, both networks exhibit similar characteristics and include several low-weight links. A possible explanation is that the affiliates

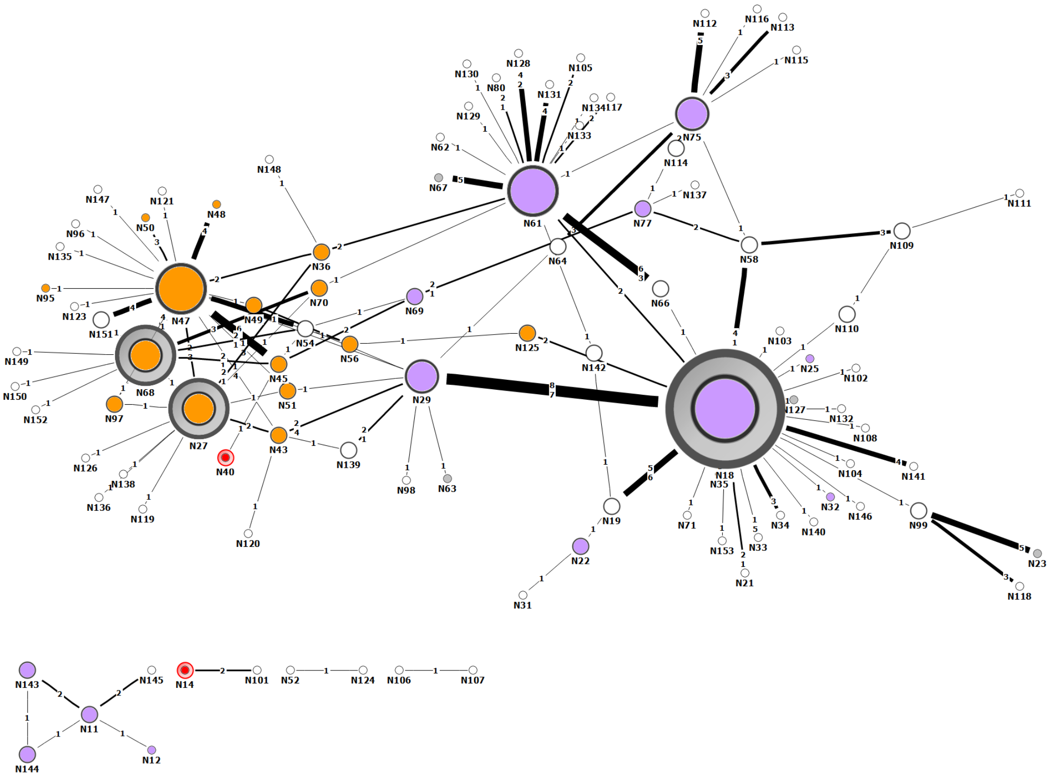

FIGURE 1.6: **The Montagna Phone Calls network.** The node size is proportional to the node degree, while the edge thickness is proportional to the edge weight. Members of the Mistretta and Batanesi families are colored in purple and orange, respectively. Circled nodes correspond to the subjects investigated for having promoted, organized and directed the Mafia association. The red and yellow circled nodes refer to bosses of Mafia families of other districts. The white nodes represent the other subjects considered to be: (i) close to the association and (ii) not classifiable in any of the previous categories, but nevertheless useful for the purposes of the Mafia-type association and the realization of its plans.

want to reduce the risk of being intercepted by LEAs, and even by other people outside the clan. In the MN network, this trend is even more accentuated since the maximum frequency in low-weight links is equal to 200, which is double with respect to that of the PC network. Moreover, the maximum weight of interactions among affiliates in the MN network (*i.e.*, $w = 10$) is greater than the one in the PC network (*i.e.*, $w = 8$). A possible explanation is that mobsters prefer to communicate by physical meetings rather than calling each other, to reduce the risk of being intercepted by the police. Mobsters will find it easier to crypt their conversations in face-by-face meetings, for instance by using body language, or generating background noise. Furthermore, bosses often have to participate to Mafia events to pursue their power inside a clan. For instance, bosses have to participate to funerals of other affiliates, and other solemn religious demonstrations (masses, processions, etc.). During those kinds of events, they also have the opportunity to pass messages to their closest subordinate affiliates. Moreover, it is harder for criminals to notice that they are going to be intercepted rather than to be eavesdropped by the police.

The histograms of shortest path length distributions of Fig. 1.8 provide useful

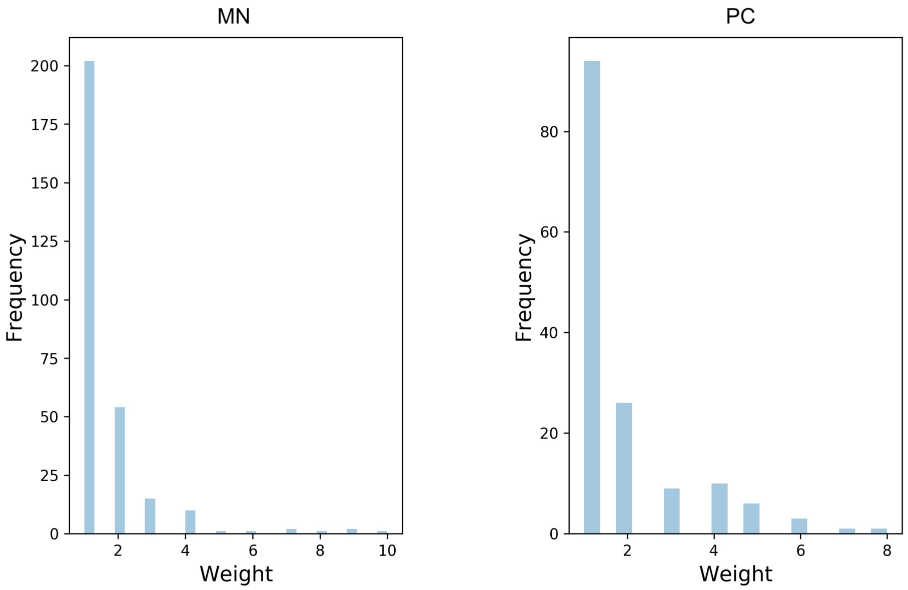

FIGURE 1.7: Weight distribution in the Montagna Meetings (MN) and Phone Calls (PC) networks.

statistical characterizations of the Montagna networks (Ficara et al., 2020). Path length statistics are closely related to dynamic properties such as velocities of network spreading processes. Usually, criminal organizations are structured in a way as to optimize the number of communications among members, and to efficiently disseminate information. These members can be discovered by following short paths of communications. Moreover, we can discover relationships among individuals belonging to distant groups in the graph because, even when two nodes seem to be distant, there may exist a relatively short path that connects them.

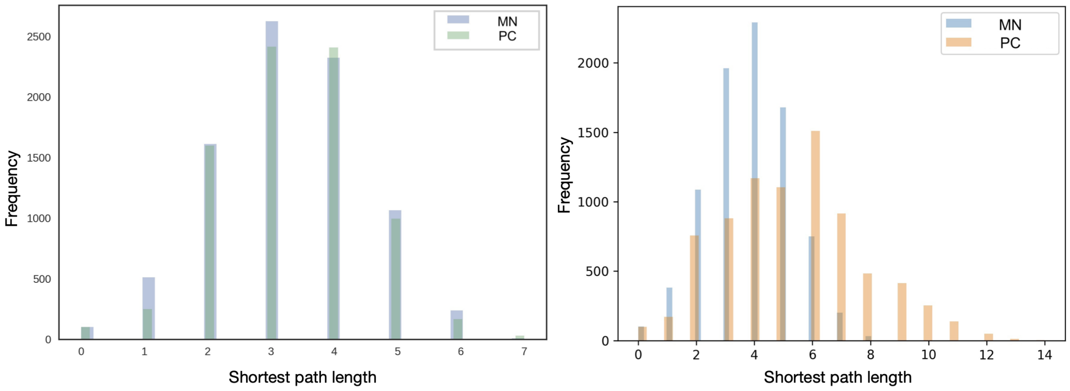

FIGURE 1.8: Shortest path length distribution in the unweighted (left column) and weighted (right column) Montagna Meetings (MN) and Phone Calls (PC) networks.

There are similarities between the weighted and the unweighted shortest path length analysis. In both scenarios, indeed, there is a higher interaction frequency among affiliates having a balanced number of intermediates. This behaviour confirms the hypothesis that inside a cosca it is better to avoid the borderline cases. On one hand, if the shortest path is composed of a lower number of affiliates, the bosses are overexpose to police investigations. On the other hand, the longest the number of intermediates, the higher the chances to be intercepted by people outside the family.

Furthermore, in the weighted simulations emerges a lower frequency of interactions in the PC network compared with the same shortest path length of the MN network. This behaviour, emerged also in Fig. 1.7, proves that the clan tries to minimize the risk of interceptions, specially to avoid exposing those mobsters who are hierarchically in a higher rank.

The availability of a real weighted graph is a valuable asset in order to conduct a more thorough network analysis. Indeed, in the unweighted scenario this behaviour is not highlighted because both networks seem to act in the same way.

The Infinito Operation

The Infinito Operation was a large law enforcement operation against 'Ndrangheta groups and Milan cosche concluded by the courts of Milan and Reggio Calabria, Italian cities situated in Northern and Southern Italy, respectively. The investigation, which started in 2003, is still in progress. On July 5, 2010, the Preliminary Investigations Judge of Milan issued a pre-trial detention order for 154 people, with charges ranging from mafia-style association to arms trafficking, extortion and intimidation for the awarding of contracts or electoral preferences.

The dataset was extracted from this judicial act, and it is available as a 2-mode matrix on the UCINET (Borgatti, Everett, and Freeman, 2002) website[1].

The Infinito Operation dataset was investigated by Calderoni and his co-authors in several works (Calderoni, 2014, 2015; Calderoni, Brunetto, and Piccardi, 2017; Calderoni and Piccardi, 2014; Grassi et al., 2019).

From the original 2-mode matrix, we constructed the weighted and undirected graph Infinito Summits Network (SN) with 156 nodes and 1619 edges (Ficara et al., 2021c,d). Nodes are suspected members of the 'Ndrangheta criminal organization. Edges are summits (*i.e.*, meetings whose purpose is to make important decisions and/or affiliations, but also to solve internal problems, and to establish roles and powers) taking place between 2007 and 2009. This network describes how many summits any two suspects may have in common. Attendance at summits was registered by police authorities through wiretapping and observations during this operation.

Some statistics about SN are displayed in Table 1.3.

The Oversize Operation

The Oversize Operation is an investigation lasting from 2000 to 2006, which targeted more than 50 suspects of the Calabrian 'Ndrangheta involved in international drug trafficking, homicides, and robberies.

The trial led to the conviction of the main suspects from 5 to 22 years of imprisonment between 2007-2009. Berlusconi et al. (2016) studied three unweighted and undirected networks extracted from three judicial documents corresponding to

[1] Available at: https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/ndranghetamafia2

TABLE 1.3: Properties of Infinito and Oversize networks.

Parameter	**SN**	**WR**	**AW**	**JU**
weights	weighted	unweighted	unweighted	unweighted
directionality	undirected	undirected	undirected	undirected
connectedness	false	false	false	false
no. of nodes n	156	182	182	182
no. of isolated nodes n_i	5	0	36	93
no. of edges e	1619	247	189	113
no. of components $\|cc\|$	6	3	38	96
max avg. path length $\langle d \rangle$ for cc	2.361	3.999	4.426	3.722
max shortest path length d	5	8	9	7
density δ	0.134	0.015	0.011	0.007
avg. degree $\langle k \rangle$	20.76	2.71	2.08	1.24
max degree k	75	32	29	13
avg. clust. coeff. $\langle CC \rangle$	0.795	0.149	0.122	0.059

three different stages of the criminal proceedings (see Table 1.1): wiretap records (WR), arrest warrant (AW), and judgment (JU).

Each of these networks has 182 nodes corresponding to the individuals involved in illicit activities (Ficara et al., 2021c,d). The WR network has 247 edges which represent the wiretap conversations transcribed by the police and considered relevant at first glance. The AW network contains 189 edges which are meetings emerging from the physical surveillance. The JU network has 113 edges which are wiretap conversations emerging from the trial and several other sources of evidence, including wiretapping and audio surveillance. These datasets are available as three 1-mode matrices on Figshare (Piccardi et al., 2016).

Some statistics about WR, AW and JU are displayed in Table 1.3.

1.3.2 Street gang and terrorist networks

Street gang networks refer to another form of criminal organization which is generally defined as street-oriented groups, whose membership is youthful, that exhibit persistence across time, and for whom illegal activity constitutes a part of group identity (Klein and Maxson, 2006). As noted by Morselli (2008), an association of criminals is not the same as a criminal association, and gangs more commonly represent the former.

Curry (2011) examined the relationships between gangs and terrorist groups finding a number of similarities but also substantial differences. Both groups are composed by male members, and are characterized by violence, solidarity, and elements of collective behavior. The violence used by both groups often represents a form of "self-help," or attempts to redress wrongs. The differences included a profit motive for gangs that is largely absent for terrorist groups, cross-national connections maintained by terrorist groups, the diversity in different types of crime that typifies gang crime, and an ideological belief among members of terrorist groups that is not present among gang members. Most of the similarities between the groups reflect the fact that terrorist groups are less structured than is publicly believed (Decker and Pyrooz, 2011).

To compare with Mafia networks, two street gang networks related to Stockholm and Montreal criminal groups, and one terrorist network related to Philippine kidnappers have been analyzed. Some statistics about them are displayed in Table 1.4.

TABLE 1.4: Properties of street gang and terrorist networks.

Parameter	**SV**	**CV**	**PK**
weights	weighted	weighted	weighted
directionality	undirected	undirected	undirected
connectedness	false	true	false
no. of nodes n	234	110	246
no. of isolated nodes n_i	12	0	16
no. of edges e	315	205	2571
no. of components cc	13	1	26
max avg. path length $\langle d \rangle$ for cc	3.534	2.655	3.034
max shortest path length d	6	5	9
density δ	0.012	0.034	0.085
avg. degree $\langle k \rangle$	2.69	3.73	20.9
max degree k	34	60	78
avg. clust. coeff. $\langle CC \rangle$	0.15	0.335	0.753

Stockholm street gangs

The Stockholm street gangs dataset was extracted from the National Swedish Police Intelligence, which collects and registers the information from different kinds of intelligence sources to identify gang membership in Sweden.

The organization investigated here is a Stockholm-based street gang localized in southern parts of Stockholm County, consisting of marginalized suburbs of the capital. All gang members are male with high levels of violence, thefts, robbery, and drug-related crimes.

Rostami and Mondani (2015b) constructed the Surveillance (SV) network (Table 1.4). It contains data from the General Surveillance Register which covers the period 1995–2010, and aims to facilitate access to the personal information revealed in law enforcement activities needed in police operations.

SV is a weighted network with 234 nodes that are gang members (Ficara et al., 2021c). Some of them were no longer part of the gang in the period covered by the data, and have been included as isolated nodes. The link weight counts the number of occurrence of a given edge. This dataset is available on Figshare (Rostami and Mondani, 2015a).

Caviar Project

Project Caviar (Morselli, 2008) was a unique investigation against hashish and cocaine importers operating out of Montreal (Canada).

The drug traffickers were targeted between 1994 and 1996 by a tandem investigation uniting the Montreal Police, the Royal Canadian Mounted Police, and other national and regional LEAs from England, Spain, Italy, Brazil, Paraguay, and Colombia. In a 2-year period, 11 imported drug consignments were seized at different moments and arrests only took place at the end of the investigation.

The principal data sources was the transcripts of electronically intercepted telephone conversations between suspects submitted as evidence during the trials of 22 individuals. Initially, 318 individuals were extracted because of their appearance in the surveillance data. From this pool, 208 individuals were not implicated in the trafficking operations. Most were simply named during the many transcripts of conversations, but never detected. Others, who were detected, had no clear participatory role within the network (*e.g.*, family members or legitimate entrepreneurs).

The final Caviar (CV) network is composed of 110 nodes. The 1-mode matrix with weighted and directed edges is available on the UCINET (Borgatti, Everett, and Freeman, 2002) website[2].

From this matrix, we extracted an undirected and weighted network (Ficara et al., 2021c) with 110 nodes which are criminals and 205 edges which represent the communications exchanges between them (see Table 1.4). Weights are level of communication activity.

Philippines Kidnappers

Philippines Kidnappers data refer to the Abu Sayyaf Group (ASG) (Gerdes, Ringler, and Autin, 2014), a violent non-state actor operating in the Southern Philippines. In particular, this dataset is related to the Salast movement that has been founded by Aburajak Janjalani, a native terrorist of the Southern Philippines in 1991. ASG is active in kidnapping and other kinds of terrorist attacks.

The reconstructed 2-mode matrix is available on the UCINET (Borgatti, Everett, and Freeman, 2002) website[3].

From the 2-mode matrix, we constructed a weighted and undirected graph (Ficara et al., 2021c) called Philippines Kidnappers (PK) (see Table 1.4). The PK network has 246 nodes and 2571 edges. Nodes are terrorist kidnappers of the ASG. Edges are the terrorist events they have attended. This network describes how many events any two kidnappers have in common.

[2] Available at: `https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/caviar`

[3] Available at: `https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/philippinekidnappings`

Chapter 2

Leader identification

To identify leaders within a criminal network, a family of measures must be used to discover the most important actors in a social network (Wasserman and Faust, 1994).

The family of centrality measures is probably the most widely applied set of SNA tools in practical contexts.

Centrality (Ficara et al., 2021b) is an intrinsically relational concept because, to be central, an actor needs to have relations. An actor might be important because he is connected to a large number of different nodes or because he is connected to other important nodes. An actor can also be considered important because his absence would result in a loosely connected social network made of many isolated components. Centrality is also often described in terms of the power that an actor could receive from it (*e.g.*, an actor strategically located within a network will have a high control over the information flowing through the network) (Ficara et al., 2021e).

Traditionally, centrality has typically been studied for graphs of relatively small size. However, in the last few years, the proliferation of digital collection of data has led to huge graphs with billions of nodes and edges. There is a clear need to develop more efficient, scalable, and accurate algorithms (Kang et al., 2011).

Degree centrality, closeness centrality, betweenness centrality and clustering coefficient can be considered as the most frequently used centrality metrics to compute node centrality. The first three measures were proposed by Freeman (1978), whereas the clustering coefficient was defined by Watts and Strogatz (1998).

Degree centrality can be efficiently measured for large networks. Nevertheless, it captures the local information of a node giving limited information. On the other hand, betweenness and closeness centralities are prohibitively expensive to compute, and thus impractical for large networks. Over the years, however, parallel implementations of betweenness and closeness have been developed (Bader and Madduri, 2006; Jamour, Skiadopoulos, and Kalnis, 2018; Madduri et al., 2009; McLaughlin and Bader, 2018; Regunta et al., 2021). As we have already mentioned at the beginning of Chap. 1, covert networks are usually composed of a small number of actors, and therefore these measures are not computationally intensive on such kinds of networks, but they become so on large graphs. Nevertheless, the problem of finding computationally-light alternatives to the standard centrality measures is interesting in itself.

Despite an abundance of methods for measuring centrality of individual nodes, there are by now only a few metrics to measure centrality of individual edges (*e.g.* edge betweenness centrality). De Meo et al. (2012, 2013, 2014) presented a novel measure called K-path to compute link centrality. The advantage of using this metric is that it can be computed with a near-linear time algorithm called Weighted Edge Random Walks – K Path or WERW-Kpath. More recently, Mocanu, Exarchakos, and Liotta (2018) developed an algorithm called Game of Thieves which is able to compute actor and link centrality in a polylogarithmic time.

An often asked, but rarely answered, question is: are these centrality measures correlated (Valente et al., 2008)? If there exists a high correlation between the centrality metrics, they will have a similar behavior in statistical analyses. For this reason, there is the possibility of approximating the metric with the highest computational complexity using the other. If there is not high correlation, these measures are unique and they can be associated with different outcomes.

Game of Thieves and WERW-Kpath have been tested on Mafia networks to know if they were capable of identifying leaders as well as the more traditional measures. Moreover, these networks perfectly reproduce the characteristics of larger networks. Mafia networks are in fact a good example of real-world networks with respect to the geometry of connections. Indeed, these connections are the building blocks of the entire Mafia, and more generally of organized crime (Mastrobuoni and Patacchini, 2012).

2.1 Standard centrality measures

To find an important node or edge in a graph, and therefore an influential person or connection in a criminal network (Ficara et al., 2021d), several centrality measures can be used: degree centrality, closeness centrality, node/edge betweenness centrality, clustering coefficient eigenvector centrality, PageRank centrality, and Katz centrality.

Degree Centrality. Degree Centrality (DC) determines the importance of a node based on the number of edges incident upon it (Freeman, 1978). It is defined as:

$$DC_i = \frac{k_i}{n-1}, \tag{2.1}$$

where k_i is the degree of i (see Eqs. 1.4 and 1.5) and n is the network size.

Node Betweenness Centrality. Betweenness Centrality (BC) quantifies how many times a node acts as a bridge along the shortest path between two other nodes (Brandes, 2008). It is defined as the sum of the fraction of all-pairs shortest paths that pass through a node i:

$$BC_i = \sum_{j,x \in N} \frac{\sigma(j,x|i)}{\sigma(j,x)}, \tag{2.2}$$

where N is the set of nodes, $\sigma(j,x)$ is the number of shortest $\sigma(j,x)$-paths, and $\sigma(j,x|i)$ is the number of those paths passing through some node i other than j,x.

Edge Betweenness Centrality. Edge Betweenness Centrality (EBC) quantifies how many times an edge acts as a bridge along the shortest path between two other nodes (Brandes, 2008). It is defined as the sum of the fraction of all-pairs shortest paths that pass through a link l:

$$EBC_l = \sum_{i,j \in N} \frac{\sigma(i,j|l)}{\sigma(i,j)}, \tag{2.3}$$

where N is the set of nodes, $\sigma(i,j)$ is the number of shortest $\sigma(i,j)$-paths, and $\sigma(i,j|l)$ is the number of those paths passing through the link l.

Closeness Centrality. Closeness Centrality (CL) determines the importance of a node based on the proximity of that node to all the other nodes in the graph (Freeman, 1978). It is defined as:

$$CL_i = \frac{n-1}{\sum\limits_j d_{j,i}}, \tag{2.4}$$

where $d_{j,i}$ is the shortest-path distance between j and i, and n is the network size.

Clustering Coefficient. Clustering Coefficient (CC) indicates how well connected the neighborhood of a node is (Watts and Strogatz, 1998). It is defined as:

$$CC_i = \frac{2T_i}{k_i(d_i - 1)}, \tag{2.5}$$

where T_i is the number of triangles through node i and k_i is the degree of i. If the neighborhood is fully connected, the CC is 1. It is 0 instead if there are hardly any connections in the neighborhood.

Eigenvector Centrality. Eigenvector Centrality (EC) computes the centrality for a node based on the centrality of its neighbors (Bonacich, 1987). Given a graph G, the EC for a node i is defined as:

$$EC_i = \frac{1}{\lambda} \sum_{j \in \mathcal{N}(i)} EC_j = \frac{1}{\lambda} \sum_{j \in N} a_{i,j} EC_j, \tag{2.6}$$

where $\mathcal{N}(i)$ is the set of neighbors of the node i, N is the set of nodes in G, λ is a constant and $A = (a_{i,j})$ is the adjacency matrix. It can be rewritten as the eigenvector notations as:

$$A\,EC = \lambda\,EC. \tag{2.7}$$

There will be different eigenvalues λ for which a non-zero eigenvector solution exists, and only the greatest one will result in the eigenvector centrality measure.

Two variants of the EC are Google's PageRank and the Katz centrality.

PageRank Centrality. PageRank (PR) Centrality is used by Google to assess the importance of a web page (Page et al., 1999). It expresses the likelihood that a user randomly clicking on a hyperlink will arrive at that particular page. Given a directed graph and its adjacency matrix $A = (a_{i,j})$, the PR_i of node i is given by:

$$PR_i = \alpha \sum_j \frac{a_{j,i}}{k_j} PR_j + \beta, \tag{2.8}$$

where α and β are constants and k_j is the out-degree of node j if such degree is positive, or $k_j = 1$ if the out-degree of j is null. In matrix form we have:

$$PR = \alpha\, PR\, K^{-1} A + \beta, \tag{2.9}$$

where β is now a vector whose elements are all equal a given positive constant and K^{-1} is a diagonal matrix with i-th diagonal element equal to $1/k_i$.

Katz Centrality. Katz Centrality (KC) computes the relative influence of a node, measuring the number of node's immediate neighbors (first degree nodes) and also all the other nodes in the network that connect to the node itself through these immediate neighbors (Katz, 1953). For a node i, this is defined as:

$$\mathrm{KC_i} = \alpha \sum_{j \in N} a_{ij}\mathrm{KC_j} + \beta\,, \tag{2.10}$$

where α and β are positive constants, $A = (a_{ij})$ is the adjacency matrix of the graph, whose eigenvalues are denoted by λ_i, $i = 1, \ldots, n$. The parameter β controls the initial centrality, while the parameter α satisfies the inequality:

$$\alpha < \frac{1}{\max\{\lambda_i : 1 \leq i \leq n\}}\,. \tag{2.11}$$

2.2 Nonstandard centrality measures

Game of Thieves. A more recent centrality measure is called Game of Thieves (GoT) (Mocanu, Exarchakos, and Liotta, 2018). It computes the importance of all elements in a network (*i*.e., nodes and edges), compared to the total number of nodes.

The game proceeds in epochs. When it begins, each node has a certain number of virtual diamonds or vdiamonds and wandering thieves, who are the leading actors in the game. If a thief carry a vdiamond, his state is "empty". If a thief does not carry a vdiamond, his state is "loaded".

In order to understand how this measure works, we have to define some notation. Given a graph $G(N, E)$,

- Φ_0^i is the initial number of vdiamonds in node $i \in N$ at time $T = 0$;
- Φ_T^i indicates the number of vdiamonds in node $i \in N$ at time T (*i.e.*, after GoT has run for T epochs);
- Ψ_T^l is the number of "loaded" thieves passing through an edge $l \in E$ at time T;
- Γ_i is the set of vertices connected by an edge with node $i, \forall i \in N$;
- $\Omega_{ij} \geq 0$ is the weight of the edge which connects the node $i \in N$ and $j \in N$;
- Υ_t is a dynamic list which contains the vertices visited by a thief t, useful to keep the path of t in his search for vdiamonds.

If the state of a thief t is "empty", the following operations will be sequentially performed in any epoch ep:

Step 1 a randomly picks a node $j \in \Gamma_i$, where i is its actual location, with a probability $p_{ij} = \frac{\Omega_{ji}}{\sum\limits_{i \in \Gamma_i} \Omega_{ij}}$.

Step 2 t moves from his home node i to node j.

Step 3 If $j \in \Upsilon_t$, then all the vertices after j in Υ_t are removed from the list.

Step 4 If $j \notin \Upsilon_t$, then j is added to the end of Υ_t.

Step 5 If $\Phi^j_{ep} > 0$, then t takes one vdiamond and changes his state to "loaded".

Step 6 Φ^j_{ep} decreases by one vdiamond.

If the state of a thief t is "loaded", the following steps will be sequentially performed in any epoch ep:

Step 1 t moves from the last node i from Υ_t, which is his actual location, to the last but one node j from Υ_t.

Step 2 i is removed from Υ_t.

Step 3 Ψ^l_{ep} increases by one (*i.e.*, edge l from i to j increases).

Step 4 If j is the home node of t, t unloads the vdiamond, and sets his state to "empty".

Step 5 Φ^j_{ep} increases by one vdiamond.

The game runs for a duration of T epochs. The number of epochs to stop the algorithm is conventionally $T = \log^3 |N|$.

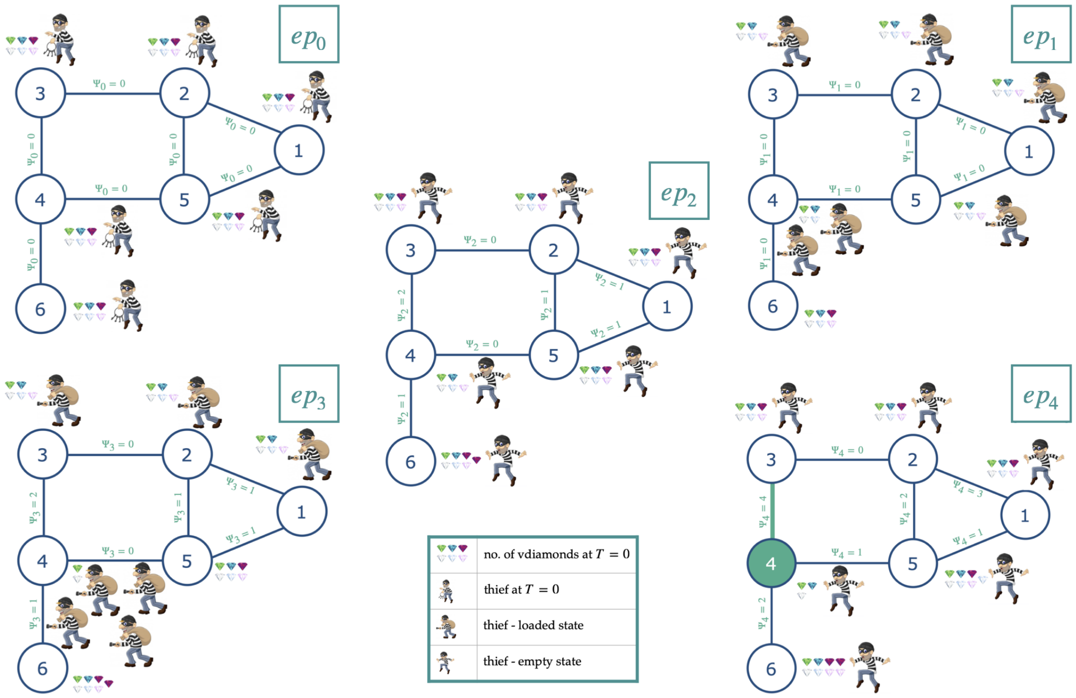

FIGURE 2.1: **Game of Thieves (GoT) illustration.** GoT behavior over epochs on a simple unweighted and undirected network with six nodes. The number of thieves is initially set to one per node. The number of vdiamonds on each node is initially equal to the number of nodes (*i.e.*, 6). The game runs for $T = \log^3 6 \simeq 5$. Ψ_T shows the number of thieves passing through each edge after T epochs. At each epoch, all thieves jump from their current location to the next one, changing state (*i.e.*, empty or loaded) when they find or deposit a new vdiamond. In the final epoch, the most important node (*i.e.*, the one with the highest number of stolen vdiamonds) and edge (*i.e.*, the one crossed by the greatest number of thieves) are marked in green.

When the game has run for a duration of T epochs, the centrality of a node i is computed as the average number of vdiamonds present on i:

$$\Phi^i_T = \frac{1}{T} \sum_{ep=0}^{T} \Phi^i_{ep} \,. \tag{2.12}$$

This measure refers to the average number of vdiamonds present on each node, after the game has run for a duration of T epochs. An important node i is indicated by a small Φ^i_T value because a lot of thieves visit the most central nodes which will are quickly depleted.

The centrality of each edge l is computed as the average number of thieves who carry a vdiamond passing through l:

$$\Psi^l_T = \frac{1}{T} \sum_{ep=0}^{T} \Psi^l_{ep} \,. \tag{2.13}$$

This measure refers to the average number of thieves who carry a vdiamond passing through an edge l after T epochs. The most important edges are indicated by a high Ψ^l_T value.

Fig. 2.1 shows GoT behavior over epochs in a graph G composed by 6 nodes and 7 edges. When the game begins, each node has a number of vdiamonds equal to the number of nodes in G and one thief. At each epoch ep, a thief located on a node i randomly picks a neighbor of i. He moves to this new node and, if he finds a vdiamond, he fetches it. Then, he brings the vdiamond back to his home node. At this point the vdiamond becomes available for the other thieves who can steal it. After T epochs, node and edge centrality are computed according to Eqs 2.12 and 2.13.

Weighted Edge Random Walks – K Path. A novel measure of edge centrality for social networks is the K-path edge centrality which is defined as:

$$L^k(l) = \sum_i \frac{\sigma^k_i(l)}{\sigma^k_i} \,, \tag{2.14}$$

where $\sigma^k_i(l)$ is the number of k-paths originating from i and traversing the edge l and σ^k_i is the number of k-paths originating from i.

A near linear time algorithm called Weighted Edge Random Walks – K Path or WERW-Kpath (WKP) (De Meo et al., 2012, 2013, 2014) is able to compute this centrality index.

It consists of three main steps:

Step 1 Node and edge weights assignment.

Step 2 Simulation of message propagations through random simple random walks of fixed length up to k.

Step 3 Final weight computation.

In the first stage of the algorithm, weights are assigned to both nodes and edges. Nodes weight is used to select the source node from which each message propagation simulation starts. Edges weight is the initial value of the edge centrality and it is updated during the execution of the algorithm. Then, the idea of message propagation is simulated in the graph using random walkers forced to make simple paths of bounded length up to a constant and user-defined value k without passing no more than once through the same edge. The reasonable values range for the length of the k-path random walks can be found in the interval $[5, 20]$. An edge is central if it is frequently exploited to diffuse information.

Its is computationally efficient since its cost is near linear with respect to the number of edges in the network.

TABLE 2.1: **Computational complexity of standard and nonstandard centrality measures.** n is the cardinality of N, and e is the cardinality of E in a graph $G(N, E)$.

Measure	Centrality	Computational Complexity
DC	Nodes	$O(e)$
BC	Nodes	$O(en)$ or $O(n^3)$
EBC	Edges	$O(en)$ or $O(n^3)$
CL	Nodes	$O(n^3)$
CC	Nodes	$O(n^2)$
GoT	Nodes and Edges	$O(log^2 n)$ or $O(log^3 n)$
WKP	Edges	$O(ke)$

Table 2.1 shows how GoT represents a great step forward in terms of computational complexity with respect to classical algorithms of node centrality such us BC, CL and CC which have at least a quadratic time complexity. The DC has a linear time complexity, as well as the WKP, but GoT still remains a better option because it is able to compute the centrality of both nodes and edges.

2.3 Correlation analysis

Correlation is a bivariate analysis used to study the degree of association between two variables, taking into account the strength of this relationship and its direction.

A correlation coefficient is a measure of a specific type of correlation, which studies the degree of association between two variables.

The most used types of correlations are Pearson linear correlation, Spearman and Kendall rank correlations.

Pearson correlation. Given a pair of random variables a and b, the Pearson's r correlation coefficient (Chen and Popovich, 2002) is defined as the covariance of the two variables divided by the product of their standard deviations:

$$r = \frac{cov(a, b)}{\sigma_a \sigma_b} \,. \tag{2.15}$$

Spearman correlation. The Spearman's ρ rank correlation coefficient (Spearman, 1904) between two variables is defined as the Pearson's r between the rank values of those two variables. For a sample of size s, the s raw scores a and b are converted to ranks rg_a and rg_b, and ρ is computed as:

$$\rho = \frac{cov(rg_a, rg_b)}{\sigma_{rg_a} \sigma_{rg_b}} \,, \tag{2.16}$$

where $cov(rg_a, rg_b)$ is the covariance of the rank variables and $\sigma_{rg_a}\sigma_{rg_b}$ are the standard deviations of the rank variables.

Kendall correlation. Given two samples a and b, where each sample size is s, Kendall's τ rank correlation coefficient (Kendall and Gibbons, 1990) is defined according to the following formula:

$$\tau = \frac{s_c - s_d}{\frac{1}{2}s(s-1)}, \tag{2.17}$$

where s_c is number of concordant pairs, s_d is number of discordant pairs and $\frac{1}{2}s(s-1)$ is the total number of pairings with a and b.

A correlation coefficient can assume any value in the interval between $+1$ and -1, including the end values $+1$ or -1 and to interpret it, we have to adopt the following rules (Ratner, 2009):

- Values equal to 0 indicate no relationship;
- Values equal to $+1$ (or -1) indicate a perfect positive (or negative) relationship;
- Values between 0 and 0.3 (or -0.3) indicate a weak positive (or negative) relationship;
- Values between 0.3 and 0.7 (or -0.3 and -0.7) indicate a moderate positive (or negative) relationship;
- Values between 0.7 and 1 (or -0.7 and -1) indicate a strong positive (or negative) relationship.

2.3.1 The impact of real and artificial network size on correlation coefficients

In Ficara et al. (2021b), we investigated the correlations among some of the traditional node centrality measures introduced in Sect. 2.1, that are DC, BC, CL and CC, and GoT described in Sect. 2.2, on network models and real world networks.

The network models (see Sect. 1.2) include SF, SW and ER random networks. For each class, we randomly generated five unweighted networks. Each network had between $1,000$ and $15,000$ nodes and between $4,970$ and $1,125,545$ edges.

For ER networks, we chose the number of nodes n between $1,000$ and $15,000$, and a probability for edge creation $p = 0.01$.

For SW networks, we built NWS models choosing the number of nodes n between $1,000$ and $15,000$, $k = 6$ neighbors with which connect each node i in the ring topology, and a probability $p = 0.6$ of rewiring each edge.

For SF networks, we built BA models choosing the number of nodes n between $1,000$ and $15,000$, we added 5 random edges for each new node i, and we chose a probability $p = 0.3$ of adding a triangle after we added each of these random edges.

The real world networks include three networks from different domains: the Dolphins social network (see Fig. 2.2-(a)), the High Energy theory collaborations network (see Fig. 2.2-(b)) and the Internet network (see Fig. 2.2-(c)).

The Dolphins social network is an undirected and unweighted network of the relationships between the bottlenose dolphins (genus Tursiops) living in a community in New Zealand (Lusseau et al., 2003). The dolphins have been observed between

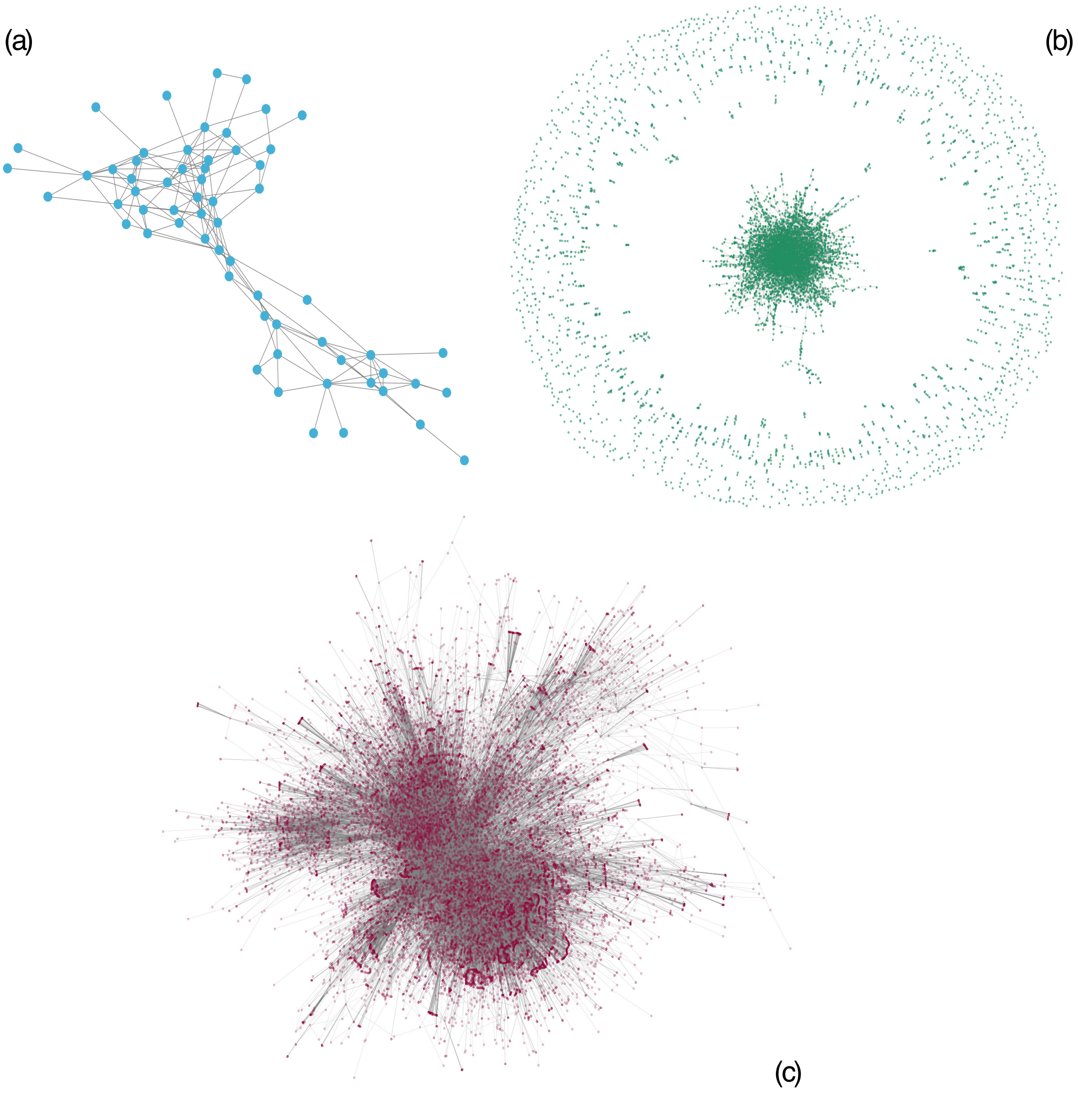

FIGURE 2.2: **Real-world networks.** Dolphins social network (a), High Energy theory collaborations network (b) and Internet network (c).

1994 and 2001. This network is composed of 62 vertices which are the bottlenose dolphins and 159 edges which are the frequent associations.

The High Energy theory collaborations is an undirected and weighted network of co-authorships between scientists who posted preprints on the High-Energy Theory E-Print Archive between January 1, 1995 and December 31, 1999 (Newman, 2001). This network is composed of 8,361 vertices which are scientists and 15,751 edges which are connections existing if the scientists have authored a paper together.

The Internet network was created by Mark Newman from data for July 22, 2006 and is not previously published. It was reconstructed from Border Gateway Protocol tables posted by the University of Oregon Route Views Project. This network is a snapshot of the structure of the Internet at the level of autonomous systems (AS), *i*.e., collections of connected IP routing prefixes controlled by independent network operators. It is an undirected and unweighted network in which the vertices are 22,963 AS and the edges are 48,436 connections between AS.

For the implementation of the traditional measures, we used Python and NetworkX library (Hagberg, Schult, and Swart, 2008). For GoT we used the implementation by Mocanu, Exarchakos, and Liotta (2018)[1], setting 1 thief and $\Phi_0^i = n$ vdiamonds per node, with n being the network size. We let GoT to run for $T = \log^3 n$ epochs. NetworkX was also used to generate the network models and to perform our experiments with the real-world networks.

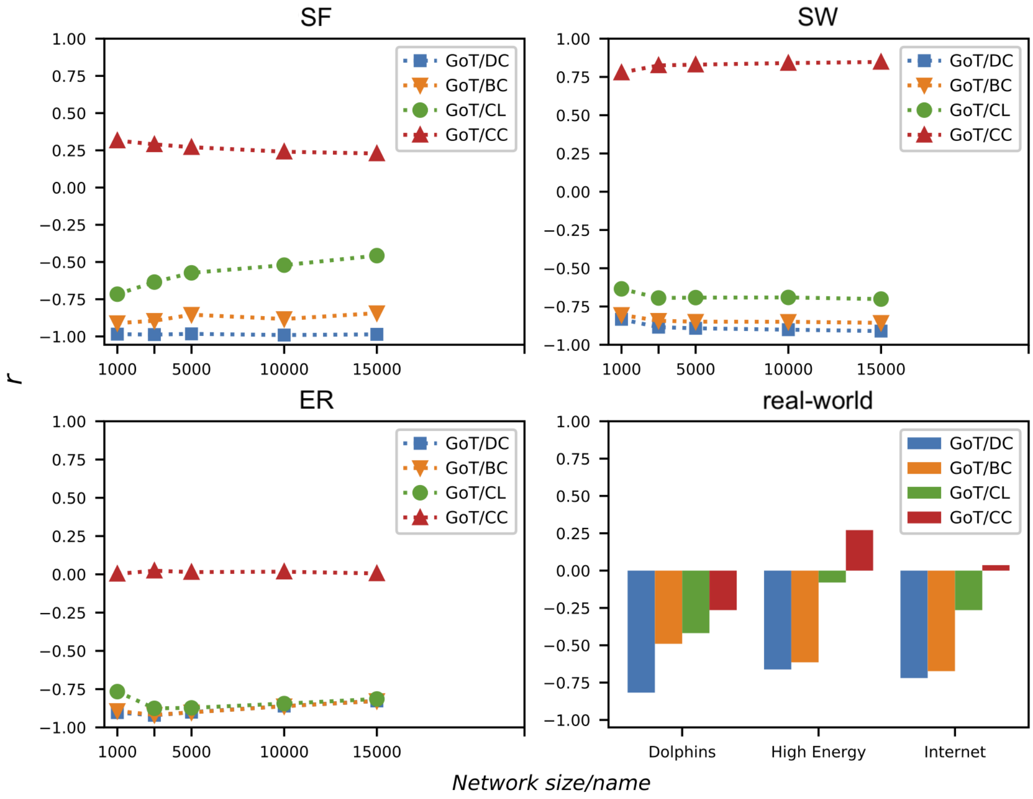

FIGURE 2.3: **Pearson correlation coefficient among Game of Thieves (GoT) and other centrality measures in real and artificial networks of different sizes.** Pearson's r between GoT and Degree Centrality (DC), GoT and Betweenness Centrality (BC), GoT and Closeness (CL) Centrality, GoT and Clustering Coefficient (CC) is represented as a function of the network size in scale-free (SF), small-world (SW), Erdos–Rényi (ER) networks and as a bar chart for real networks.

The results of the Pearson correlation coefficient r are presented in Fig. 2.3, the Spearman rank correlation coefficient ρ in Fig. 2.4 and the Kendall rank correlation coefficient τ in Fig. 2.5, with the growth of networks' sizes. Small deviations of rank correlation coefficients can be observed when the size of the networks is rather small. However, when networks grow big enough, the deviations are not visible anymore, especially for the rank correlation coefficients. Spearman correlation coefficient ρ was much higher than Pearson correlation coefficient r, and therefore more capable of capturing the underlying ranking correlation between GoT and the other measures. Moreover, we can observe that ρ is always larger than τ, but there is no distribution difference between these two coefficients.

[1] Available on GitHub (github.com/dcmocanu/centrality-metrics-complex-networks)

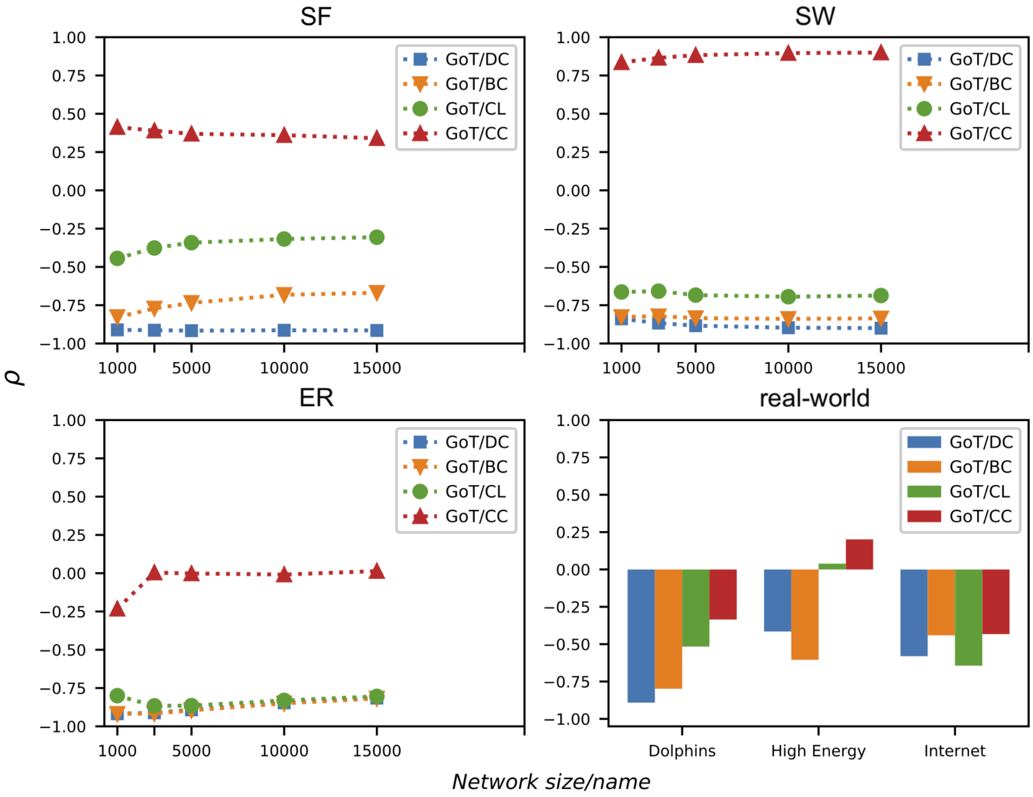

FIGURE 2.4: **Spearman rank correlation coefficient among Game of Thieves (GoT) and other centrality measures in real and artificial networks of different sizes.** Spearman's ρ between GoT and Degree Centrality (DC), GoT and Betweenness Centrality (BC), GoT and Closeness (CL) Centrality, GoT and Clustering Coefficient (CC) is represented as a function of the network size in scale-free (SF), small-world (SW), Erdos–Rényi (ER) networks and as a bar chart for real networks.

GoT and DC have the strongest negative correlation. GoT and BC also exhibit a large negative correlation. GoT and CL are negative correlated, but this correlation is less than that between GoT and both DC and BC. GoT and CC centrality have no correlation in most cases. In ER networks, we can observe the strongest and almost identical negative correlation among GoT and DC, BC and CL. In SW networks, a very strong and unique positive correlation between GoT and the CC can be observed. Real networks are more complex than the artificial ones, but also in this case the correlation among GoT and DC is confirmed to be the strongest one.

2.3.2 The impact of artificial network density on correlation coefficients

In Ficara et al. (2021a), we investigated the correlations between GoT and the standard node centrality measures (*i.e.*, DC, BC, CL and CC) on three types of network models (*i.e.*, SF, SW and ER). We also used GoT to compute edge centrality comparing it with the WKP.

This time we considered the increase of the number of links with a fixed network size. For each class of networks, we randomly generated undirected and unweighted networks with 10, 000 nodes and between 5, 000 and 50, 000 edges.

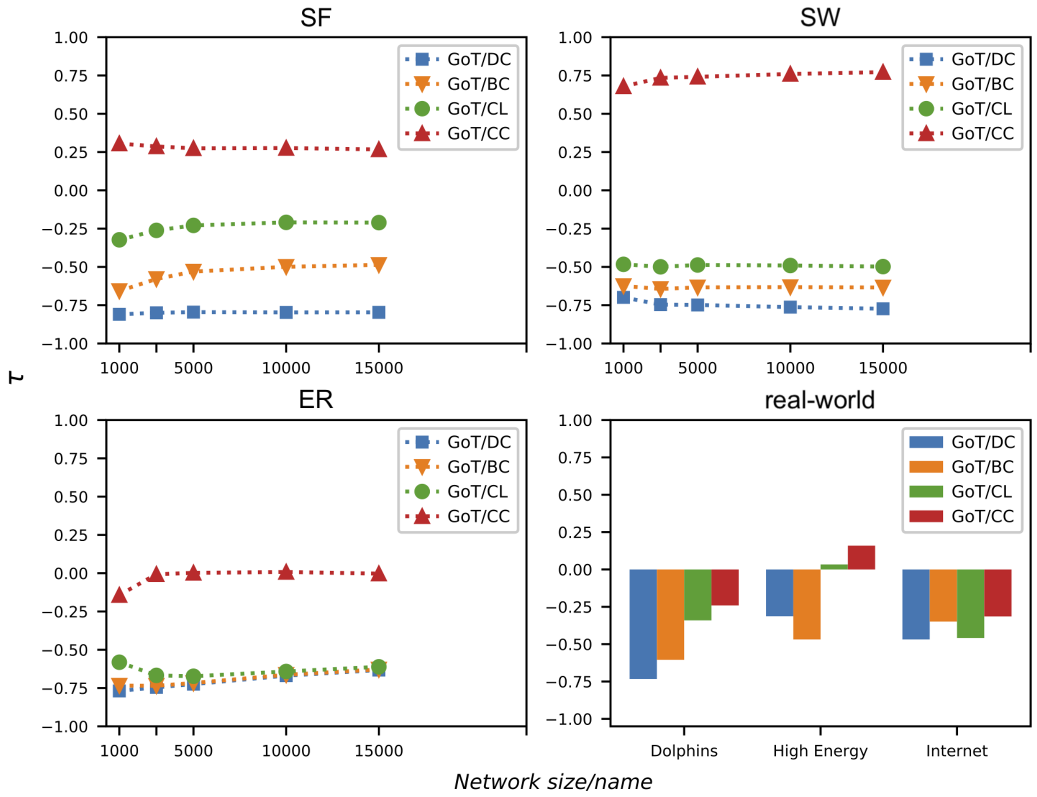

FIGURE 2.5: **Kendall rank correlation coefficient among Game of Thieves (GoT) and other centrality measures in real and artificial networks of different sizes.** Kendall's τ between GoT and Degree Centrality (DC), GoT and Betweenness Centrality (BC), GoT and Closeness (CL) Centrality, GoT and Clustering Coefficient (CC) is represented as a function of the network size in scale-free (SF), small-world (SW), Erdos–Rényi (ER) networks and as a bar chart for real networks.

We used the model proposed by Holme and Kim to generate the SF networks. In each experiment, we chose the number of nodes $n = 10,000$, we added $m = \{5, 15, 25, 35, 50\}$ random edges for each new node i, and we picked a probability $p = 0.3$ of adding a triangle after adding a random edge.

SW graphs were generated using NWS small-world model. In each experiment, we chose the number of nodes $n = 10,000$, $k = \{6, 18, 32, 64\}$ neighbors with which connect each node i in the ring topology, and a probability $p = 0.6$ of rewiring each edge.

ER networks were generated choosing the network size $n = 10,000$, and for edge creation the probability values $p = \{0.001, 0.003, 0.005, 0.010\}$.

For the implementation of the artificial networks and the centrality metrics such as DC, BC, CL, and CC, we used Python and NetworkX module. To run the WERW-Kpath[2], we set the value of the random walk to $k = 10$. For GoT, we set 1 thief per node and the initial amount of vdiamonds per node equal to the network size n. We let GoT to run for $T = \log^3 n$ epochs.

[2] Available at: http://www.emilio.ferrara.name/code/werw-kpath/

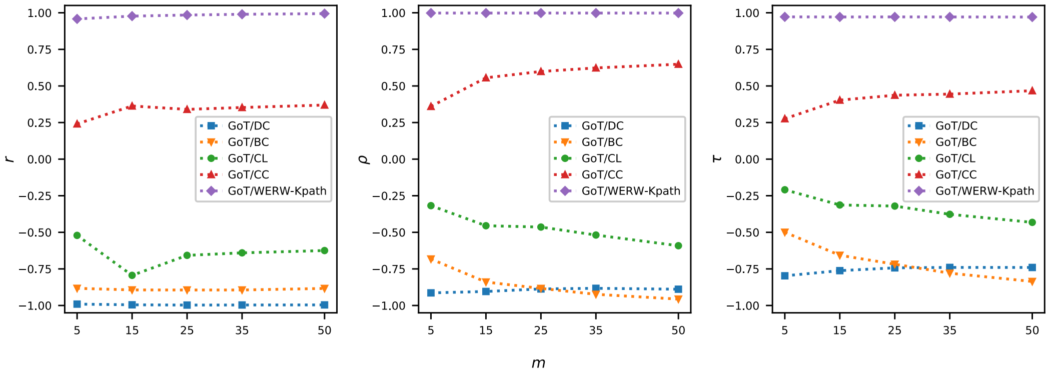

FIGURE 2.6: **Correlation coefficients among Game of Thieves (GoT) and other centrality measures in scale-free (SF) networks of different densities.** Pearson's r, Spearman's ρ and Kendall's τ between GoT and Degree Centrality (DC), GoT and Betweenness Centrality (BC), GoT and Closeness (CL) Centrality, GoT and Clustering Coefficient (CC), GoT and Weighted Edge Random Walks – K Path (WERW-Kpath) are represented as functions of the network density in SF networks.

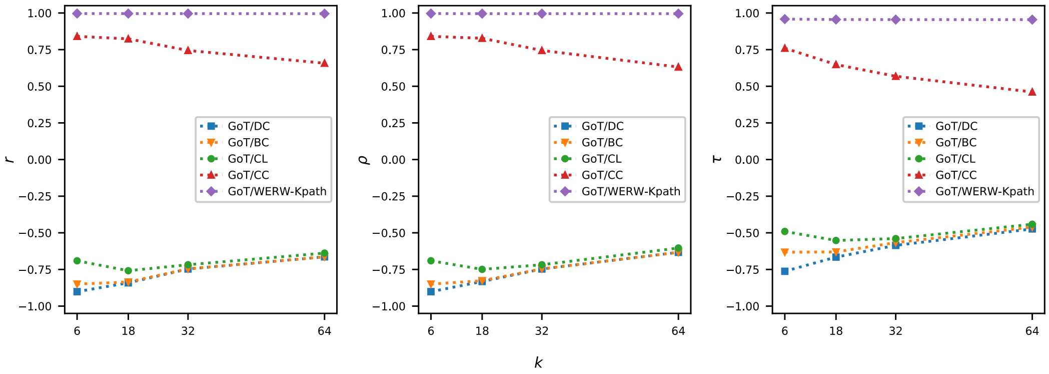

FIGURE 2.7: **Correlation coefficients among Game of Thieves (GoT) and other centrality measures in small-world (SW) networks of different densities.** Pearson's r, Spearman's ρ and Kendall's τ between GoT and Degree Centrality (DC), GoT and Betweenness Centrality (BC), GoT and Closeness (CL) Centrality, GoT and Clustering Coefficient (CC), GoT and Weighted Edge Random Walks – K Path (WERW-Kpath) are represented as functions of the network density in SW networks.

In Figs. 2.6, 2.7 and 2.8 are shown the results of the Pearson's r correlation coefficient (left column), the Spearman's ρ (middle column) and the Kendall's τ rank correlation coefficients (right column) for SF, SW and ER networks respectively.

In SF networks (see Fig. 2.6), GoT and DC have the strongest negative correlation. GoT exhibits a strong negative correlation with the BC and slightly weaker with the CL. There is a positive correlation between GoT and the CC which becomes stronger for the rank correlation coefficients. In particular, we can observe that the Spearman's ρ is always larger than the Kendall's τ. Except for the DC, we can observe a small deviation of the rank correlation coefficients when the number of edges

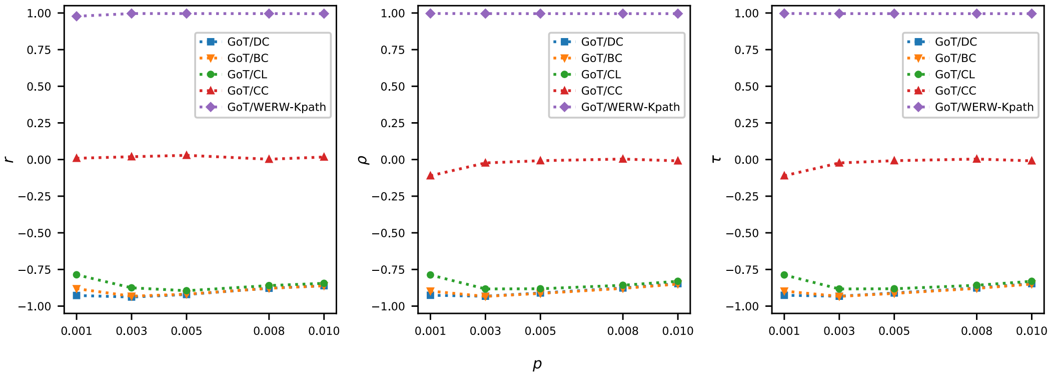

FIGURE 2.8: **Correlation coefficients among Game of Thieves (GoT) and other centrality measures in Erdos–Rényi (ER) networks of different densities.** Pearson's r, Spearman's ρ and Kendall's τ between GoT and Degree Centrality (DC), GoT and Betweenness Centrality (BC), GoT and Closeness (CL) Centrality, GoT and Clustering Coefficient (CC), GoT and Weighted Edge Random Walks – K Path (WERW-Kpath) are represented as functions of the network density in ER networks.

in the analyzed networks is smaller which is not visible anymore when edges grow big enough.

In SW networks (see Fig. 2.7), there is an almost identical strong negative correlation among GoT and DC, BC and CL. We can also still observe a strong positive correlation between GoT and the CC. All of these correlations become weaker when the number of edges grows.

In ER networks (see Fig. 2.8), the correlation among GoT and DC, BC and CL is the same as in SW networks. But, in this kind of networks, there is no correlation between GoT and the CC even if we can observe a very little deviation when the number of edges is small.

In all networks, we can observe a strong positive correlation among GoT and WKP which remains constant when the number of edges grows.

According to our results, there is a strong correlation among GoT and the most known centrality algorithms. For this reason, our future works will explore the possibility to substitute them with GoT in the computation of node centrality in large networks.

2.3.3 Case study on Mafia networks

In Ficara et al. (2021d), we explored at first the correlation among GoT and DC, BC, CL and CC for measuring node centrality. Then, we explored the correlation between EBC, GoT and WKP for measuring edge centrality. This two kinds of studies were conducted on specific type of complex criminal networks which are Mafia networks. Our analysis focused on six real criminal networks related to three distinct Mafia operations called Montagna, Infinito and Oversize (see Subsect. 1.3.1).

The first experiment we performed consists in the identification of the ten most important nodes in the six Mafia networks using GoT and the four canonical nodes centrality measures DC, BC, CL and CC (see Fig. 2.9). GoT seems to be able to identify the most important nodes in the networks in a pretty similar way to DC, BC and CL. The CC seems instead to identify different nodes as the most central.

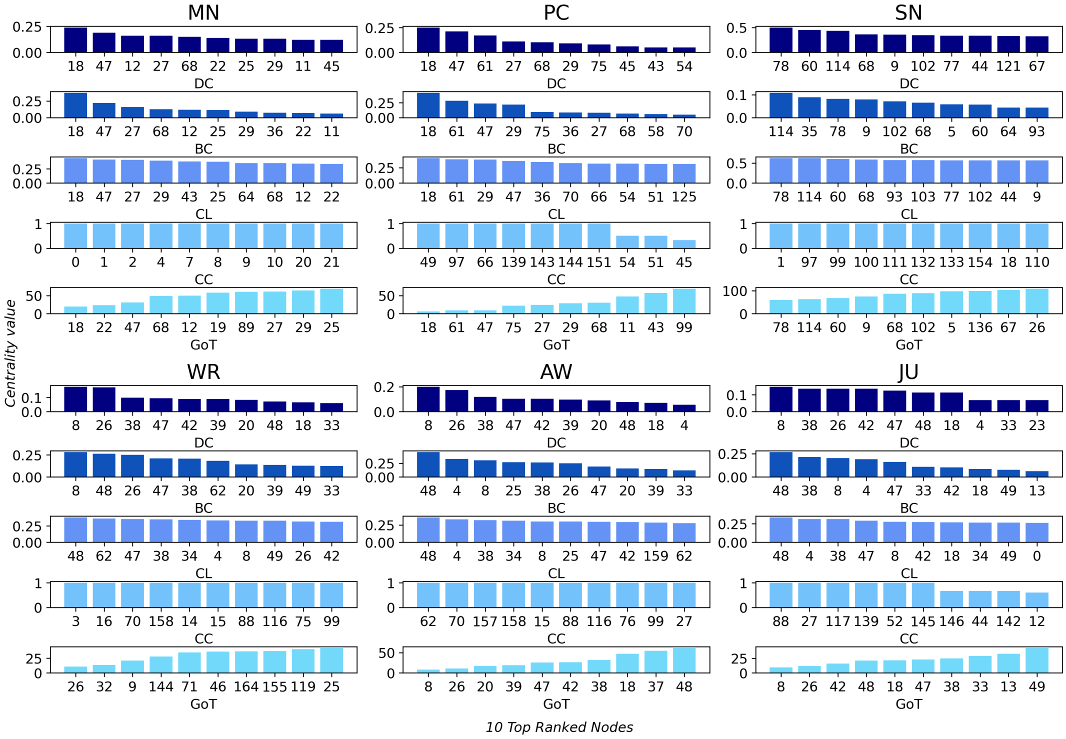

FIGURE 2.9: **The 10 top ranked nodes in Mafia networks.** The 10 most central nodes are computed with degree centrality (DC), betweenness centrality (BC), closeness (CL) centrality, clustering coefficient (CC) and Game of Thieves (GoT) in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW) and Judgment (JU) networks.

Regarding the Montagna Operation, GoT is able to identify the two most important nodes, 18 and 47, which are respectively the Caporegime of the Mistretta family and the deputy Caporegime of the Batanesi family. Mistretta and Batanesi are the two Mafia families at the centre of this investigation. Node 22 is also important because it represents a pharmacist who can have a key role in drug synthesis processes which require pharmacological and chemical knowledge (Cavallaro et al., 2020b). Only future experiments may share insights about the reason why this node seems to be more central using GoT. Nodes 68, 27 and 25 are caporegimes while the others are associates as entrepreneurs. More details about the roles of nodes in the Montagna Operation can be found in Table 6.1.

If applied to the Infinito *SN*, GoT is capable to find some of the leaders of the criminal networks such as Node 78 which is is always at the top rank across all measures as described by Grassi et al. (2019). The authors discovered 22 leaders in the Infinito Operation. Some of them, such as nodes 114, 9 and 6, are also found by GoT.

About the Oversize networks (*i.e.*, *WR*, *AW* and *JU*), GoT is able to discover two drug wholesaler (*i.e.*, nodes 26 and 39), a drug sealer (*i.e.*, node 13) and also the boss' son and important drug dealer (*i.e.*, node 49).

Our results seem to be confirmed by our correlation analysis. We used the most well-known correlation coefficients (*i.e.*, Pearson's r, Spearman's ρ and Kendall's τ). Since the results for the three coefficients were quite similar, we chose to show only those for the Spearman's ρ because it best captured the relationships among all the considered centrality measures.

The Spearman's ρ and the traditional centrality measures were computed in Python also using the NetworkX module. To improve these experiments, the available version of GoT in Python 2 was ported to Python 3, while the available Java version of WKP was ported to Python. Moreover, to get more reliable results, GoT and WKP were repeated for 30 times on each network. Then, we computed the mean and standard deviation values. This was necessary because in such measures the centrality values change at each execution. They are not in fact deterministic measure as DC, BC, EBC, CL and CC.

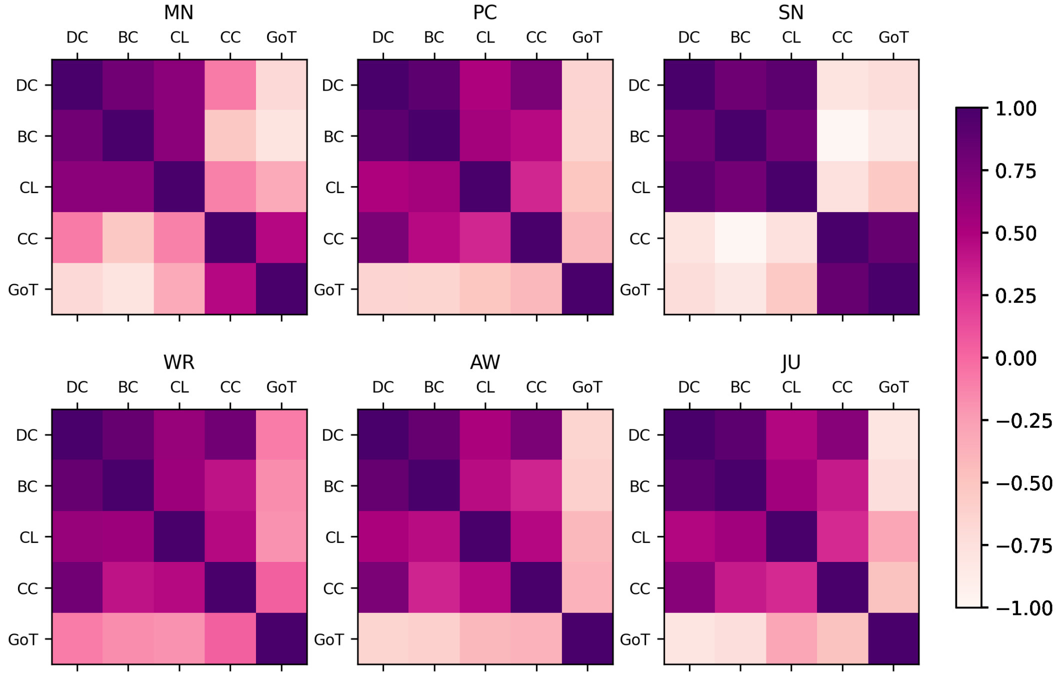

FIGURE 2.10: **Spearman rank correlation coefficient among Game of Thieves (GoT) and node centrality measures in Mafia networks.** Spearman's ρ is computed among GoT, degree centrality (DC), betweenness centrality (BC), closeness (CL) centrality and clustering coefficient (CC) in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW) and Judgment (JU) networks.

The Spearman coefficient (see Fig. 2.10) shows how in most cases there is a strong negative correlation among GoT, BC and DC, and a moderate negative correlation between GoT and CL. More peculiar seems to be the relationship between GoT and CC, which seem to have a strong positive correlation in networks as *MN* or *SN*, and a moderate or strong negative correlation in the other networks. In the Oversize *WR* network, we obtained a weak or absent correlation among all the measures. This result is an exception with respect to the other graphs and it can be explained through the peculiar degree distribution (see Fig. 1.3) of this network which indicates that there are only two hubs, while most nodes have only 1 connection.

The negative correlation is easily explained by the fact that the most important nodes for GoT are those with the smaller number of vdiamonds, and therefore the smaller centrality value.

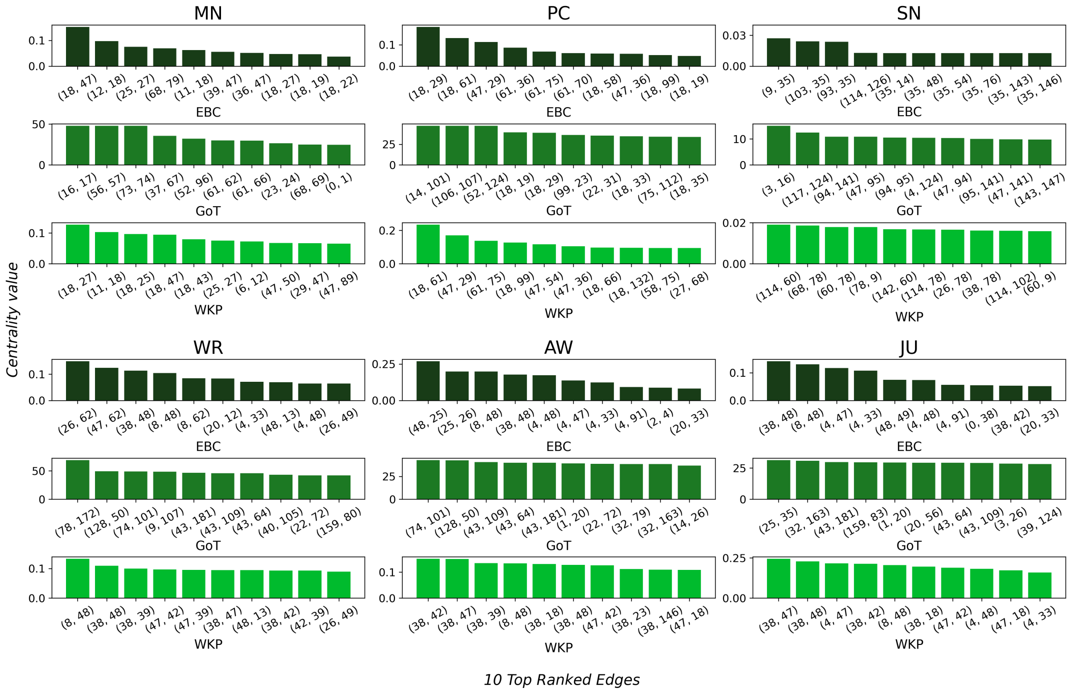

FIGURE 2.11: **The 10 top ranked edges in Mafia networks.** The 10 most central edges are computed with edge betweenness centrality (EBC), Game of Thieves (GoT) and WERW-Kpath (WKP) in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW) and Judgment (JU) networks.

Then, we continued with the experiments on edge centrality computing the ten most important edges in the six Mafia networks using GoT, WKP and the canonical edge centrality measure EBC (see Fig. 2.11). This time, WKP seems to find results more similar to EBC in the identification of the most important edges, if compared to GoT.

The Spearman coefficient in Fig. 2.12 shows how in all the cases WKP has a moderate positive correlation with EBC, and a moderate or strong negative correlation with GoT. GoT has a weak or absent correlation with EBC.

The correlation among WKP and EBC is an important finding because we can think to substitute random edge betweenness computing edge centrality through WKP in a much shorter time than that required by EBC for very large networks.

Although the existence of a correlation among GoT and the standard centrality measures does not imply the replaceability of them with the other, a future series of experiments may lead us to consider the possibility of using GoT to compute node and edge centrality along with the standard measures. These experiments should be about GoT behaviour varying the input parameters (*i.e.*, the number of thieves per node, the number of vdiamonds per node and the number of epochs) and applying on networks of different characteristics (*e.g.* BA models with different densities).

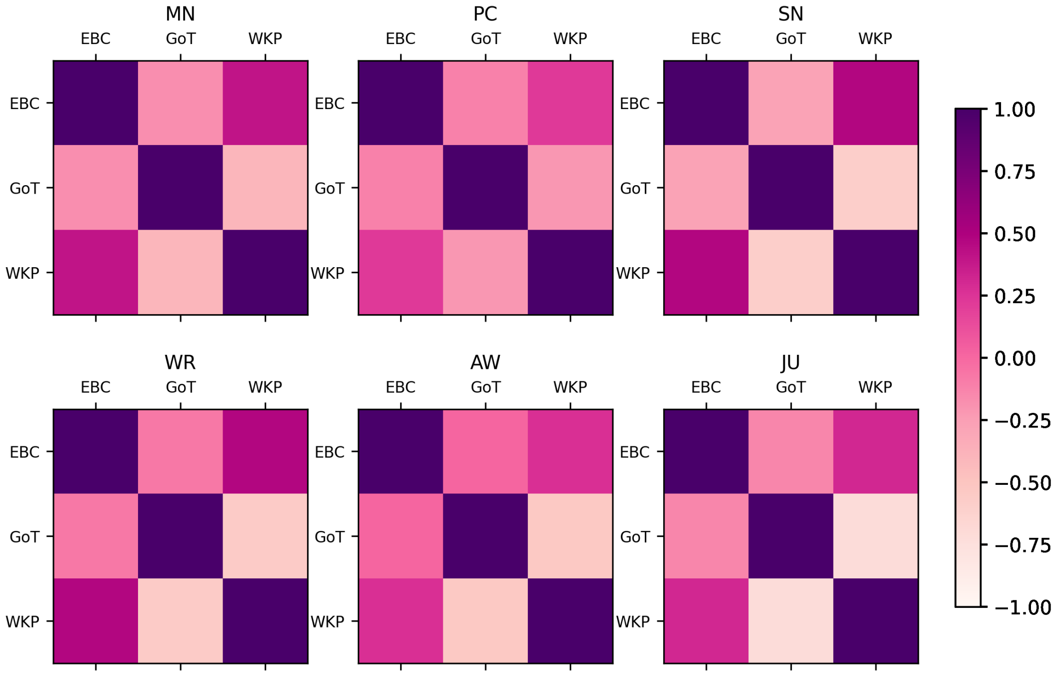

FIGURE 2.12: **Spearman rank correlation coefficient among Game of Thieves (GoT) and edge centrality measures in Mafia networks.** Spearman's ρ is computed among GoT, WERW-Kpath (WKP) and edge betweenness centrality (EBC) in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW) and Judgment (JU) networks.

Chapter 3

Graph comparison between artificial and covert networks

One common application in graph theory is to develop random graph models which mimic the structure and behavior of real networks. Even if the growing mechanism of such criminal networks 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 plausible as well as fruitful in terms of detecting insights about the structure and behavior of the real network. The growth of available data and number of network models (Newman, 2018; Peixoto, 2018; Squartini, Mastrandrea, and Garlaschelli, 2015), 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 (Tantardini et al., 2019). This is a non-trivial task, since one of the most faced issues in such regard deal with the result effectiveness, their interpretability and the computational efficiency. The validity of such techniques has indeed been assessed, being cospectrality issues one of the main reasons that could potentially make them weak. It was though shown that the fraction of cospectral graphs is 21% for networks composed of 10 nodes and is less for 11 nodes (Wilson and Zhu, 2008). 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 (Donnat and Holmes, 2018; Emmert-Streib, Dehmer, and Shi, 2016; Soundarajan, Eliassi-Rad, and Gallagher, 2014). Hartle et al. (2020) proposed simple ensembles of random networks as natural benchmarks for network comparison methods showing that the expected distance between two networks independently sampled from a generative model can be a useful property that encapsulates many key features of that model. The authors calculated the within-ensemble graph distance and related quantities for classic network models using 20 distance measures commonly used to compare graphs. Wills and Meyer (2020) 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 (Akoglu, Tong, and Koutra, 2015) drastically reduces when one requires an algorithm which runs in reasonable time on large graphs.

A completely new SNA approach to study crime could be the identification of the best measures for distance between graphs in a criminal scenario. The novelty of this type of work consists in generating artificial networks which mirror the topology and functionality of real criminal networks; this study help to understand which artificial model best simulates real criminal networks and it concretely aids police forces to predict the formation of links between criminals as well as to detect the individuals who, if arrested, would damage the most the information flow across the organization.

3.1 Graph distances

3.1.1 Spectral distances

Spectral distances allow to measure the structural similarity between two graphs starting from their spectra. The spectrum of a graph (see Subsect. 1.1.3) is widely used to characterize its properties and to extract information from its structure.

The most common matrix representations of a graph are the adjacency matrix A, the Laplacian matrix L, and the normalized Laplacian $\mathcal{L}$.

The adjacency matrix (see Eq. 1.2) and the degree matrix (see Eq. 1.8) are used to compute the combinatorial Laplacian matrix L, which is an $n \times n$ symmetric matrix defined as:

$$L = D - A\,. \tag{3.1}$$

The diagonal elements L_{ii} of matrix L are then equal to the degree k_i of the node i, while the off-diagonal elements L_{ij} are -1 if the node i is adjacent to j, and 0 otherwise. A normalized version of the Laplacian matrix $\mathcal{L}$ is defined as:

$$\mathcal{L} = D^{-\frac{1}{2}} L D^{-\frac{1}{2}}\,, \tag{3.2}$$

where the diagonal matrix $D^{-\frac{1}{2}}$ is given by:

$$D_{i,i}^{-\frac{1}{2}} = \begin{cases} \frac{1}{\sqrt{k_i}} & \text{if } k_i \neq 0 \\ 0 & \text{otherwise}\,. \end{cases} \tag{3.3}$$

If the representation matrix is symmetric, its eigenvalues are real and they can be sorted. The spectrum of a graph consists indeed of the set of the sorted eigenvalues of one of its representation matrices. The sequence of eigenvalues may be ascending or descending depending on the chosen matrix. The spectra derived from each representation matrix may reveal different properties of the graph. The largest eigenvalue in modulus is called the spectral radius of the graph. If λ_k^A is the k^{th} eigenvalue of the adjacency matrix A, then the spectrum is given by the descending sequence:

$$\lambda_1^A \geq \lambda_2^A \geq \cdots \geq \lambda_n^A\,. \tag{3.4}$$

If λ_k^L is the k^{th} eigenvalue of the Laplacian matrix L, such eigenvalues are considered in ascending order so that:

$$0 = \lambda_1^L \leq \lambda_2^L \leq \cdots \leq \lambda_n^L\,. \tag{3.5}$$

The second smallest eigenvalue of the Laplacian matrix of a graph is called its algebraic connectivity. Similarly, if we denote the k^{th} eigenvalue of the normalized

Laplacian matrix $\mathcal{L}$ as $\lambda_k^{\mathcal{L}}$, then its spectrum is given by:

$$0 = \lambda_1^{\mathcal{L}} \leq \lambda_2^{\mathcal{L}} \leq \cdots \leq \lambda_n^{\mathcal{L}} \, . \tag{3.6}$$

The spectral distance between two graphs is the euclidean distance between their spectra (Wilson and Zhu, 2008). Given two graphs G and G' of size n, with their spectra respectively given by the set of eigenvalues λ_i and λ_i', their spectral distance, according to the chosen representation matrix, is computed as follows by the formula:

$$d(G, G') = \sqrt{\sum_{i=1}^{n} (\lambda_i - \lambda_i')^2} \, . \tag{3.7}$$

Based on the chosen representation matrix and consequently its spectrum, the most common spectral distances are the adjacency spectral distance d_A, the Laplacian spectral distance d_L and the normalized Laplacian spectral distance $d_{\mathcal{L}}$.

If the two spectra are of different sizes, the smaller graph is brought to the same cardinality of the other by adding zero values to its spectrum. In such case, only the first $k \ll n$ eigenvalues are compared. Given the definitions of spectra of the different matrices, the adjacency spectral distance d_A compares the largest k eigenvalues, while d_L and $d_{\mathcal{L}}$ compare the smallest k eigenvalues. This determines the scale at which the graphs are studied, since comparing the higher eigenvalues allows to focus more on global features, while the other two allow to focus more on local features.

3.1.2 Matrix distances

Another class of distances between graphs is the matrix distance (Wills and Meyer, 2020). A matrix of pairwise distances d_{ij} between nodes on the single graph is constructed for each as:

$$M_{ij} = d_{ij} \, . \tag{3.8}$$

While the most common distance d is the shortest path, other measures can also be used, such as the effective graph resistance, or variations on random-walk distances. Such matrices provide a signature of the graph characteristics and carry important structural information. Matrices M are then compared using some norm or distance.

Given two graphs G and G', having M and M' as their respective matrices of pairwise distances, the matrix distance between the G and G' is introduced as:

$$d(G, G') = \| M - M' \| \, , \tag{3.9}$$

where $\|.\|$ is a norm to be chosen. If the matrix used is the adjacency matrix A, the resulting distance is called edit distance.

Two graphs can also be compared using a similarity measure called DELTACON (Koutra, Vogelstein, and Faloutsos, 2013). It is based on the root euclidean distance $\mathrm{d}_{\mathrm{rootED}}$, also called Matsusita difference, between matrices S created from the fast belief propagation method of measuring node affinities.

The DELTACON similarity sim_{DC} is defined as:

$$sim_{DC}(G, G') = \frac{1}{1 + \mathrm{d}_{\mathrm{rootED}}(G, G')} \, , \tag{3.10}$$

where the root euclidean distance $\mathrm{d}_{\mathrm{rootED}}(G, G')$ is defined as:

$$\mathrm{d}_{\mathrm{rootED}}(G, G') = \sqrt{\sum_{i,j}(\sqrt{S_{i,j}} - \sqrt{S'_{i,j}})^2} \,. \tag{3.11}$$

When used instead of the Euclidean distance, $\mathrm{d}_{\mathrm{rootED}}(G, G')$ may even detect small changes in the graphs. The fast belief propagation matrix S is defined as:

$$S = [I + \varepsilon^2 D - \varepsilon A]^{-1} \,, \tag{3.12}$$

where $\varepsilon = 1/(1 + \max_{1 \le i \le n} D_{ii})$ and it is assumed to be $\varepsilon \ll 1$, so that S can be rewritten in a matrix power series as:

$$S \approx I + \varepsilon A + \varepsilon^2(A^2 - D) + \ldots \tag{3.13}$$

Fast belief propagation is an effective algorithm and it is designed to perceive both global and local structures of the graph (Koutra, Vogelstein, and Faloutsos, 2013).

3.2 Case study on the Montagna operation

In Cavallaro et al. (2021) and Ficara et al. (2021f), we used traditional network models from graph theory (*i.e.*, ER, WS, BA and EBA) to replicate the topology of the Montagna Meetings network. We built 1000 networks for each type with a number of edges as close as possible to that of our Mafia network, which is equal to 256.

To compare the Montagna Meetings network to the network models, we used two graph distances: the adjacency spectral distance d_A (see Eq. 3.7) and the root euclidean distance $\mathrm{d}_{\mathrm{rootED}}$ (see Eq. 3.11). From $\mathrm{d}_{\mathrm{rootED}}$, we also derived the DELTACON similarity sim_{DC}. Then, we computed the average values of d_A, $\mathrm{d}_{\mathrm{rootED}}$ and sim_{DC} for each type of network model together with the error rates.

The aim of our study was to find the best model which reproduces a criminal network. Both the graph distances identified the BA models as the ones that better approximate our Mafia network. BA models are built based on a specific parameter m, which indicates the number of edges that are preferentially attached to existing nodes with high degree. We tried two different configurations of the BA graphs with $m = 2$ and $m = 3$. But, it was not possible to obtain the exactly same number of edges of our criminal network. For this reason, we used preferential attachment and random strategies to add or remove edges from them. This further experiment was done to discover if the graph distances decreased, when the number of edges coincided perfectly with 256.

3.2.1 How to simulate a covert network

The first step of our analysis was the computation of the sim_{DC} similarity and the $\mathrm{d}_{\mathrm{rootED}}$ distance (see Eqs. 3.10 and 3.11) to measure how well an artificial network may catch some real network features in a criminal scenario.

Thus, we compared the Montagna MN with three network models, i.e., ER, WS and BA with several configurations, for a total of 5 models. The analysis of the MN network, which was conducted in Ficara et al. (2020), found that it followed a scale-free power law. For this reason, we chose the BA model.

Even if this is not the main purpose of our study, it is worth highlighting that criminal organizations adopt specific criteria for recruiting new affiliates (growing and preferential attachment dynamics) (Williams, 2001). A single network snapshot such as *MN* we created is clearly insufficient, as a temporal network would be better suited. But this would require a deeper knowledge of the dynamics of the criminal network which is usually unknown. For comparison, we have selected also the ER and WS models, notwithstanding the fact that the random nature of these models hardly can reproduce the nature of a real network. The WS model is more realistic than the ER model because it exhibits a small diameter, short average path lengths and high clustering coefficient. In most real networks, in fact, nodes tend to create close groups with a high density of edges. Despite this, WS models cannot model real networks where degree distributions are usually power-law as in the BA models.

We used Python and NetworkX (Hagberg, Schult, and Swart, 2008) to create all the network models. In Table 3.1 are listed the parameters and the corresponding values used in our experiments. The number of nodes n is defined a priori in all the models considered, whereas the number of edges e is set only in the ER model. In WS, k represents the number of nearest neighbors in ring topology to which each node is connected. We chose $k = 6$ so to obtain a number of edges as close as possible to the real criminal network. The same has been done for the input parameters of all the BA models chosen herein. But, in this case, three different configurations have been selected: BA2, BA3 and EBA. BA2 and BA3 are standard BA models in which each new node is connected to $m = 2$ and $m = 3$ "old" nodes respectively. The EBA model requires two more parameters: (i) p, *i.e.*, the probability that m randomly chosen pairs of nodes are connected by an edge, and (ii) q, *i.e.*, the probability of rewiring an edge. We set $q = 0$ to avoid introducing more randomness in the network process.

Table 3.1: **Network model parameters.** Erdös-Rényi (ER), Watts-Strogatz (WS), Barabási-Albert (BA), Extended Barabási-Albert (EBA) have the same number of nodes n of the Montagna Meetings network. The number of edges e changes according to their specific parameters.

Network model	**Parameter**					
	n	**e**	**m**	**k**	**p**	**q**
ER	101	256				
WS	101			6	0.6	
BA2	101		2			
BA3	101		3			
EBA	101		2		0.225	0

Then, we computed the DeltaCon similarity, which allows to compare two graphs having different numbers of nodes and/or edges. Unfortunately this measure did not yielded indisputable results about the network model closest to the real network. We therefore resorted to compute the adjacency spectral distance which, in contrast, clearly allowed us to identified the BA model networks as the best at catching the real network features.

The last step consisted in considering the number of edges of the network models. The BA models with $m = 2$ and $m = 3$ have a number of edges different from the real network. For this reason, we decided to further investigate whether the adjacency spectral distance could have been reduced by increasing (in the case of BA2) or reducing (BA3) the number of edges until they were equal to the number of edges of the real network. This is required to iteratively add an edge to the BA2 (respectively, remove an edge from the BA3) and recalculate the adjacency spectral distance. The procedure ends when the number of edges coincides with that of the real network. Two strategies have been devised to select the candidate edge: (i) a preferential attachment selection, in which the edge is added (or removed) among the edges of the best connected nodes, and (ii) a random selection, in which the edge is selected at random.

In order to significantly reduce statistical errors, the experiments have been repeated 1000 times for each artificial network (ER, WS, BA2, BA3, EBA), from which the average values have been computed.

3.2.2 The best model to simulate a covert network

Table 3.2 shows the average values of the root euclidean distance d_{rootED} and the DELTACON similarity sim_{DC} between the real network and the five random models. Being d_{rootED} a distance measure, the higher its value is, the more the two compared networks are different. Viceversa, being sim_{DC} a similarity measure that takes values between 0 and 1, the more its value is close to 1, the more the two compared networks are similar. The error of sim_{DC} is equal to 0.015 for all the network models and has not been reported.

TABLE 3.2: Root euclidean distance d_{rootED} and DELTACON similarity sim_{DC} between the Montagna Meetings network and the network models, *i.e.*, Erdös-Rényi (ER), Watts-Strogatz (WS), Extended Barabási-Albert (EBA), and Barabási-Albert (BA) with two different configurations. The number of edges e is also showed.

Network model	e	$\mathbf{d_{rootED}}$	$\mathbf{sim_{DC}}$
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

From the analysis of the results shown in the Table 3.2, it is clear that all the BA models are able to better approximate our Montagna *MN* network with respect to ER and WS models.

The similarities between the real network and the random models were further analyzed by evaluating the adjacency spectral distance d_A. These results are shown in Table 3.3.

Also in this case, we can observe a huge adjacency spectral distance d_A among the criminal networks and the ER and WS models which even reaches more than 9. The BA models are confirmed to be the most similar to the Montagna *MN* network. This time, the EBA has the best performance.

Both the selected graph distances d_{rootED} and d_A agree that the ER and WS models are are the most distant from a criminal network.

Tables 3.2 and 3.3 also show how the BA models have a different number of edges e. A different number of edges implies a different number of nonzero elements of the adjacency or Laplacian matrices, thus affecting the resulting eigenvalues.

To obtain more precise and comparable results, we tried to change the BA models to reach a number of edges closer to our *MN* (*i.e.*, 256 edges). The BA2 model is characterized by a smaller e than *MN*, while the BA3 model possesses a higher e.

TABLE 3.3: Adjacency spectral distance d_A between the Montagna Meetings network and the network models, *i.e.*, Erdös-Rényi (ER), Watts-Strogatz (WS), Extended Barabási-Albert (EBA), and Barabási-Albert (BA) with two different configurations. The number of edges *e* is also showed.

Network model	e	d_A
ER	256	8.4 ± 0.2
WS	202	9.2 ± 0.2
EBA	255	6.6 ± 0.2
BA2	198	6.9 ± 0.2
BA3	294	7.1 ± 0.2

Two procedures were, then, adopted to iteratively add to BA2 or remove from BA3 the percentage of *e* needed to reach the 256 edges of the Montagna *MN*. The two procedures are based on two different approaches: preferential attachment and random selection.

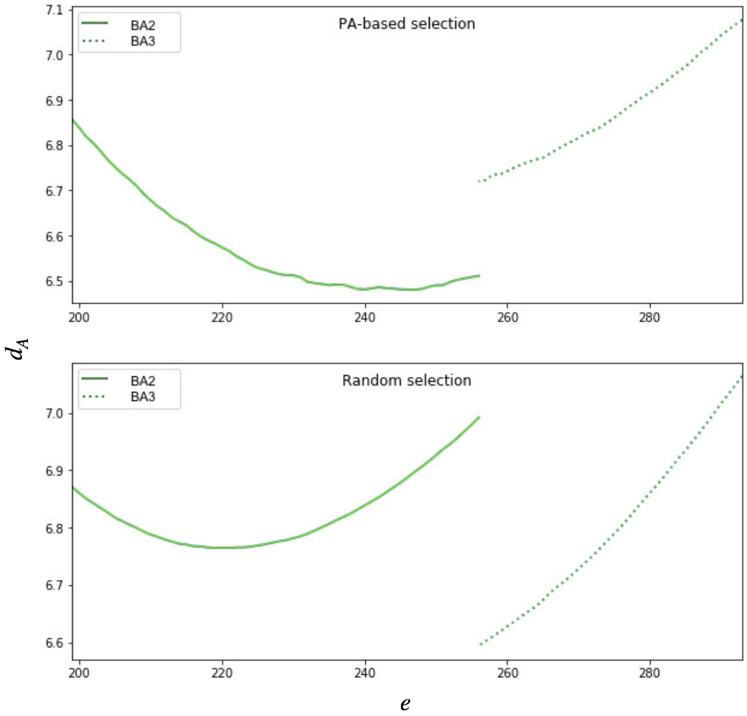

FIGURE 3.1: **Difference between adjacency spectral distances when different strategies are applied to change the number of edges of Barabási-Albert models.** Adjacency spectral distance d_A is represented as a function of the number of edges *e* added to BA2 and removed from BA3 with a Preferential Attachment (PA) or Random strategy. BA2 and BA3 are Barabási-Albert models with respectively 2 and 3 edges preferentially attached to existing nodes with high degree.

Fig. 3.1 shows the difference between ordinates when abscissa is equal to 256. Ideally, this difference should reduce to 0 when both the BA models reach the same number of edges (*i.e.*, 256). This does not happen because the BA2 and BA3 models are still different and it is not enough to add or remove edges to make them identical. However, we can observe that the PA approach works better reducing this difference more than the random approach.

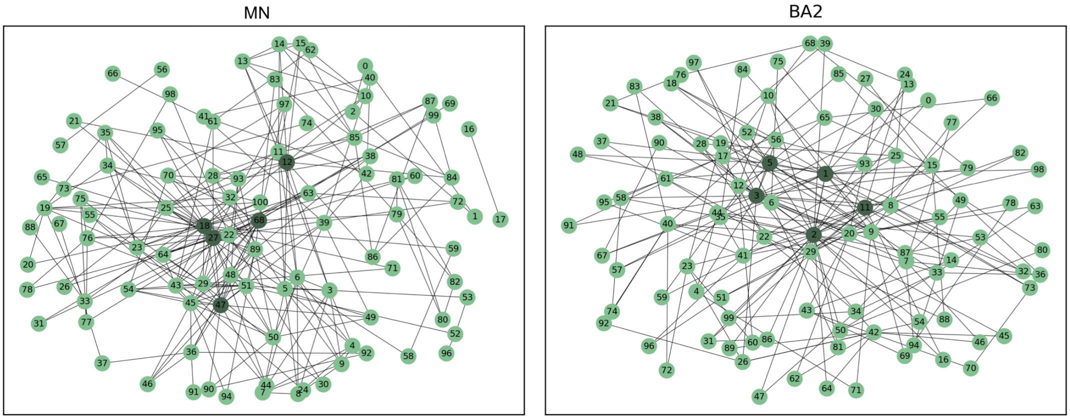

FIGURE 3.2: **Graphical comparison between the Montagna Meetings (MN) network and the BA2 model.** BA2 is a Barabási-Albert model with 2 edges preferentially attached to existing nodes with high degree. The five high degree nodes in MN and BA2 are marked in dark green.

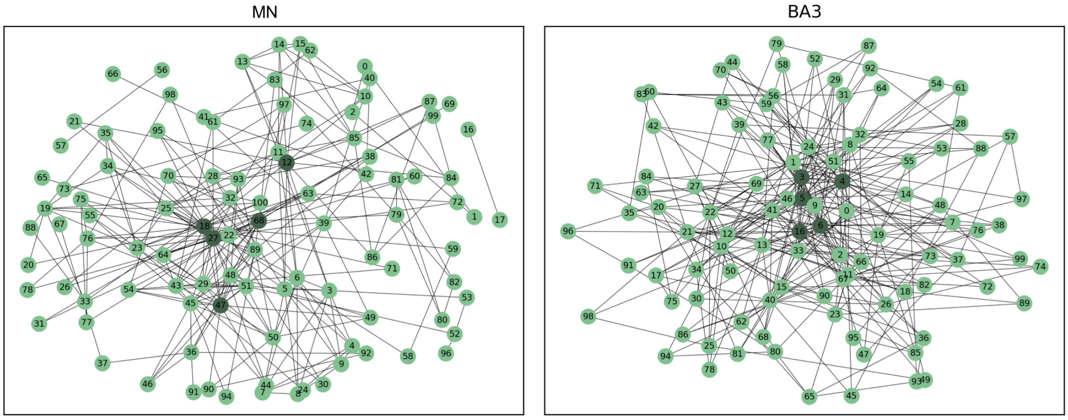

FIGURE 3.3: **Graphical comparison between the Montagna Meetings (MN) network and the BA3 model.** BA3 is a Barabási-Albert model with 3 edges preferentially attached to existing nodes with high degree. The five high degree nodes in MN and BA3 are marked in dark green.

In Figs. 3.2 and 3.3 is shown a graphical comparison between the Montagna *MN* network and the BA models. The five high degree nodes are highlighted because the identification of the most important nodes in an artificial model could lead to also find the key nodes in criminal network thus helping in police investigations.

Our experiments identify the BA model as the one which better represents a criminal network. For this reason, we could expect that new members of a criminal organization will be more likely to establish connections with high degree nodes rather than low degree nodes. Such studies could indeed help LEAs in their investigations because they could focus their resources and attention on high degree individuals to intercept criminals instead to waste time and resources to follow individuals without obtaining any concrete results.

These studies have limitations which may be addressed by future research. First, our results rely on a single case study, which implies limited external validity. Our analysis focused on the Sicilian Mafia which has a very peculiar hierarchical structure (see Fig. 1.4). Its peculiarities may hinder the generalizability of our results to other form of organized crime.

Our research can pave the way to the application of network models in police investigations. LEAs could create models which replicate criminal networks starting from the investigation data, even if they are affected by noise or missing information. Network models could be used to predict and prevent the creation of relationship ties between criminals or to break those ties by arresting one or more of the suspects.

Chapter 4

The missing data problem

In the analysis of criminal networks, missing data can refer to missing nodes and/or missing edges (Morselli, 2008). The problem of missing nodes has already received attention (Hric, Peixoto, and Fortunato, 2016; Kim and Leskovec, 2011) but it is not particularly relevant in Mafia networks because it is quite improbable that LEAs may disregard central criminals during prolonged anti-mafia investigations. On the other hand, while it is possible to predict some missing edges among already detected criminals, it is impossible to detect missing criminals relying only on pre-trial detention orders.

Missing edges refer to the lack of information on the relations between two known criminals. LEAs, in fact, may miss a lot of criminal activities such as meetings or phone calls, and therefore relevant plans of the criminal organization (Agreste et al., 2016; Campana and Varese, 2012; Catanese et al., 2014; Ferrara et al., 2014). For this reason, we do not have a complete dataset of all possible meetings or phone calls between suspected criminals, but it is reasonable to assume that they have occurred. Therefore, it becomes necessary to make predictions.

A crucial application of SNA methods to intelligence is the so-called link prediction problem (Liben-Nowell and Kleinberg, 2003; Pandey et al., 2019): given a graph G which describes interactions between pairs of criminals, it is possible to predict which edges are more likely to appear in G in the near future. Algorithms to solve the link prediction problem may hugely impact police activities: in fact, if we would be able to accurately predict the formation of new links, we would be able to discover pairs of criminals who are likely to collaborate and, thus, we could early detect and prevent crimes.

Many link prediction methods have been designed and implemented in a broad range of domains (Liben-Nowell and Kleinberg, 2003; Pandey et al., 2019) and, more recently, Berlusconi et al. (2016) applied link prediction algorithms on a dataset derived from an Italian criminal case against a Mafia group.

Almost all of the existing approaches to link prediction focus on maximizing the accuracy, and they overlook fundamental aspects such as the robustness of predictions, namely the extent to which the incompleteness of information about relations may affect the quality of predictions. By construction, in fact, datasets associated with criminal networks are noisy and incomplete: on one hand, investigations often encounter individuals unrelated to the criminal organization (*e.g.*, friends, relatives, and other frequent contacts) and, on the other hand, some members of the organization actively attempt to avoid detection, *e.g.*, by refraining from the use of telephone, using intermediaries, and coding messages. As a consequence, imprecise and incomplete information is a critical impediment to understand network boundaries and topology and, ultimately, it constitutes a main challenge for LEAs which plan to get reliable results from the application of link prediction algorithms.

A completely new SNA approach to study the problem of missing data could be done using graph distances (see Sect. 3.1) to quantify the effects of missing nodes or edges on a criminal network. Given a graph G, nodes or edges are randomly removed to simulate scenarios in which a criminal, a meeting or a phone call eludes audio or physical surveillance. After the removal, a second graph G' is created. Graph distances (see Sect. 3.1) can be used to compare G and G'. In this way, it is possible to know how much the overall understanding of G changes with incomplete data.

4.1 Link prediction in Montagna

In Calderoni et al. (2020), we tackled the problem of estimating the robustness of link prediction algorithm in the Montagna Meetings and Phone Calls networks.

The link prediction problem (Liben-Nowell and Kleinberg, 2003) is defined as follows:

Definition 1 *Let $G = \langle N, E\rangle$ be an undirected graph and let $G' = \langle N, E'\rangle$ be a subgraph of G which contains all nodes in G and a subset $E' \subseteq E$ of its edges. The link prediction problem consists of printing a list of non-edges in G' which are edges in G.*

We will call the set E' as the training set and the set $E - E'$ as the test set.

In practice, algorithms to solve the link prediction problem build a matrix $\mathbf{\Omega}$ in which the entry $\mathbf{\Omega}_{ij} = \sigma_{ij}$ specifies the degree of similarity between the nodes i and j; all pair of non edges $\langle i, j\rangle$ in G are thus ranked in decreasing order of similarity and non-edges with the largest similarity scores are the most likely to exist (Liben-Nowell and Kleinberg, 2003).

We can define many similarity scores to compute the similarity degree of two nodes in G. Methods to compute node similarity can be classified into local and global methods.

4.1.1 Local methods for node similarity

A first class of methods to calculate node similarity in graphs is known as local methods (Leicht, Holme, and Newman, 2006; Liben-Nowell and Kleinberg, 2003), because they only require the knowledge of the neighbors N of two nodes i and j. Some of the most popular local methods are as follows:

(1) Jaccard Coefficient (JC) (Jaccard, 1912; Liben-Nowell and Kleinberg, 2003):

$$JC(i, j) = \frac{|\mathcal{N}(i) \cap \mathcal{N}(j)|}{|\mathcal{N}(i) \cup \mathcal{N}(j)|}\,. \tag{4.1}$$

(2) Common Neighbors (CN) (Liben-Nowell and Kleinberg, 2003; Newman, 2001):

$$CN(i, j) = |\mathcal{N}(i) \cap \mathcal{N}(j)|\,. \tag{4.2}$$

(3) Preferential Attachment (PA) (Liben-Nowell and Kleinberg, 2003; Newman, 2001):

$$PA(i, j) = |\mathcal{N}(i)| \cdot |\mathcal{N}(j)|\,. \tag{4.3}$$

(4) Adamic-Adar coefficient (AA) (Adamic and Adar, 2003; Liben-Nowell and Kleinberg, 2003):

$$AA(i,j) = \sum_{x \in \mathcal{N}(i) \cap \mathcal{N}(j)} \frac{1}{\log |\mathcal{N}(x)|} \,. \tag{4.4}$$

4.1.2 Global methods for node similarity

Both the *MN* and *PC* networks are highly sparse and, thus, we expect that the task of predicting edges is hard if we would rely only on local information.

However, both *MN* and *PC* display a very high clustering coefficient (see Table 1.2), which is much higher than that we observe in other types of real-life social networks of roughly equal size. A large clustering coefficient implies that if two nodes i and j share at least one neighbor, then there is a high chance that i and j will be linked by an edge too. Therefore, methods to calculate node similarity which leverage higher order structures (*e.g.*, as walks or paths) or, more in general, the full knowledge of the graph topology, might be more accurate than local methods in predicting edges.

We will call these methods as global methods and one of the most popular global methods is the so called Katz score (Katz, 1953).

The Katz score $\kappa(i,j)$ associated with a pair of nodes i and j considers the whole ensemble of walks connecting i and j, and it assumes that each walk provides a contribution to determine the degree of similarity between i and j. A core assumption in the calculation of $\kappa(i,j)$ is that long walks are to be penalized with respect to short ones, which implies that two nodes are highly similar if they are connected by many short walks in G. To formally encode such a principle, we introduce a discount factor α and we denote $w_k(i,j)$ as the number of walks of length $k = 0, 1, \ldots,$ from i to j. The Katz coefficient score is then computed as follows:

$$\kappa(i,j) = w_0(i,j) + \alpha w_1(i,j) + \alpha^2 w_2(i,j) + \ldots + \alpha^k w_k(i,j) + \ldots = \sum_{k=0}^{\infty} \alpha^k w_k(i,j) \,. \tag{4.5}$$

Observe that $w_0(i,j) = 1$ if and only if nodes i and j coincide, 0 otherwise. If we let $\mathbf{A}$ be the adjacency matrix of G and suppose that α is less than $\frac{1}{\lambda_1}$, λ_1 being the largest eigenvalue of $\mathbf{A}$[1], then the Katz score between any pair of nodes in G can be seen as a matrix $\mathcal{K}_\alpha$, which can be computed as follows:

$$\mathcal{K}_\alpha = (\mathbf{I} - \alpha \mathbf{A})^{-1} - \mathbf{I} \,. \tag{4.6}$$

Here $\mathbf{I}$ is the identity matrix.

In our analysis we considered also Node2Vec (Grover and Leskovec, 2016), a recent but promising approach for embedding graphs onto vectors. More specifically, given a graph $G = \langle N, E \rangle$, Node2Vec seeks at finding out a function $f : N \to \mathbb{R}^k$ where k is a fixed constant and $\mathbb{R}^k$ is the set of k-th dimensional arrays of real numbers. The main requirement we imposed on f is that if two nodes i and j are "close"in G, then their representations $f(i)$ and $f(j)$ should be close in $\mathbb{R}^k$ too. To detect pairs of close nodes, Node2Vec simulates a random walk on G which can be thought as an interpolation of two popular procedures to explore a graph, namely the Breadth First Search (BFS) and the Depth First Search (DFS). More specifically, such a random walk is regulated by two parameters, namely the return parameter p (which specifies the likelihood the random walk will immediately revisit a node) and the in-out

[1] The parameter λ_1 is also known as the spectral radius of $\mathbf{A}$.

parameter q: if $q > 1$, the random walk acts as a BFS because it tends to visit nodes which are close to the currently visited node; vice versa, if $q < 1$, the walk tends to move to nodes that are farther away from the current, thus simulating a DFS.
After applying the Node2Vec algorithm, each node i is associated with a vector $\mathbf{v}_i$ and the similarity of two nodes i and j is defined as the cosine similarity of vectors $\mathbf{v}_i$ and $\mathbf{v}_j$.

A further method to compute node similarity is the Personalized PageRank similarity score (PPR) (Avrachenkov, Chebotarev, and Rubanov, 2019), which is defined in matrix form as follow:

$$PPR_\alpha = (\mathbf{I} - \alpha\mathbf{P})^{-1} \ . \tag{4.7}$$

The matrix $\mathbf{P}$ is a row-stochastic matrix defined as $\mathbf{P} = \mathbf{D}^{-1}\mathbf{A}$: here $\mathbf{D}$ is a diagonal matrix storing the degrees of nodes in G and, $\mathbf{A}$ is the adjacency matrix of G. Therefore, the sum of the elements within each row of $\mathbf{P}$ is 1 and we can interpret $\mathbf{P}$ as the transition probability of a random walk over G in which the random walker, at any step, chooses uniformly at random one of its neighbors.

4.1.3 Our link prediction methods

As a first step of our analysis, we compared local and global methods. Specifically, let $\sigma_{\text{met}}(i, j)$ be the similarity score between a pair of nodes i and j calculated according to the method *met*, where *met* is one of the methods introduced in Subsects. 4.1.1 and 4.1.2. Similarity scores generated by each method were normalized to range from 0 to 1. We claimed that i and j are connected if and only if $\sigma_{\text{met}}(i, j)$ was bigger than a threshold θ and we negated the existence of that edge if $\sigma_{\text{met}}(i, j) < \theta$. In this way, we were able to map continuous similarity scores onto discrete labels (*i.e.*, 0 and 1 to claim/negate the existence of an edge).

We used two metrics to evaluate the level of association between a particular measure of similarity and the existence of an edge: (i) the True Positive Rate (TPR) and (ii) the True Negative Rate (TNR). The TPR measures the proportion between the number of edges that a similarity measure claims exist and the real number of edges. The TNR is the proportion between the number of node pairs that according to a particular similarity measure are not connected and the actual number of pairs of nodes not connected. The TPR and TNR of local methods for a broad range of values of θ are not reported. However, it is instructive to comment the configuration $\theta = 0.5$: here we observed that the TPR of all local methods was around 0 and their TNR were close to 1. Such a result implies that local methods almost always negate the existence of an edge and, thus, due to the sparsity of *MN* and *PC*, their guesses are almost always exact. Of course, local methods fail to identify edges actually existing. The Katz and PPR scores, instead, work much better than local methods. In Fig. 4.1 we plot only the TPR and TNR for Katz score as function of α; similar results hold true for PPR as function of α.

The main conclusions we drew from our analysis are as follows: (i) An increase of α yields a decrease in TPR; (ii) The TNR achieved by the Katz score in *MN* and *PC* is generally very large (bigger than 0.99) even if slightly smaller that achieved by local methods. Specifically, Fig. 4.1 (left panel) indicates the presence of a turning point $\overline{\alpha}$ (with $\overline{a} \simeq 0.52$ in case of the *MN* network and $\overline{a} \simeq 0.44$ in case of the *PC* network) beyond which the TPR quickly drops. The Katz score thus perfectly addresses issues we highlighted above and, with a suitable choice of α, all highly-scored pair of nodes are actually tied by an edge. Such a result agrees fairly well with our model about information flow in criminal networks: criminals often do not communicate

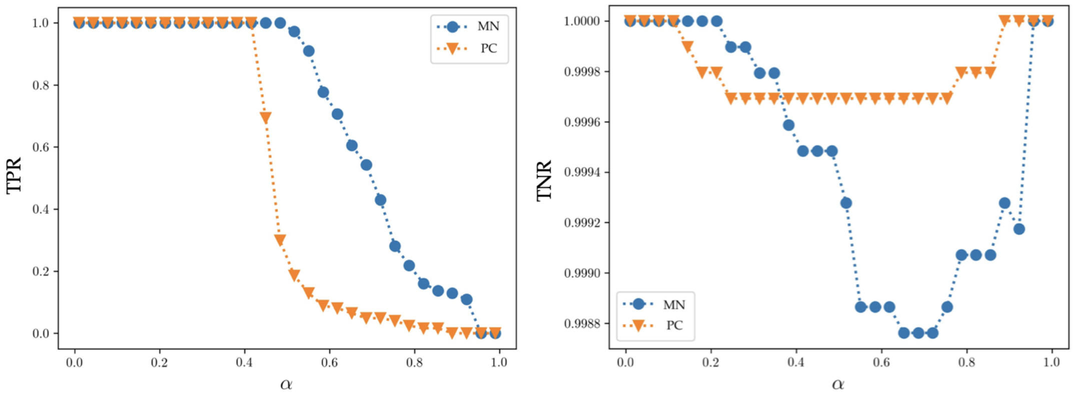

FIGURE 4.1: **Level of association between the Katz score and the existence of an edge in the Montagna Meetings (MN) and Phone Calls (PC) networks.** True Positive Rate (TPR) and True Negative Rate (TNR) associated with the Katz score are represented as functions of the discount factor α in the criminal networks.

directly with each other but they prefer to make use of intermediaries to convey messages, both in face-to-face meetings and in case of phone calls; however, the chain of intermediaries is generally very short for security reasons.

4.1.4 Accuracy of our link prediction methods

As a further step of our analysis, we analyzed the accuracy of the methods to calculate node similarity.

We applied 10-fold cross validation to quantify the predictive accuracy of each previous predictor. Cross-validation is a procedure used to assess the accuracy of a Machine Learning algorithm which, in the latest years, gained an astonishing popularity (Hastie, Tibshirani, and Friedman, 2009). The main reasons underlying the popularity of k-fold cross validation are its simplicity as well as its ability of producing less optimistic accuracy assessment than methods based on the (random) division of a dataset into a training and a test part. In short, in the k-fold cross validation we randomly shuffled a dataset $\mathcal{D}$ and divided it into k groups, say, $G_1, \ldots, G_k$; common choices for k are $k = 5$ and $k = 10$. For each group G_i, we took G_i as test dataset and we used the remaining $G_1, G_2, \ldots, G_k$ groups as training set: in other words, we used all groups G_j (but G_i) to fit our model; once our model had been fitted, we evaluated its accuracy on G_i. Such a procedure was repeated for each group G_i and, consequently, any sample in the original dataset was used $k - 1$ times for training purposes and one time for testing purposes. At the end of evaluation procedure, we obtained k values of accuracy (one for each group used as test set); we thus took the average of the accuracy scores on each group G_i as the accuracy of the algorithm to evaluate.

The prediction accuracy was evaluated by a standard metric, the Area Under the Receiving Operating Curve (AUROC) [2]. We repeated the calculation of AUROC $n = 50$ times, thus generating a sample of the true AUROC scores. Then, we calculated the empirical mean m and the empirical standard deviation s of the sample

[2] The AUROC is understood as the probability that a randomly chosen edge in the test set gets a higher score than a randomly chosen non-edge.

above; if we denote as μ the true AUROC, the random variable $t = \frac{\sqrt{n}(m-\mu)}{s}$ follows a t-student distribution with $n-1$ degrees of freedom (Ross, 2017). We then calculated the value of A for which $P(-A \leq t \leq A) = 0.95$ and we take the interval $\left(m - A\frac{s}{\sqrt{n}}, m + A\frac{s}{\sqrt{n}}\right)$ as the 95% confidence interval associated with the true AUROC score.

In Table 4.1 we report the confidence intervals associated with AUROC for AA, CN, PA, JC, Node2Vec, Katz and PPR methods on the MN and PC networks. We report the AUROC 95% confidence intervals for the Katz and PPR methods. Moreover, we considered some specified values of the parameter α (namely $\alpha = 0.1, 0.3, 0.5, 0.7$ and 0.9), and we investigated how the α parameter affected the AUROC.

TABLE 4.1: Area Under the Receiving Operating Curve (AUROC) confidence intervals for the Adamic Adar (AA), Common Neighbors (CN), Preferential Attachment (PA), Jaccard Coefficient (JC), Node2Vec, Katz ($\mathcal{K}$) and Personalized PageRank (PPR) methods computed on the Montagna Meetings (MN) and Phone Calls (PC) networks.

Method		**Confidence Interval**	
Name	α	**MN**	**PC**
JC		(0.917, 0.938)	(0.57, 0.623)
CN		(0.938, 0.953)	(0.595, 0.634)
PA		(0.754, 0.789)	(0.872, 0.913)
AA		(0.939, 0.957)	(0.602, 0.643)
Node2Vec		(0.899, 0.919)	(0.577, 0.646)
$\mathcal{K}$	0.1	(0.946, 0.959)	(0.706, 0.753)
	0.3	(0.95, 0.965)	(0.711, 0.772)
	0.5	(0.939, 0.955)	(0.701, 0.754)
	0.7	(0.927, 0.946)	(0.73, 0.778)
	0.9	(0.927, 0.946)	(0.696, 0.748)
PPR	0.1	(0.939, 0.956)	(0.66, 0.724)
	0.3	(0.954, 0.968)	(0.696, 0.752)
	0.5	(0.942, 0.958)	(0.698, 0.747)
	0.7	(0.939, 0.955)	(0.687, 0.743)
	0.9	(0.922, 0.94)	(0.688, 0.75)

In case of MN network, the AUROC was generally very high for all methods under investigation and the worst-performing method is PA. The Katz score and the PPR score generally outperformed but their AUROC tended to slightly decrease as α increased: for instance, if $\alpha > 0.7$ the AUROC achieved by Katz score ranges from 0.893 to 0.918 while the AUROC measured for PPR ranges between 0.922 and 0.94. The JC, CN and AA methods achieved an AUROC which was slightly smaller than that of the Katz and the PPR score. In contrast, PA displayed the worst performance, and its AUROC was 17.51% less than that of AA and 17.25% smaller than that of JC.

On the PC network, instead, the PA method achieved the highest AUROC and the performances of all other methods significantly deteriorated. For instance, the AA method achieved an AUROC ranging from 0.602 to 0.643, with a loss of more than 30% with respect to MN.

We observed our methods were very accurate and they achieved an AUROC, which in some cases was higher than 0.9.

We reported that graph topology actually played an important role on the process of predicting edges: specifically, methods which were very accurate on MN

performed badly on PC (and vice versa). In detail, it seems that if a graph is poorly connected (with a low edge density and a small clustering coefficient) local methods are to be preferred to global ones. Vice versa, global methods as the Katz score achieved their best accuracy on graphs which displayed a better level of connectivity (*i.e.*, in graph with larger edge density and clustering coefficients).

4.1.5 Robustness of our link prediction methods

Let us assume that we know all the nodes of a network and do not know a percentage of its edges. This realistic situation must allow us to make predictions about how much the network can help LEAs, even if there are some missing edges.

We used the complete Montagna networks MN and PC to study the usefulness of a partial knowledge of them. To understand if a partial knowledge of the edges is sufficient, we assumed that we did not know a percentage of their edges and applied similarity algorithms for link prediction.

Both MN and PC are built upon the evidence collected by police forces, and therefore they are an incomplete sample of true graphs MN' and PC'. An important discrepancy between MN and MN' (resp., PC and PC') might significantly alter the conclusions we can draw from the analysis of MN (resp. PC), and in particular it might severely alter our ability of predicting edges between criminals.

We ran our analysis in parallel for the two networks MN and PC, and rely on the methods achieving the highest prediction accuracy in the analysis of the previous section: for MN, we concentrated on the Katz score with different levels of parameter α; for PC, we focus on PA.[3] Let us consider the MN network. Our aim was to quantify the difference between $\mathcal{K}_\alpha(MN)$ and $\mathcal{K}_\alpha(MN')$. At an aggregate level, we introduced the parameter $\rho_\alpha(MN, MN')$ to quantify such a difference:

$$\rho_\alpha(MN, MN') = \frac{||\mathcal{K}_\alpha(MN) - \mathcal{K}_\alpha(MN')||_2}{||\mathcal{K}_\alpha(MN)||_2}\,. \tag{4.8}$$

Eq. 4.8 can be applied to networks PC and PC' and method PA, which yielded the highest prediction accuracy in the telephone call network. However, the equation is not applicable in practice because we do not know the true graphs MN' and PC'. We can overcome this issue by assuming that missing edges – those edges in MN' (resp., PC') but not observed in MN (resp., PC) – have been generated using a suitable probabilistic model.

Our probabilistic model assumes that non-observed edges in MN' (resp. PC') are non-edges in MN (resp., PC); each non-edge in MN (resp., PC) is associated with a parameter ℓ, called likelihood, such that the higher the likelihood, the more likely a non-edge in MN (resp., PC) will correspond to an edge in MN' (resp., PC'). If the likelihood ℓ is specified, we can select non-edges from MN (resp., PC) on the basis of their likelihood, and we can incrementally insert them into MN (resp., PC) until a pre-defined stop condition is satisfied. At the end of this procedure, we obtain MN' (resp., PC').

We considered multiple strategies to model the likelihood ℓ, namely: (i) CN (see Eq. 4.2), (ii) JC (see Eq. 4.1), and (iii) a random model, a baseline where ℓ is distributed as a uniform random variable in the interval $[0, 1]$.

The model above resemble network-growth models (Newman, 2010) which describe the creation/evolution of a network (for example, a mechanism similar to the preferential attachment is at the base of the generation of BA networks). However,

[3] For MN, we have also run our analysis in the case of PPR score with similar results.

in network-growth models we assume that new nodes arrive and join the network, and the last node can decide which other nodes to connect to. In contrast, in our model, there are no new nodes that can be added to the network: this is equivalent to the simplifying hypothesis that the network is perfectly observable about what concerns the subjects in it (that is, the investigation has not excluded any criminal subject), and the possible lack of information only concerns the relations observed by the investigators.

Our experimental protocol consisted of the following steps:

Step 1 Let T be the list of non-edges in MN (resp., PC) sorted by decreasing likelihood scores. We took 50% of the top elements in T, *i.e.*, we chose half of the non-edges that have the highest likelihood. This step was necessary to create a group of potential non-edges that was sufficiently large but, at the same time, which was reliable enough because non-edges with low values of likelihood were filtered out. We called $C \subseteq T$ the set of the non-edges generated at the end of Step 1.

Step 2 We randomly chose a sample of $R(p) \subseteq C$ with size equal to p from C. In our experiments, we set $p = \{1\%, 5\%, 10\%, 15\%\}$. Of course, the larger p, the higher the number of missing edges.

Step 3 We add elements in $R(p)$ to MN (resp., PC), thus creating a new graph $MN'(p) = \langle N, E \cup R(p) \rangle$ (resp., $PC'(p) = \langle N, E \cup R(p) \rangle$).

Step 4 We calculate the relative variation ρ using Eq. 4.8, where the graph MN' (resp., PC') is replaced by $MN'(p)$ (resp, $PC'(p)$) .

Steps 2-4 have been repeated 30 times to avoid statistical fluctuations. The results are shown in Fig. 4.2 for MN, and in Table 4.2 and in Fig. 4.3 for PC.

TABLE 4.2: ρ, *i.e.*, the difference among the initial graph and the one with predicted edges, as function of p, *i.e.*, percentage of added edges, in the Montagna Phone Calls (PC) network. Edges are predicted according to Common Neighbors (CN), Jaccard Coefficient (JC), and Random strategies.

p	**CN**	**JC**	**Random**
1.0	0.134	0.107	0.121
5.0	0.157	0.174	0.179
10.0	0.232	0.235	0.201
15.0	0.291	0.296	0.233

As for the meeting network, the random strategy clearly induces the highest values of ρ for any value of α and p. This was a largely predictable result: if the probability of the existence of a non-edge follows one of the other strategies (*i.e.*, JC and CN), then the network structure is somehow able to predict the existence of missing edges. On the other hand, if edges were randomly placed, the network structure would not offer any insight to predict the existence of missing edges and, thus, the parameter ρ significantly grows: for instance, it suffices to set $p = 5\%$ and $\alpha = 0.2$ to obtain $\rho \simeq 1$.

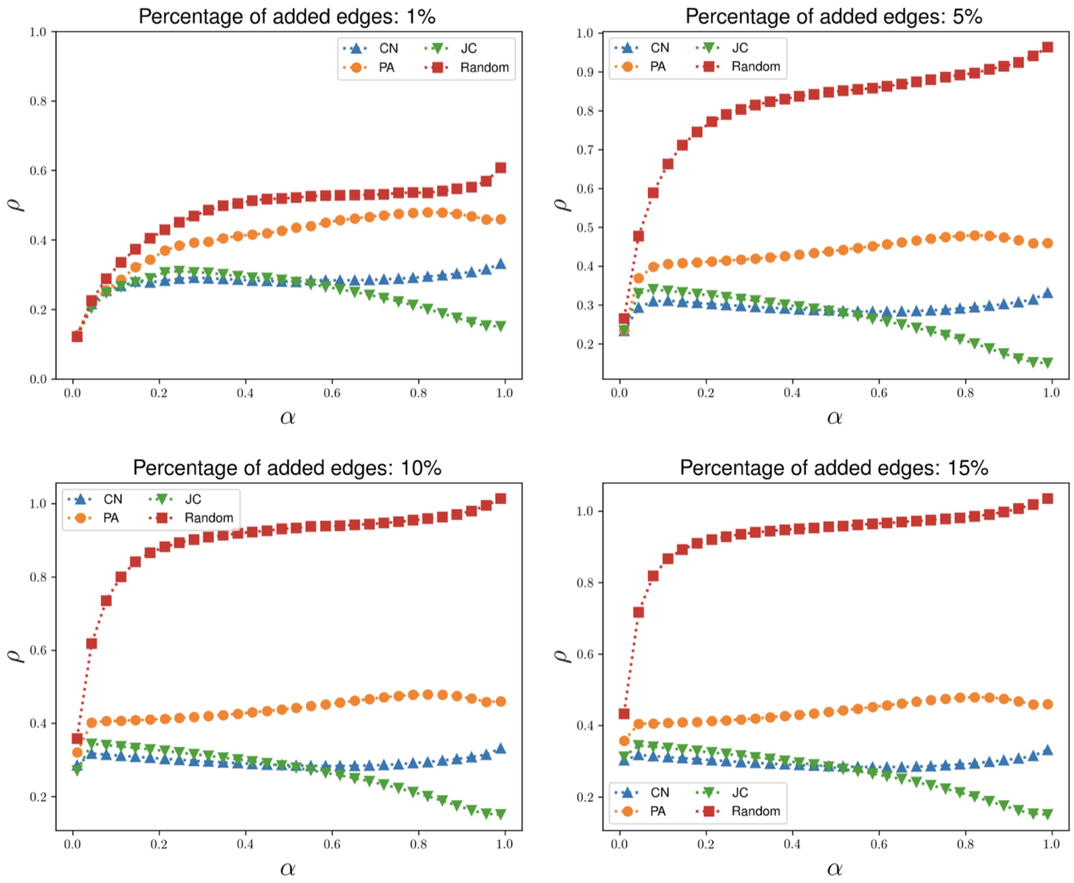

FIGURE 4.2: **Variation of ρ as a function of the discount factor α in the Montagna Meetings (MN) network for $p = 1\%, 5\%, 10\%, 15\%$.** The parameter ρ quantifies the difference between MN and MN' which is created from MN adding a percentage of edges p according to Common Neighbors (CN), Jaccard Coefficient (JC), Preferential Attachment (PA) and Random strategies.

The growth of α implies a growth of ρ for the random strategy. For CN, ρ is relatively stable, only slightly increasing for higher values of α. A limit case happened when we decided to adopt JC as the likelihood function: in that case, the result was anti-intuitive because when α increased, a reduction of ρ occurred (with peaks up to 18%). In practice, if $\alpha \to 1$, the contribution of relatively long walks was not-negligible, and thus long walks were capable of contrasting high level of uncertainty associated with larger values of p. For a fixed α, the parameter p plays a key role on the value of ρ and, obviously, the higher p, the higher ρ.

We obtained totally different results in the PC network. The random and JC likelihood functions were the only strategies that generated the highest value of ρ, and there was a crossover point $\overline{\alpha}$ in the JC likelihood beyond which we observed a variation of ρ greater than that detected in the random generative model. The variations of ρ in the CN generative model become almost imperceptible if α gets larger than 0.1, and thus CN seems an unhappy choice to analyze telephone conversation flows. The trend of ρ is relatively little affected by p if $p < 15\%$; however, if $p > 15\%$ the value of ρ in all the generative models analysed undergoes significant changes.

Link prediction algorithms are sensitive not only to uncertainty in MN and PC (captured by the parameter p) but also on the type of graph they operate on. If

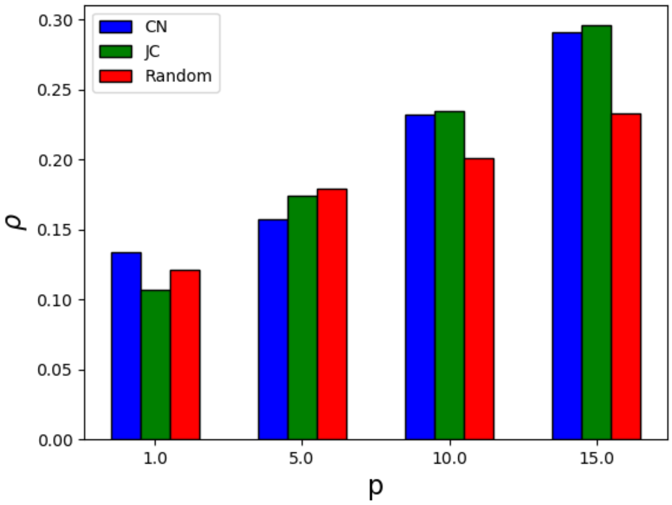

FIGURE 4.3: **ρ as a function of p in the Montagna Phone Calls (PC) network.** The parameter ρ quantifies the difference between PC and PC' which is created from PC adding a percentage of edges $p = 1\%$, 5%, 10%, 15% according to Common Neighbors (CN), Jaccard Coefficient (JC) and Random strategies.

the amount of uncertainty is relatively small, and non-observed edges derive from a specified generative model, we can hope for robust edge prediction. This is confirmed by the results in MN, where both CN and JC generate lower values of ρ than the random strategy for different combination of of p and α. Conversely, there is no clear indication from PC, suggesting that the network growth does not follow a specific strategy. We can thus conclude that the robustness of link prediction is not only dependent on the amount of uncertainty (*i.e.*, p), but also on type of network and underlying relations.

In the light of our studies, we recommend LEAs not only to build a detailed map of connections between criminals, but also to investigate how such a map evolves over time: in this way, we would be able to determine which of the likelihood functions better fit experimental observations, and if required we could design more sophisticated likelihood functions to help LEAs to detect and prevent crimes.

4.2 Graph distances in missing data scenarios

In Ficara et al. (2021c), a network science approach was adopted to assess how much of the available data of a criminal network may be missing, before it starts to be unreliable. In other words, our aim was to quantify how much the partial knowledge of a criminal network can affect investigations in a significant way.

As mentioned in Chap. 3, one of the most interesting SNA application consists of comparing networks, by finding and quantifying similarities and differences between them (Newman, 2018; Peixoto, 2018; Squartini, Mastrandrea, and Garlaschelli, 2015). This network comparisons require measures for the distance between graphs (see Sect. 3.1), such as the adjacency spectral distance d_A, the Laplacian spectral distance d_L, the normalized Laplacian spectral distance $d_{\mathcal{L}}$ and the root euclidean distance $\mathrm{d}_{\mathrm{rootED}}$. In Cavallaro et al. (2021) and Ficara et al. (2021f), some of these measures were exploited to quantify how well artificial (but realistic) models could simulate real criminal networks (see Sect. 3.2). But, graph distances can be also used for different tasks.

In Ficara et al. (2021c), we analyzed the nine real criminal networks described in Sect. 1.3, *i.e.*, Mafia networks, street gangs and terrorist networks.

To quantify the impact of incomplete data, and to determine what kind of network mostly suffers from it, we adopted the following strategy:

(1) We pruned input networks using two specific methods, namely: random edge removal and random node removal.

(2) We compared the original and complete networks to their pruned version through spectral (*i.e.*, d_A, d_L, and $d_{\mathcal{L}}$) and matrix (*i.e.*, $\mathrm{d}_{\mathrm{rootED}}$) graph distances.

4.2.1 Experimental design

We implemented distances to understand the extent by which a partial knowledge of a criminal network may negatively affect the investigations. Since we tried to estimate differences based on the types/amount of data missing, we set up the experiments based on two main strategies: random edges removal and nodes removal. The first case simulates the scenario in which LEAs miss to intercept some calls or to spot sporadic meetings among suspects (*i.e.*, due to the delays in obtaining a warrant). In node removal procedures, the selected nodes are removed along with their incident edges, and afterwards they are reinserted within the networks as isolated nodes. Indeed, the second case models the scenario in which some suspects cannot be intercepted. For instance, if a criminal is known to be a boss but there are not enough proofs to be investigated, then that criminal can be identified as an isolated node with no incident edges. However, node removal is expected to have a greater impact than simple edge removal, since removing a node implies the deletion of all its edges as well.

Note that for a better comparison among the networks, all the graphs were considered as unweighted (as AW and JU). Also, all the suspects showed as isolated nodes of the original network were excluded. In fact, our input parameter was the edge list of the graph, which does not take into account nodes with no incident edges.

Algorithm 1 shows the pseudocode of our approach. The full code is available at `https://github.com/lcucav/criminal-nets/tree/master/missing_data`. In order to obtain the subgraphs, we started from the datasets described in Table 1.1; then, we converted them into graphs (*i.e.*, G) and, lastly, we pruned them (*i.e.*, $G^{'}$) according to a prefixed range of fractions with $0 < torem \leq 10\%$. We opted for the 10% because the criminal networks considered are small, as they have less than 250 nodes. Afterwards, we computed the spectral and matrix distances between the original and the pruned graphs. Each edges removal process was repeated a fixed number of times ($nrep = 100$), and the obtained results were averaged. Thus, the averaged distances values $\langle X \rangle$ and their standard deviations σ were computed.

4.2.2 Node and edge removal effects

The distance analysis between the real and the pruned networks is reported starting from the random edge removal approach (see Fig. 4.4), moving to the analysis on the networks after node pruning (see Fig. 4.5). The plots show the distances between the

Algorithm 1 Pseudocode for computing the distances

```
Input parameters: $data$, $nrep$, $torem$, and $exptype$
Read $data$ and convert it to graph $G$
if $exptype = True$ then
    Isolate $torem$ of nodes
else
    Remove $torem$ of random edges
end if
Compute $S(G)$
Compute the matrices $A(G)$, $L(G)$, $\mathcal{L}(G)$
for $torem$ do
    for $nrep$ do
        Create a pruned graph $G^{'}$ and compute $S^{'}(G^{'})$
        Compute $\mathrm{d}_{\mathrm{rootED}}(G, G^{'})$, $d_A(G, G^{'})$, $d_L(G, G^{'})$, and $d_{\mathcal{L}}(G, G^{'})$
    end for
    Compute $\langle X \rangle, \sigma \; \forall \; d(G, G^{'}) \in nrep$
end for
```

original graphs and their pruned versions up to 10% of edges (F_e) and nodes (F_n), respectively.

In both removal processes, d_A displays a saturation effect that makes the results difficult to be interpreted. Hence, this distance is not effective for highlighting the effects of missing data on criminal networks. Furthermore, from this metric it might seem that the two pruned networks of PK and SN show a greater deviation from their original counterparts, but this is due to the inner structure of this metric, which is highly influenced by the node degree. In fact, the average degree of PK and SN (see Tables 1.3 and 1.4) is significantly higher (*i.e.*, $\langle k \rangle \simeq 21$) than the other networks herein studied (*i.e.*, $1 < \langle k \rangle < 4$); moreover, their different topology is also evident from their degree distribution (see Fig. 1.3). This is the reason why these networks seem to have a more significant detachment effect than others; however, they too suffer the saturation effect mentioned above as they grow. A similar behavior has also been encountered in d_L and its explanation is the same.

On the other hand, the distance metric which more effectively catches the damage caused by a significant amount of missing data is $d_{\mathcal{L}}$, where distance growth is linear. Indeed, the effects of $\langle k \rangle$ are smaller as this aspect is compressed by the structure of this distance metric. It would seem that this metric is the most effective measure compared to other spectral distances, in understanding how much lacking data affects the total knowledge of the network. A similar trend was also found in $\mathrm{d}_{\mathrm{rootED}}$; however, for a better comparison between node and edge removal processes, we analyzed in more detail this last metric by considering the DELTACON similarity sim_{DC}. Fig. 4.6 shows the difference between the original and pruned networks as the fraction of elements removed increases (*i.e.*, F_e for edges and F_n for nodes). Before pruning the networks, we have $sim_{DC} = 1$. Afterwards, the drop begins to become more evident as the fraction F increases. In addition, as expected, the node removal process affects more significantly the networks. This means that if the lack of data relates to sporadically missed wiretaps, or to just a few random connections between suspects, then the network structure is not as much misinterpreted as if the case when one suspect has not been tracked at all. Indeed, pruning the network by 2%, causes a $sim_{DC} \geq 0.8$ for edge pruning, compared to a $sim_{DC} \simeq 0.2$ for the nodes

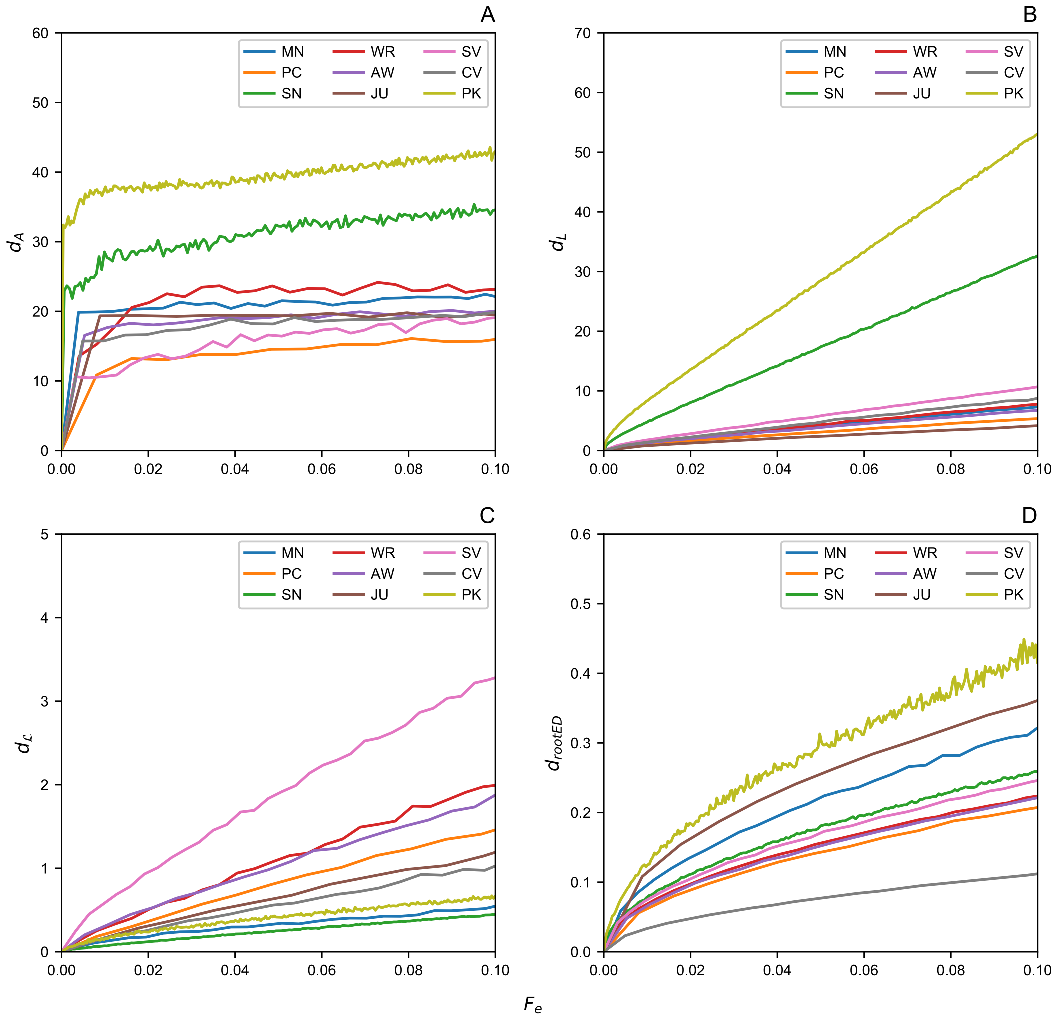

FIGURE 4.4: **Matrix and spectral graph distances after random edge removal in covert real-world networks.** Adjacency spectral distance d_A, Laplacian spectral distance d_L, the normalized Laplacian spectral distance $d_{\mathcal{L}}$ and root euclidean distance $\mathrm{d}_{\mathrm{rootED}}$ are represented as functions of the fraction of removed edges F_e in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW), Judgment (JU), Surveillance (SV), Caviar (CV) and Philippines Kidnappers (PK) networks.

ones. Therefore, even when a small amount of suspects are not included in the investigations, this can lead to a very different network. The exclusion of the suspects could be voluntary or not. It highly depends on the overall investigation process, starting from the very preliminary analysis, and up to the judges' decision to allow warrants, or to exclude data considered irrelevant for the current investigation.

Our analysis suggests that:

(1) the spectral metric $d_{\mathcal{L}}$ is best at catching the expected linear growth of differences with the incomplete graph against its complete counterpart;

(2) the node removal process is significantly more damaging than random edge removal because of the edges that are removed as a result, which makes it difficult to quantitatively compare the two types of experiments.

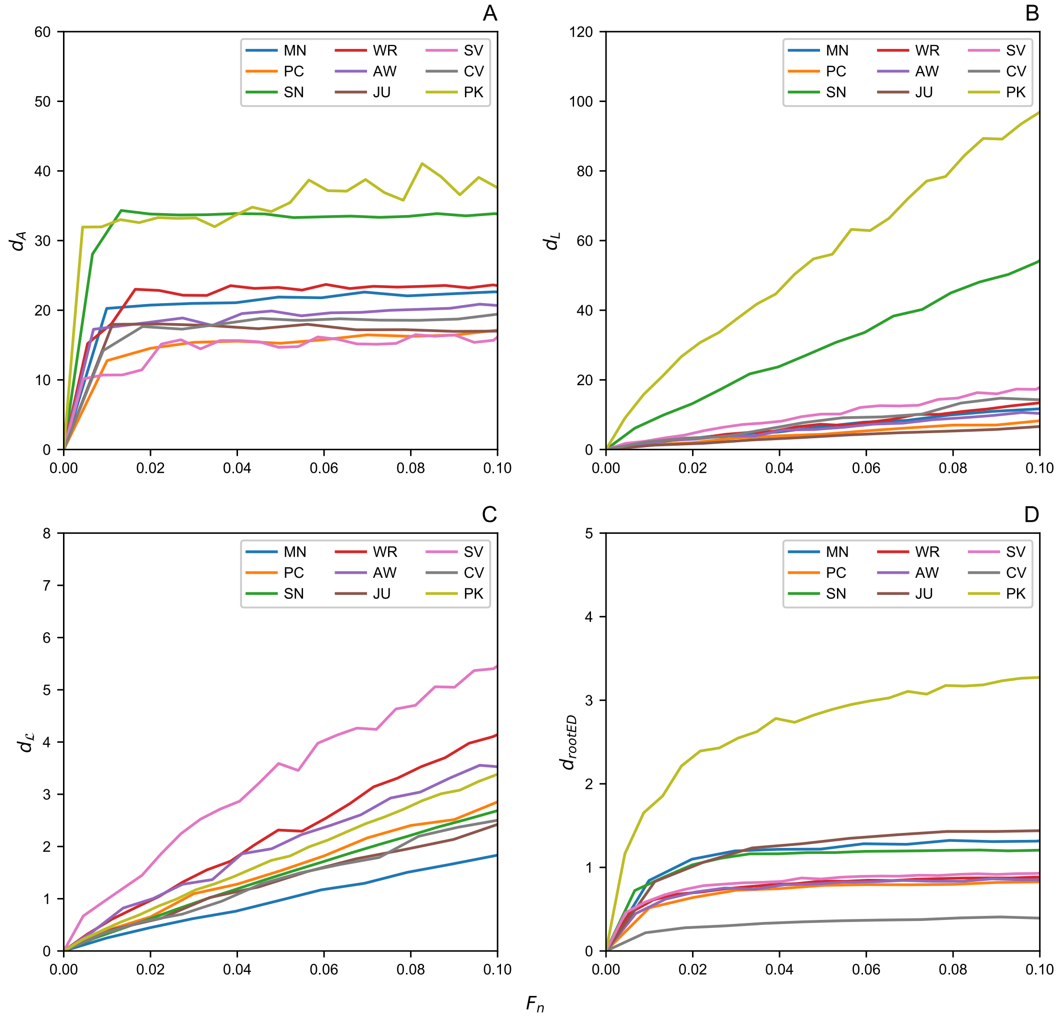

FIGURE 4.5: **Matrix and spectral graph distances after random node removal in covert real-world networks.** Adjacency spectral distance d_A, Laplacian spectral distance d_L, the normalized Laplacian spectral distance $d_{\mathcal{L}}$ and root euclidean distance $\mathrm{d}_{\mathrm{rootED}}$ are represented as functions of the fraction of removed nodes F_n in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW), Judgment (JU), Surveillance (SV), Caviar (CV) and Philippines Kidnappers (PK) networks.

This translates to a negligible error in terms of graph analysis when, for example, some wiretaps are missing. Indeed, in terms of sim_{DC} drop, there is a 30% difference from the real network, for a pruned version at 10%. On the other hand, it is crucial to be able to investigate the suspects in a timely fashion, since any exclusion of suspects from an investigation may lead to significant errors (due to substantial differences from the actual network) - we observed drops of up to 80% of sim_{DC} on some networks.

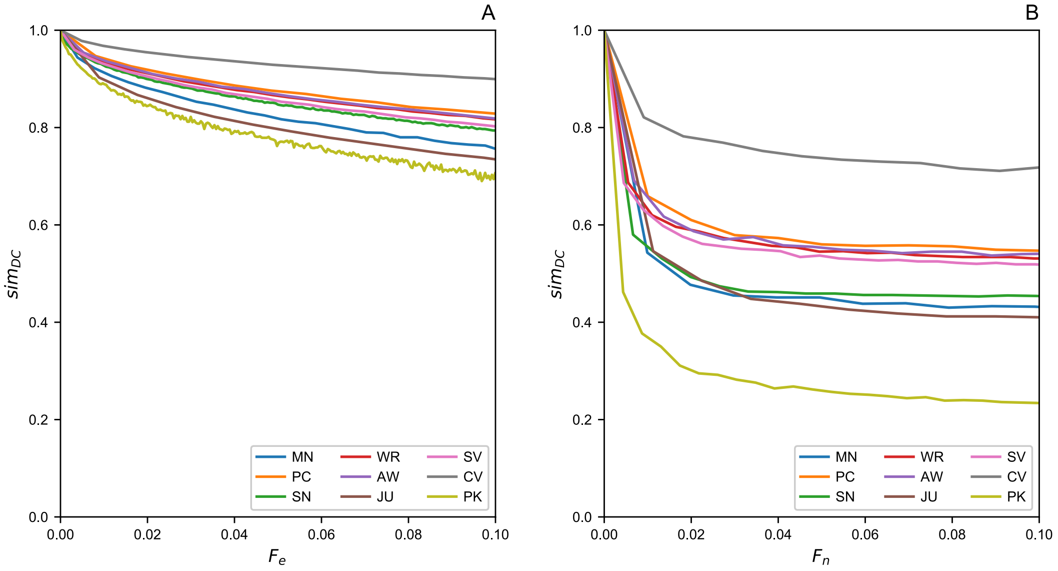

FIGURE 4.6: **DELTACON similarity after edge and node removal in covert real-world networks.** DELTACON similarity sim_{DC} is represented as a function of the fraction of removed edges F_e (left column) and the fraction of removed nodes F_n (right column) in Meetings (MN), Phone Calls (PC), Summits Network (SN), Wiretap Records (WR), Arrest Warrant (AW), Judgment (JU), Surveillance (SV), Caviar (CV) and Philippines Kidnappers (PK) networks.

Chapter 5

Disruption and resilience

5.1 Covert network disruption

The aim of criminal intelligence is to allow the police to disrupt the structure and working mechanisms of groups of individuals engaged in criminal activities.

According to Strang (2014), there are two core questions that an intelligence professional should pose when applying network analysis to disrupt organized crime:

(1) How does the organization operates?

(2) How could it be broken?

SNA allows to discover which individuals of the organization are most important, and to produce targeted recommendations for intelligence collection and operational disruption. Other tools such as value chains, production chains, attack preparations, and other criminal conspiracies have given practitioners insights into core activities of criminal and terrorist organizations, and have assisted at identifying their crucial requirements and potentials. In order to be successful at disrupting organized crime, the aim is to disrupt their activities (Strang, 2014). For instance, the Sicilian Mafia would stop to be a problem if it maintained its structure turning into a social club, rather than being an economic organization based on looting, coercion, and other illegal activities.

We can distinguish three indicators of destabilization for a criminal or terrorist organization (Duijn, Kashirin, and Sloot, 2014):

(1) a reduction of the quantity of the information that circulates in the organization;

(2) a reduction of the capacity to exercise its functions;

(3) a collapse or a significant decline of the decision making process (Carley, Lee, and Krackhardt, 2001).

The three steps above can summarize the disruption of criminal and terrorist associations as the incapacity to diffuse information, goods and knowledge in an efficient way (Carley, Reminga, and Borgatti, 2003). The term information refers to information and resources to flow through the organization. The term knowledge refers to skills, competences and expertise into a specific job of a specific member of the organization.

Generally, disruption strategies can be categorized into two main techniques (Duijn, Kashirin, and Sloot, 2014): the human capital approach and the social capital approach (McCarthy and Hagan, 2001). The combination of the two gives rise to a third one: the mixed approach. These strategies can be applied on covert networks (*i.e.*, criminal and terrorist), which are built from law enforcement data considering social relationships in terms of network theory (see Sect. 1.1).

In Ficara et al. (2022a), we provided a systematic organization of the most significant works about covert network disruption and resilience, described the main approaches, and summarized the key references in relation to this research field (see Table 5.1).

TABLE 5.1: Key references about techniques in covert network disruption.

Approach	Key concepts		References
Human capital	Substitutability		Sparrow, 1991
	Value chain		Gottschalk, 2009
	Crime script analysis		Cornish, 1994; Dehghanniri and Borrion, 2021
	Crime and human capital accumulation		Brown and Velásquez, 2017
Social capital	Social network analysis	Degree centrality	Sparrow, 1991
		Betweenness centrality	Sparrow, 1991
		Closeness centrality	Krebs, 2002
		Eigenvector centrality	Hutchins and Benham-Hutchins, 2010
		PageRank centrality	Singh, Verma, and Tiwari, 2020
		Katz centrality	Cavallaro et al., 2020b
		Collective influence	Cavallaro et al., 2020b
		Network capital	Schwartz and Rouselle, 2009
		Attribute gravity centrality	de Andrade et al., 2021
		Energy disruptive centrality	de Andrade et al., 2021
	Order theory		Farley, 2003
Mixed	Combination of human and social capital techniques		Duijn, Kashirin, and Sloot, 2014 Bright et al., 2017 Villani, Mosca, and Castiello, 2019

5.1.1 The human capital approach

Human capital is defined by the Organization for Economic Cooperation and Development (OECD) as «the knowledge, skills, competencies and attributes embodied in individuals that facilitate the creation of personal, social and economic well-being» (Keeley, 2007).

The economic concept of human capital showed up in the earlier years of the 20th century in the studies of the Scottish economist Adam Smith, but it wasn't really until the 1960s that economists systematically began to incorporate this idea into their work. In those years, some economists like Theodore Schultz began to use the metaphor of "capital" - an economic concept of long standing date - to explain how education and expertise contributed to prosperity and the economic growth. They argued that people who invest in their education and training build a stock of skills and capabilities (a capital) that will pay off in the long term. Such an investment can also be profitable for national economies and helps to fuel economic growth. Usually, human capital is defined in a broad sense as a mix of: (i) skills and innate individual skills, and (ii) competences and knowledge acquired at school, and in courses of vocational training. Sometimes, health is also included in the definition of the human capital. The world of industry, which adopted with enthusiasm this concept, tends to give it a more restrictive meaning, considering it mainly as a set of skills and talents of the workforce that contributes directly to the economic success of the company or one specific sector of industry.

The strength of a criminal organization, as for a company, depends on the human capital of their members which includes their knowledge, skills, competences, and expertise into a specific job. Criminal organizations are increasingly infiltrating very specialized areas of activity that require particularly important advisory services, skills, and expertise. These may include pharmacological and chemical knowledge needed, for instance, in synthetic drug synthesis productions, or the skills of civil servants who are able, through technical suggestions, to facilitate the award of public contracts to companies close to criminal organizations. The removal of such important human capital individuals could cause a weakening of the resilience of criminal organizations, as their elimination is not easily replaceable with other individuals (Duijn, Kashirin, and Sloot, 2014; Robins, 2009; Sparrow, 1991). Sparrow (1991) suggested that a great opportunity to damage a criminal network is represented by the identification of subjects who own many resources or present specialized skills or can have access to scarce resources. He explained the concept of substitutability which is an important criterion for network disruption. The removal of subjects with specific skills leads indeed to major consequences inside the criminal network, if compared to the removal of ones who are instead concerned with more general tasks and roles.

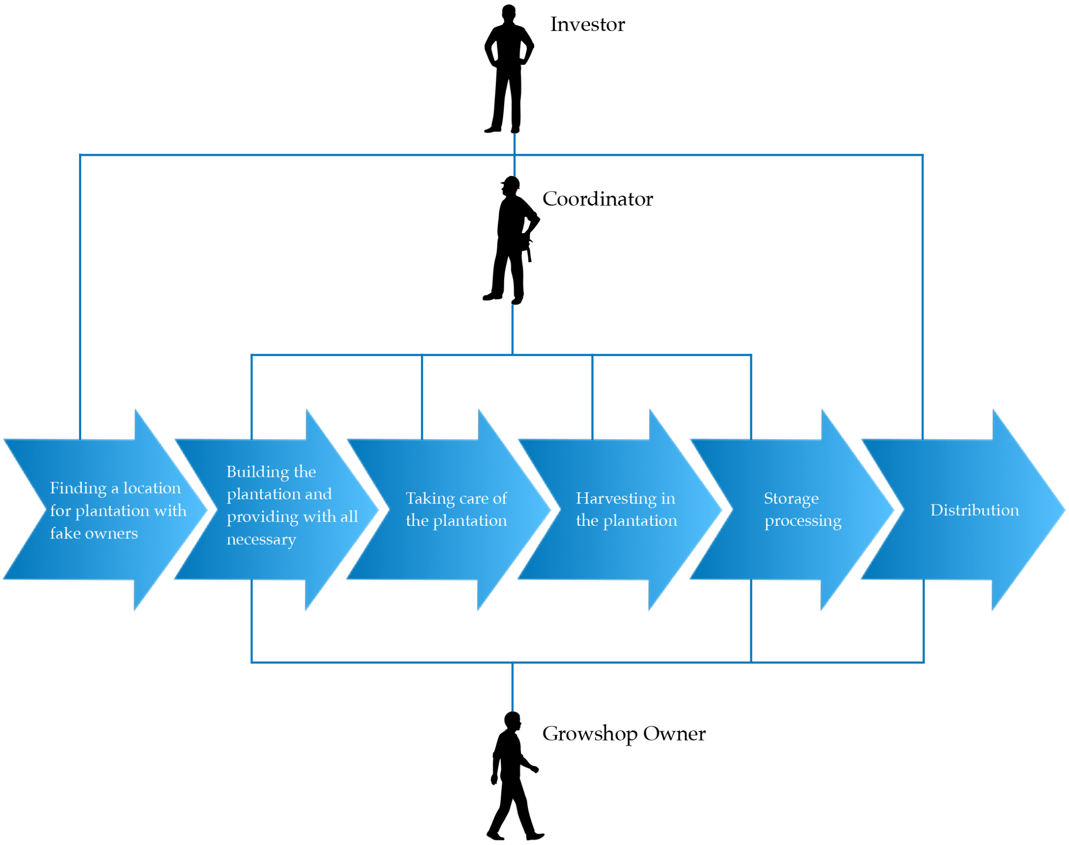
Investor
Coordinator
Finding a location for plantation with fake owners
Building the plantation and providing with all necessary
Taking care of the plantation
Harvesting in the plantation
Storage processing
Distribution
Growshop Owner

FIGURE 5.1: Crime script of cannabis cultivation.

If we think about criminal markets, each of them involves a business procedure that is made of several stages of production and activity (Klerks, 2003; Morselli, 2008; Spapens, 2011). Just as in a typical chain structure, different kinds of information, goods and human capital are exchanged at each step of the process and added to the next one. For this reason the whole process can be considered a value chain in all respects (Gottschalk, 2009). Based on the distinct features of the illegal activity, a distinct radius of both skills- and knowledge-based human capital is necessary at each stage of the value chain (Bruinsma and Bernasco, 2004; Cornish, 1994; Morselli and Roy, 2008). Duijn, Kashirin, and Sloot (2014) offered an example of the value chain units in case of organized cannabis cultivation (see Fig. 5.1). Primary activities in this value chain are:

(1) finding location;

(2) building;

(3) taking care;

(4) harvesting;

(5) storage and processing;

(6) distribution.

Within this system there are some roles, such as the coordinator and the growshop owner, who administer the majority of the steps of the value chain. Since they even gather the right roles at the right place and time, they function as criminal brokers (see Fig. 5.1), making their roles, under a human capital point of view, extremely vulnerable in terms of disruption.

An important method to identify high human capital actors within criminal value chains is the crime script analysis. Cornish (1994) introduced the notion of the script which if correctly identified can prevent or disrupt crime commission. The script is an event schema which organizes knowledge about how to understand and enact commonplace behavioral processes or routines. For example, a robbery script can be realized taking into account the crime setting, the entry to the setting, the awaiting or establishment of conditions under which the crime in question is committed. Information about preparations or aspects of the offense's aftermath are often missing, and can be identified through the script. In this way, it is possible to find motivation and purpose that together with origins or development are important to understand the crime-commission act and its goals. Then, crime script analysis showed to be an important method to identify high human capital actors within criminal value chains. In the case of an organized cannabis production, crime script analysis allowed to describe all the tasks, roles, information, and resources involved in the value chain for such a delicate business process (see Fig. 5.1).

5.1.2 The social capital approach

Social capital may have first appeared in a book published in 1916 in the United States that discussed how neighbors could work together to oversee schools. In it, Lyda Hanifan referred to social capital as «those tangible assets that count for most in the daily lives of people: namely goodwill, fellowship, sympathy, and social intercourse among the individuals and families who make up a social unit» (Keeley, 2007).

We can think of social capital as the links, shared values and understandings in society that enable individuals and groups to trust each other, and so work together. Social capital can take various forms which can be divided into three main categories: bonds, bridges and linkages (Keeley, 2007). Bonds are links to people based on a sense of common identity (*i.e.*, people like us) such as family, close friends and people who share our culture or ethnicity. Bridges are links which stretch beyond a shared sense of identity (*e.g.*, to distant friends, colleagues and associates). Linkages are links to people or groups further up or lower down the social ladder.

The creation of competitive advantages through social connections is the key for a criminal organization (just as it is for a company) to be successful in achieving goals which would not be feasible in its absence (Coleman, 1990). It is indeed clear that criminal organizations are heavily based off social ties, connections and the capacity of retrieving resources to accomplish their tasks (van der Hulst, 2009). Such ties make it possible for actors in strategic positions to exchange and share resources with other individuals within the organization (Bouchard, 2020; Bouchard and Malm, 2016; Burcher, 2020; Campana, 2016; Ficara et al., 2021e; Klerks, 2003; Natarajan, 2006).

Research in this field is commonly based on SNA which considers social relationships in terms of network theory (see Subsect. 1.1.3). SNA can be used to evaluate LEAs interventions aimed at dismantling and disrupting covert networks because it allows to identify central actors, *i.e.*, the ones involved with significant and powerful positions of social capital (Duijn, Kashirin, and Sloot, 2014; Lin, Cook, and Burt, 2001).

As mentioned in Chap. 2, there are several reasons for an actor to be central within a network and centrality can be measured in many ways through SNA. DC and BC are the most common centrality measures to find strategic positions within a covert network (Klerks, 2003; Sparrow, 1991).

High degree actors possess higher social capital because they can exchange more information and resources than actors with fewer ties. They are also called hubs since they are relevant in order for information and resources to flow through the network. As stated by Peterson (1994), an high degree centrality value can be a sign of vulnerability instead of strength. He argued that the most central actors in covert networks could be the most likely to be detected if they were the most visible. Fig. 5.2 shows a simulation of the fragmentation of the Montagna MN (see Subsubsect. 1.3.1). At each step, the actor with maximal DC (marked in red) is removed.

As opposed to high degree actors, high betweenness actors occupy strategic positions within the network due to their ability to transfer and exchange of resources (Burt, 2007; Burt, Jannotta, and Mahoney, 1998; Morselli, 2010). They are called brokers and connect criminal networks linking criminal collectives within illegal markets (Morselli, 2001, 2008; Morselli and Roy, 2008; Natarajan, 2006). Fig. 5.3 shows another simulation of the fragmentation of the Meetings network. This time, at each step, the actor with maximal BC (marked in brown) is removed.

Berlusconi (2017) discussed the network approach to study crime and the different fields of application of SNA in the criminologist context. She described how SNA can be considered not only a valuable tool for research purposes but it can also help LEAs in their investigations. However, there are some cases in which traditional methods to target leaders in criminal networks are not applicable (*e.g.*, loose networks of collaborating criminals). In fact, the leader removal does not automatically lead to the vulnerability of a criminal organization, or its disruption, because the effects of LEAs targeting can be reduced by the network flexibility (Bright, Greenhill, and Levenkova, 2013; Carley, Reminga, and Borgatti, 2003; Morselli and Petit, 2007). Hence, the impact of LEA interventions is not always effective, for instance when it leads to better adaptation strategies by the targeted criminal group (rather than disrupting the network) (Ayling, 2009).

We also made a study (Cavallaro et al., 2020b) borrowing methods and tools from SNA to unveil the structure and organization of Sicilian Mafia gangs, based on the Montagna dataset (see Subsubsect. 1.3.1), and gain insights as to how to reduce the size of the *lcc* (see Subsect. 1.1.3) of our Mafia networks. We employed four different centrality metrics (see Sect. 2.1) to identify the actors having a high level of social

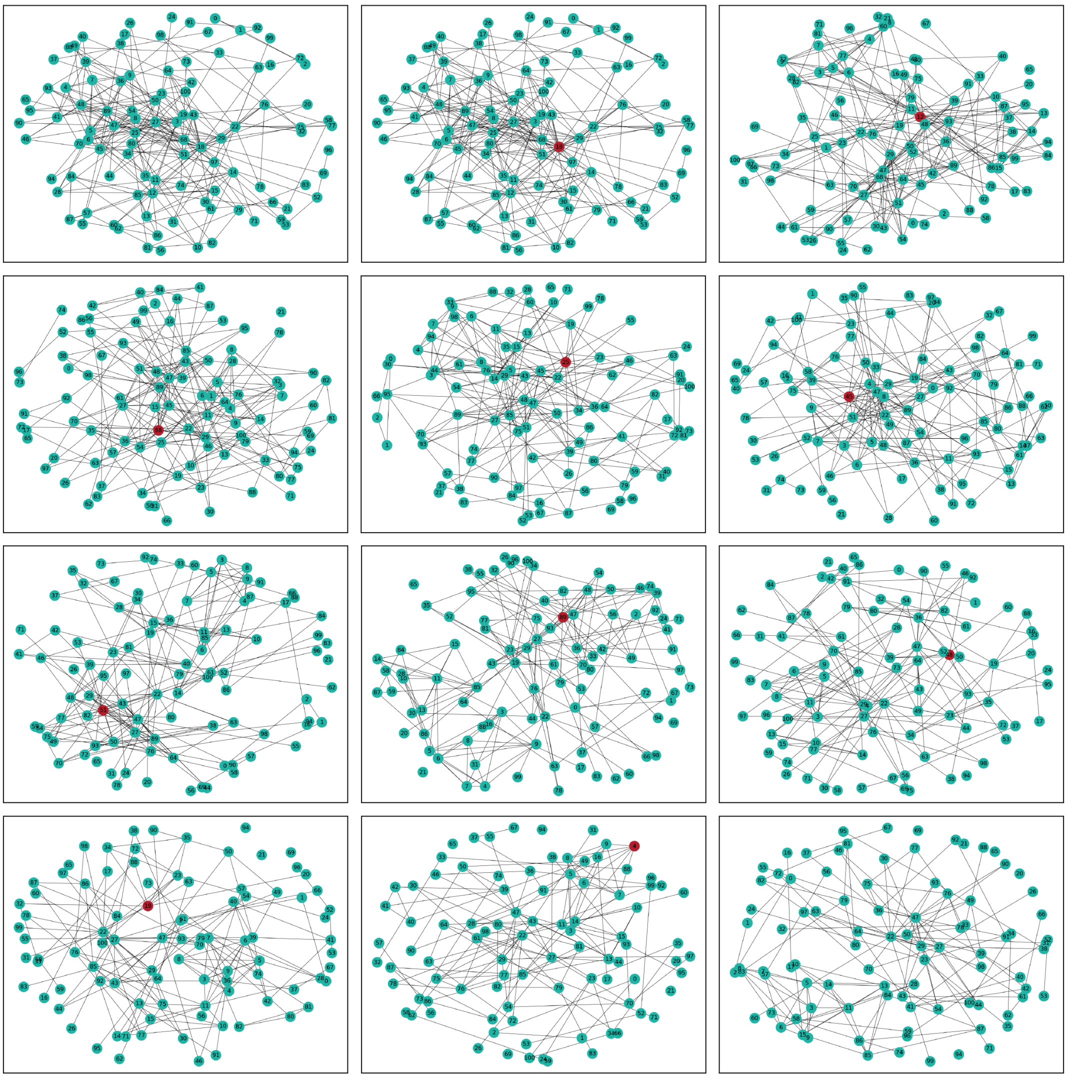

FIGURE 5.2: **Removal of the 10 most important nodes according to degree centrality in the Montagna Meetings network**. The first picture shows the complete network. Then, at each step the node with the highest value of degree centrality is marked in red and, then, removed. The last picture shows the network without its 10 most central nodes.

capital: DC, BC, Katz centrality and the collective influence. The removal of key actors increased the *lcc* size drop inside the networks, which was our aim.

5.1.3 The mixed approach

The mixed approach consists in the use of disruption strategies which are characterized by a combination of social capital (*i.e.*, SNA metrics) and human capital (*i.e.*, special abilities or competence and the supposed substitutability within the value chain). Regarding the human capital, nodes can also be targeted based on the highest value chain degree within the network (Duijn, Kashirin, and Sloot, 2014), which is measured by the amount of edges defined within the social system of the value chain configuration (see Fig. 5.1). This strategy refers to the LEA ability to identify actors who have a great reputation. These actors could commit to other and various

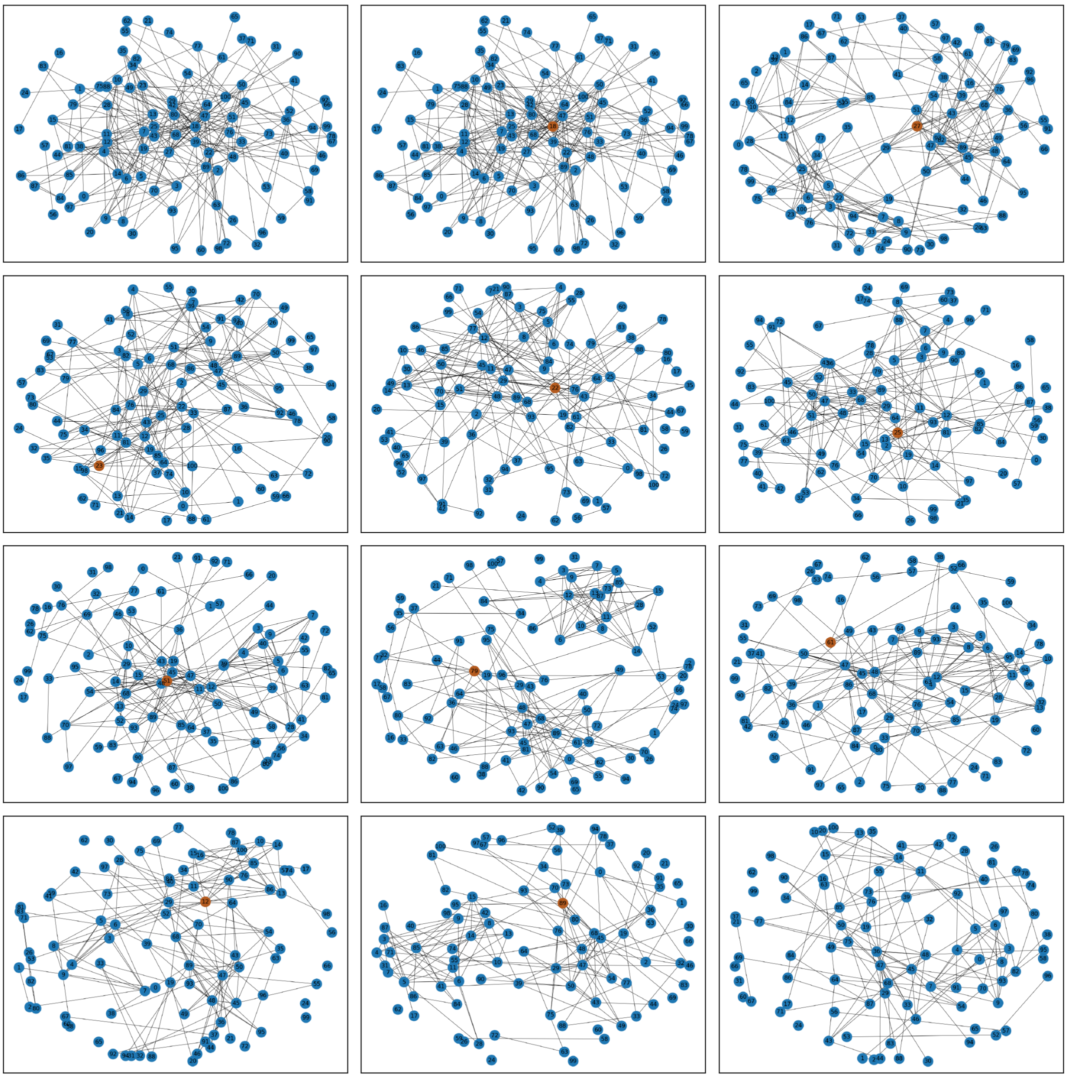

FIGURE 5.3: **Removal of the 10 most important nodes according to betweenness centrality in the Montagna Meetings network**. The first picture shows the complete network. Then, at each step the node with the highest value of betweenness centrality is marked in brown and, then, removed. The last picture shows the network without its 10 most central nodes.

value chains within the value chain network as well. This means that they could be the most visible within the network, and therefore they could have a higher DC. Robins (2009) emphasized on the interaction between the characteristic of network topology and the factors at an individual level. Knowledge, skills, information, expertise, and all the other qualities of individual actors are essential to understand the complex dynamics of criminal networks.

Morselli and Roy (2008) analyzed two stolen-vehicle exportation operations (*i.e.*, Siren and Togo) within a framework which merged SNA and crime script analysis, to examine the impact that brokers have on crime commission processes. In fact, key players in criminal organizations do not maintain authoritarian roles, but instead maintain brokerage positions that: (i) bring flexibility, integration, and creativity to the ensemble of an organization, and (ii) benefit the individuals occupying such positions (Burt, 1992). A broker occupies a position between disconnected nodes within a network. These disconnected nodes may be members of different criminal organizations working together for a given operation. They also may have a hierarchical role within the criminal organization. Brokers are at first identified through crime script analysis, which has as main objective to untangle how some participants (*i.e.*, the brokers) in criminal activities contribute in varying degrees to keeping the inherent channels of a script in place. Then, they used two brokerage indicators from SNA: BC and brokerage leverage (Gould and Fernandez, 1989). Their framework and results are particularly useful for research on disruption strategies in various criminal networks, and for direct applications in law-enforcement settings.

Duijn and Klerks (2014) focused on a cannabis cultivation network called the Blackbird crime network, illustrating the potentiality of the combination of SNA and crime script analysis. The authors defined the topology of the Blackbird network and its substructures, and exposed the key actors using a mix of qualitative and quantitative analysis. They showed how analysts and informant handlers could work together developing a better understanding of the strategies to target key individuals, and discover access points to criminal communities and markets. In another work, Duijn, Kashirin, and Sloot (2014) extracted a criminal network from unique data from the Dutch Police discovering that targeted attacks could make criminal networks even stronger. Their results emphasized the importance of criminal network interventions at an early stage, before the network gets a chance to re-organize to maximum resilience. Disruption strategies such as the social and human capital approaches force criminal networks to become more exposed, which causes successful network disruption to become a long-term effort. Duijn and Sloot (2015) also explained how LEAs are seeking for more proactive strategies in targeting these criminal network structures more effectively. This starts with a better understanding of the way they operate and adapt over time. A key element to developing this understanding remained largely unexploited: big data and big data analytics. This provides novel insight into how criminal cooperations on a micro and meso level are embedded in small-world criminal macro-networks, and how this fosters its resilience against disruption.

Bright et al. (2017) explored the validity of five LEA interventions in dismantling and disrupting criminal networks. They tested three LEA strategies targeting social capital and two interventions targeting human capital in criminal networks. The authors identified the actor removal based on BC as the most efficient strategy. In fact, this strategy led to network disruption in few steps, which was relatively consistent across all their experiments.

Villani, Mosca, and Castiello (2019) tried to check if, and to which extent, contrasting strategies based on human capital may be used in combination with the strategies based on social capital to reduce or neutralize the resistance and adaptation abilities of criminal organizations. The elements that influence the resilience ability of a criminal network are various, such as the knowledge, skills and technical abilities available in the network, that translate into the available human capital. Since their importance is often underestimated or ignored, the adoption of new and diversified repression policies based on both human and social capital could be profitable to develop a valid resilience index.

5.2 Covert network resilience

Covert networks might be able to withstand or absorb disruption adapting to changes when necessary - that is referred to as network resilience (Duijn, Kashirin, and Sloot, 2014). More precisely, these networks develop the above abilities as a consequence of being disrupted. Key references in relation to this research field are summarized in Table 5.2, as we discuss next.

TABLE 5.2: Key references about covert networks resilience.

Resilience	Description	References
Key concepts	Definition	Norris et al., 2008
	Characteristics	Ayling, 2009; Bouchard, 2007
	Efficiency/security tradeoff	Morselli, Giguère, and Petit, 2007
	Redundancy	Williams, 2001
	Non-redundancy	Duijn, Kashirin, and Sloot, 2014
Case studies	Illegal drug markets	Bouchard, 2007
	Terrorism	Kenney, 2007
	Street gangs	Ayling, 2009
	People smuggling	Munro, 2011
	Police corruption	Lauchs, Keast, and Chamberlain, 2012
	Rhino horn trading	Ayling, 2013
	Cannabis cultivation	Duijn, Kashirin, and Sloot, 2014
	Mafia	Catanese, De Meo, and Fiumara, 2016
	Financial crimes	Hardy and Bell, 2020

The term resilience has first been used in physics and mathematics to illustrate the ability of certain materials to resume their original shape after external strain actions (Ayling, 2009; Catanese, De Meo, and Fiumara, 2016; Norris et al., 2008; Oliver et al., 2014); but it was actually Holling who introduced the concept of resilience in an ecological context (Ayling, 2009; Holling, 1961). This concept has since been applied to describe the adaptive capacities of individuals (Bonanno, 2004), human communities (Kulig et al., 2013), and larger societies (Adger, 2000). There are many ways to define resilience (Norris et al., 2008). The most common definition is the adaptive capacity in disturbance, stress, or adversity situations. The difference between resistance and resilience in mathematics and technology has been widely discussed. Given a system which has to return to equilibrium, resilience refers to the time required to achieve the purpose, while resistance refers to the force required to displace the system from equilibrium (Bodin and Wiman, 2004). Across these definitions, all the scientists agree on two key points about the concept of resilience:

(1) it refers more to an ability or process than an outcome (Pfefferbaum et al., 2007);

(2) it refers more to adaptability than stability (Handmer and Dovers, 1996).

The increasing awareness of the business vulnerability to threats such as natural disasters, accident and employee/management error, neglect or recklessness, terrorism or cybercrime has brought the attention on the concept of resilience also in organizational literature and business circles (Ayling, 2009). An organization is resilient if it is able to change its operations and objectives to survive during a state of chaos (Ayling, 2009; Lengnick-Hall and Beck, 2005).

As mentioned at the beginning of Chap. 1, Morselli, Giguère, and Petit (2007) criminal and terrorist organizations are characterized by a different time-to-task, which is long for the former and limited for the latter. Moreover, criminal organizations are more flexible and agile being able to quickly adapt to external shocks. This flexibility is fundamental for criminal network resilience against dismantling attempts.

5.2.1 The characteristics of resilient criminal organizations

Illegal drug markets

Bouchard (2007) analyzed the concept of resilience to understand the impact of repressive policies on illegal drug markets. According to him, three main characteristics should be considered to determine if a system is resilient:

(1) vulnerability;

(2) elasticity;

(3) adaptive capacity.

The vulnerability to attacks refers to the degree to which a criminal organization is likely to be damaged by an external shock (Luers et al., 2003). It first depends on the organization level of exposure to attacks (*i.e.*, on its capacity to protect itself or hide from attacks). For example, an illegal drug market will suffer weaker external shocks if the police have to make a great effort to seize drugs or to arrest a dealer (Bouchard, 2007). If the criminal organization cannot absorb an external shock without compromising its functioning, then it has to use its elastic properties to recover. Elasticity refers to the efficiency of the organization to return to its original state after an external shock (Gunderson and Holling, 2001). The organization can go back to function properly using its elasticity, and replacing what has been removed by the external shock. Illegal drug markets possess elasticity if they are able to replace specific drug dealers or drug quantities seized by LEAs (Bouchard, 2007). A criminal organization may not necessarily use a recovery process to return to its original state, but it may adapt its structure. The adaptive capacity of the organization consists in the possibility to make its components less vulnerable modifying its circumstances (Luers et al., 2003). Adaptation is considered as an option only when recovery is too difficult to achieve or it is not possible because it is more demanding than recovery. In illegal drug markets, adaptation can happen in a variety of ways: drug dealers can change the location of transactions; or drug producers can make their sites less vulnerable to detection changing their production methods.

Consequently, covert networks show resilience to attacks when they possess either one of the mentioned features (*i.e.*, vulnerability, efficiency and adaptation) or a combination of them. The most resilient network will show a tendency towards all three characteristics (Bouchard, 2007).

Street gangs

Ayling (2009) explained the characteristics of resilient licit organizations, which include:

(1) approach based on capabilities;

(2) planning of strategic scenario;

(3) good communication within the organization;

(4) good communication with key stakeholders;

(5) sharing of the same vision, sense of purpose and set of values;

(6) distributed power;

(7) inbuilt redundancy;

(8) bricolage;

(9) inspirational, enthusiastic and intellectually stimulating leaders;

(10) capacity for effective organizational learning.

According to the author these characteristics cannot simply be applied to illicit organization because licit and illicit organizations have some differences which have implications for their resilient characteristics. Criminal organizations in fact operate against the state (Paoli, 2002) and constantly risk interference such as asset seizure or member arrest. The existence of this threat requires an efficiency/security tradeoff by criminal organizations, defined as «the interplay between the need to act collectively and the need to assure trust and secrecy within these risky collaborative settings» (Morselli, Giguère, and Petit, 2007). The resilience which comes from transparent democratic processes is undermined by the need for operational secrecy. At the same time, criminal organizations have a certain freedom, which can facilitate operational and structural changes because they do not have to report to stakeholders or explain their unethical behavior to institutions or media. In particular, Ayling focused on street gangs identifying three environmental sources of gang resilience:

(1) high level of interpenetration between gangs and legitimate businesses or state authorities;

(2) community support;

(3) thick crime habitats.

The associations between legitimate businesses, state authorities and gangs provide a source of gang resilience to disturbance. Nightclubs rely on gangs for security services, overlooking in return their drug dealing on the premises. Some gangs have also extensive investments in legitimate businesses or actively support particular political factions. Sometimes communities support the gang as an institution. This happens because gangs assist residents with bills and accommodation, protect them from exploitation and physical attacks, organize recreational activities or keep local rents low. Residents may also refuse to ostracize gang members because they are friends children or even their own relatives. This kind of community support is clearly a source of resilience because it gives gang members places, materials and psychological resources to reorganize and regroup after disruption. Thick crime habitats make also street gangs more resilient because they continually generate new criminal opportunities for the gang, providing a space to self-organize. In these spaces, gang members can find co-offenders, share information or make plans; they can recover from setbacks, such as injury or arrest of members. Thick crime habitats are plentiful in large urban conglomerates, particularly in weak or failing states.

According to Ayling (2009), gang resilience is also to be found in characteristics peculiar to a gang itself, such as its structure and operational methods. Gangs have simple structures which are flatter or minimally hierarchical, and decision-making power is therefore equally distributed throughout the organization. Thanks to this kind of structure, gangs have a capacity of adaptation to changing conditions (Pina e Cunha and Vieira da Cunha, 2006). Strong trust between members speeds information flow through a gang, making possible lightning adjustments to game plans and facilitating more measured debate about longer-term adjustments. However, close relationships may also increase the vulnerability of an organization, should there be an information leak. Security of information is a priority in a gang and it can be achieved through compartmentalization (Kenney, 2007; Williams, 2001) (*i.e.*, the isolation of important information within certain organizational cells). Compartmentalization allows to isolate the active parts (*i.e.* the cells which contain essential knowledge) of the gangs from the damaged ones and an adaptive and fast regeneration of gang operations after LEAs attacks. The identity of leaders or others central roles is an example of information which can be compartmentalized by a gang. Gangs, in fact, cannot prosper without a leader who mentor younger members and provide continuity. Leaders personal attributes and the way they influence the decisions and leadership styles may affect the gang resilience. Gangs also need skills of bricolage in order to creatively deal with hostile interventions and environmental changes. Bricolage is an ability to take available resources and make something new from them, even when these are seemingly unconnected.

The Sicilian Mafia

Catanese, De Meo, and Fiumara (2016) focused on the Sicilian Mafia emphasizing its most peculiar features. After the capture of a boss (*i.e.*, the leader of a Mafia family) and/or of his more close collaborators, this criminal organization shows high qualities in terms of regeneration and rearrangement of top positions equilibria. This ability allows it to reconstruct the specific skills of the various families active in the territory.

Mafia networks are able to resist even in situations of large pressure thanks to the large economic incomes which derive from the criminal activities and sustain them during the regeneration process. Even after substantial node removals, the network efficiency seems not to be significantly affected.

On the contrary, this property increases over time when old paths are restored, new paths are built and the overall dimension of the structure is reduced. Mafia associations have a powerful organizational structure which is highly resistant, adaptive, and flexible even after particularly incisive interruptions. Moreover the Sicilian Mafia has a peculiar feature called apparent appeasement which usually draw attention of magistrates and LEAs. It consists in the ability to change its visibility strategy maintaining the equilibria, an internal peace status and a low profile.

Cannabis cultivation

Duijn, Kashirin, and Sloot (2014) studied the resilience of criminal networks involved in organized cannabis cultivation. They reminded the studies of Ayling (2009) and Bouchard (2007), asserting that the notion of resilience involves two features:

(1) the ability to undergo and resist to disruption;

(2) the ability to adapt to alterations caused by that disruption.

Their work pointed out that cannabis cultivation is a delicate criminal process which is organized in a flexible and adaptive network structure, and it is highly resilient against network disruption. The authors also showed how criminal network resilience is a paradoxical concept which depends on:

(1) redundancy, which is essential for finding trustworthy replacements after losses due to disruption;

(2) non-redundancy, as the increased risks associated with the search replacement, demand compartmentalization of the flow of information to prevent further detection.

5.2.2 Resilience as behavior after disruption

Resilient criminal organizations are those that can respond quickly and effectively to disruption, enabling them to maintain illegal activities over time. Thus, to measure resiliency, it is necessary to factor in both the network robustness to disruption (*i.e.*, the structural characteristics of a network that insulate it from damage) as well as the length of time it takes for network recovery when disruption occurs (Duxbury and Haynie, 2019). Unfortunately, very little is known regarding criminal network recovery or behavior in the aftermath of disruption. Next, we review relevant works for the cases of terror and criminal networks, identifying prominent differences.

Agreste et al. (2016) investigated the network structure of a Mafia syndicate, describing its evolution, and highlighting its plasticity to membership-targeting interventions and its resilience to disruption caused by police operations. They analyzed two different datasets dealing with Mafia gangs built by examining different digital trails and judicial documents in a period of ten years. The first dataset included the phone contacts among suspected individuals, and the second captured the relationships among individuals actively involved in various criminal offenses. They showed that, although criminal networks were extremely resilient to different kinds of attacks, contact networks (*i.e.*, the network reporting suspects and reciprocated phone calls) were much more vulnerable.

Duxbury and Haynie (2019) evaluated covert network resilience by examining network recovery from different disruption strategies in an array of different covert networks:

(1) the September 11, 2001 terrorist network (Krebs, 2002);

(2) the Siren stolen-vehicle exportation network (Morselli and Roy, 2008);

(3) the Caviar network (see Subsubsect. 1.3.2);

(4) the New York network Terrorist (Natarajan, 2006).

They used an agent-based model to evaluate how covert networks recover from disruption, and identified which disruption strategies are most effective at damaging various covert networks. The authors found variability in the effects of disruption and time to recovery for different covert networks, depending on whether the network was organized to prioritize security or efficiency. Network vulnerability to specific targeting strategies, in terms of both network robustness and time to recovery, were considered when evaluating or developing LEAs interventions for the four covert networks. According to the authors, security-oriented networks tend to be more resilient than efficiency-oriented covert networks, in terms of both robustness and recovery.

5.3 Case study on the Montagna operation

As mentioned in Subsect. 5.1.2, we investigated the robustness of the Montagna networks across different scenarios, pinpointing the most effective metric, and demonstrating an effective strategy to obtain a faster *lcc* size drop (Cavallaro et al., 2020b),. We simulated two types of police operations:

(1) arresting one criminal at a time (sequential node removal);

(2) police raids (block node removal).

We evaluated how the different types of networks are impacted by these two types of perturbations, in terms of *lcc* size drop. We employed SNA methods to identify the actors having a high level of social capital. To this end, we put to test four different centrality metrics, namely: DC, BC, Katz Centrality and the Collective Influence.

As mentioned in Subsect. 5.1.2, DC and BC are the most used centrality measures to find strategic positions within a network. For the sake of completeness, we also considered two more prominent centrality metrics, that are Katz centrality and the collective influence. As already explained in Sect. 2.1, KC measures is a generalization of the EC, which computes the centrality of a node based on the centrality of its neighbors.

Collective Influence (CI) (Morone and Makse, 2015) establishes the centrality of a node in a criminal network taking into account the degree of the node neighbors at a given distance l from it. For a node i, it is defined as:

$$\mathrm{CI}_{\ell}(\mathrm{i}) = (k_i - 1) \sum_{j \in \delta B(i,\ell)} (k_j - 1), \tag{5.1}$$

where k_i is the degree of node i, $B(i, \ell)$ is the ball of radius ℓ centered on node i, and $\delta B(i, \ell)$ is the frontier of the ball (*i.e.*, the set of nodes at distance ℓ from i). To compute $CI_{\ell}(i)$, we first find the nodes on the frontier $\delta B(i, \ell)$.

KC and CI are not centrality measures traditionally applied to develop criminal network disruption strategies. Our aim was to verify if actor removal based on these measures was more or less effective than the most used degree and betweenness targeting strategies.

5.3.1 Montagna networks disruption strategies

We tried to disrupt the Montagna MN and PC networks, and evaluated the effects of node removal under different conditions and strategies. Both networks were used with and without considering the edge weights. Two node removal strategies have been studied. These are iterative procedures in which the nodes have been removed in decreasing order of their centrality score. After the node removal stage, the *lcc* size was updated, and the process was resumed.

Let us denote by $lcc(G)$ the size of the *lcc* of a graph G. Denote by G_i the graph resulting after the i-th iteration of the node removal algorithm, and by $lcc(G_i)$ the size of its *lcc*. The initial graph is denoted by G_0 and the size of its *lcc* is $lcc(G_0)$.

The relative difference between the size of the *lcc* when the simulation begins and i steps (*i.e.*, after the removal of i nodes or i set of nodes) is given by $\rho_i \in [0, 1]$:

$$\rho_i = 1 - \left| \frac{lcc(G_i) - lcc(G_0)}{lcc(G_0)} \right|. \tag{5.2}$$

Note that $\rho_0 = 1$ and $\rho_n = 0$, where n is the last iteration (sequential removal).

Both strategies (sequential and block removal) may be summarized as follows:

Step 1 We first computed $lcc(G_0)$, *i.e.*, the lcc size for the initial graph G_0.

Step 2 This step depends on the removal strategy. Either the highest ranking of the remaining nodes (in the sequential strategy), or the set of the five most influential nodes of the remaining ones (in the block strategy) are removed. Ranks were computed with the current centrality score. The new graph G_i, with $i = 1, 2, \ldots, n$ was obtained (for block removal we had fewer iterations).

Step 3 We computed $lcc(G_i)$ and ρ_i.

Step 4 Steps 2 and 3 were repeated until the graph size could no longer be reduced.

Sequential node removal simulates the scenario in which affiliates are arrested one-by-one by the police.

Block node removal simulates the scenario in which affiliates are arrested during a raid by the police. This strategy is similar to the sequential one. The main difference is that nodes are removed in blocks of five. The block size depends on the type and scale of the dataset. The fraction of nodes to be removed during block police operations is a reasonable value that took into account some considerations. In Agreste et al. (2016), we obtained a serious reduction of the lcc with only 5% as block size. Moreover, in such a relatively small criminal network, larger fractions of block sizes appear unrealistic. This is why we chose to remove five nodes at once.

5.3.2 Montagna networks behavior after disruption

Weighted Graphs. Fig. 5.4 shows the results obtained on the Montagna MN and PC networks applying sequential and block node removal strategies, where nodes are targeted according to DC, BC, KC and CI.

KC is configured with the default values of $\alpha = 0.1$ and $\beta = 1.0$. Remarkably, it is the least effective one (*i.e*, the slowest one) at causing the lcc size drop, in all the cases. To understand this result intuitively, we need to look at the way this centrality metric operates. Katz determines the importance of each node based on the number of walks that pass through it; but it does not consider their length. Furthermore, shortest paths were not considered, hence a walk may visit the same node multiple times. Yet, this is in contrast to how criminals would operate in practice. Affiliates typically prefer to spread the information through a number of intermediaries, to minimize the risk of interception by non-family members. This was consistent with our earlier findings (Ficara et al., 2020). Ultimately, it would not make sense (and would be unwise) to send the same message multiple times through the same path, which is what Katz would help identifying. Therefore, removing nodes by the highest Katz score would not be a winning strategy.

All the other metrics act better than KC, and comparably among each other. This happens because of the weight distribution shape (see Fig. 1.7), which exhibits a long tail of nodes, with just a few dominating ones (see Subsubsect. 1.3.1). Thus, after removing the most central nodes (*i.e.*, the first five iterations), the network get almost totally disconnected and the remaining nodes have the same weight ($w = 1$). Hence, all the metrics focused on either degree (*i.e.*, DC and CI) or shortest paths (*i.e.*, BC) follow the same ρ drop speed. On the other hand, KC with its default parameters focuses on walks of undefined lengths, thus producing a slower ρ drop.

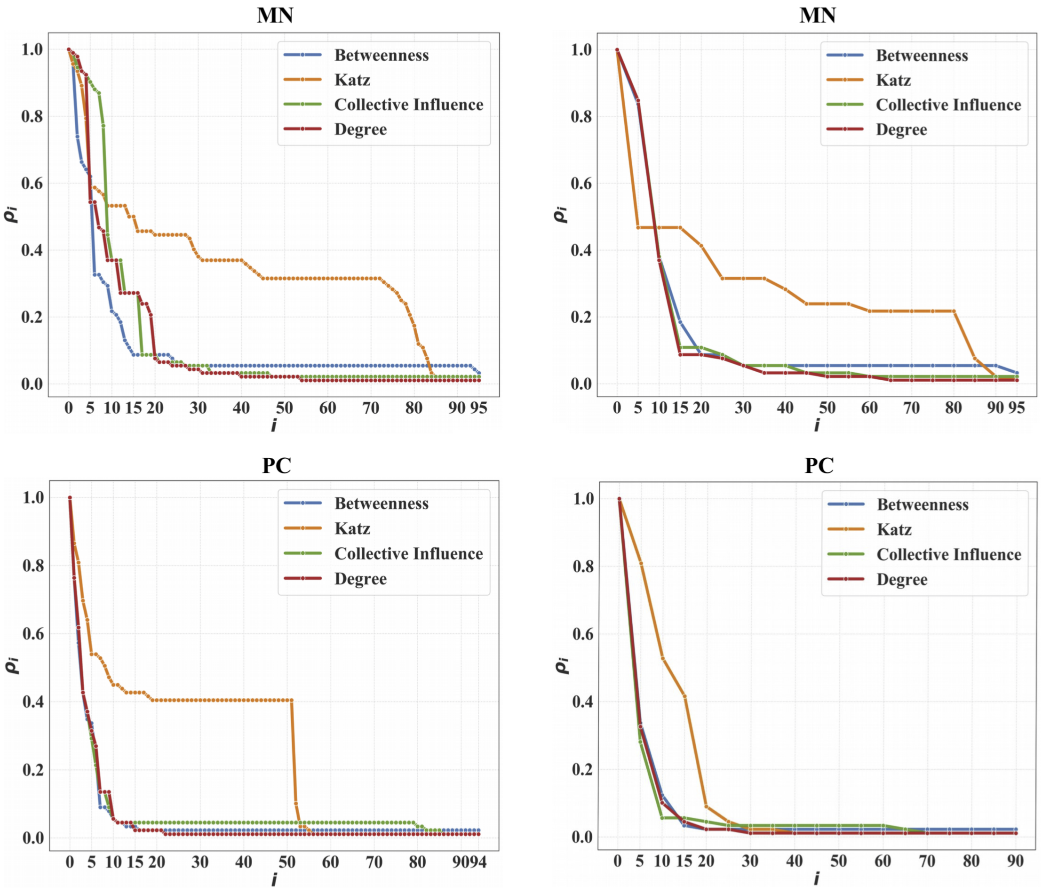

FIGURE 5.4: **Sequential and block node removal strategies in the Montagna Meetings (MN) and Phone Calls (PC) networks.** ρ is the relative difference between the size of the largest connected component in the initial graphs and after i steps when sequential (left column) and block (right column) node removal strategies are applied to the weighted networks.

Sequential vs Block Removal. Looking at Fig. 5.4, with the exception of Katz, no significant differences are visible between the two node-removal strategies (*i.e.*, sequential and block). This is somewhat counter-intuitive, since in real life police raids are typically aimed at breaking up the network more effectively. In our case, this result originates from the particular type of our dataset. When constructing our networks, we did not have access to information about the way criminals reconstructed their communication channels following arrests. Hence, our networks are static (*i.e.*, they miss the network reconfiguration data), which is why our analysis is not fully capturing the dynamic aspects that differentiate sequential and block strategies. In network terms, this translates into no differences in terms of *lcc* size drop as the networks are static. On the other hand, significant network re-tuning of node importance, due to internal reorganization of trusted affiliates used to spread messages within and outside the criminal network, would be expected in the case of dynamic graphs (*i.e.*, graph snapshots before and after police operations).

Weighted vs Unweighted. Considering now the differences between weighted and unweighted graph analysis, we noticed that the majority of cases did not pinpoint major differences. This was due to the peculiar way in which weights were distributed in criminal networks (as noted in the *Weighted Graphs* paragraph at the beginning of Subsect. 5.3.2).

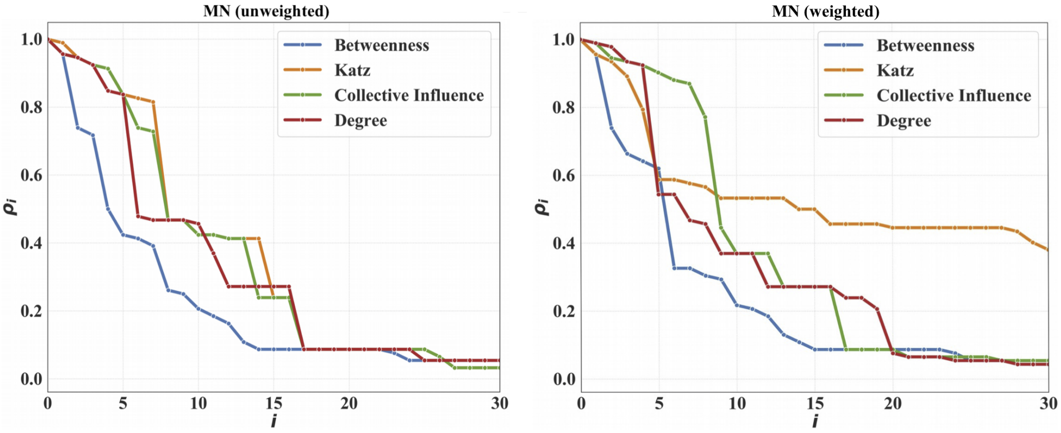

FIGURE 5.5: **Sequential node removal strategies in the Montagna Meetings (MN) network.** ρ is the relative difference between the size of the largest connected component in the initial graph and after i steps when a sequential node removal strategy is applied to the unweighted and weighted criminal network.

Nevertheless, interesting differences are visible in the MN network - sequential node removal (see Fig. 5.5). The unweighted case is mostly faster than (although occasionally equivalent to) the weighted case. This is because the weights (*i.e.*, the affiliates' interaction frequency) are concentrated in very few individuals, with most other weights having $w = 1$. This is also why, with the exception of the initial transient period (involving very few interactions), most algorithms converge to similar values.

The best centrality metric. Comparing the algorithms in Fig. 5.5, it emerges that BC is by far the most effective centrality index for reducing the size of the lcc of a criminal network.

This result is consistent with literature reports upon criminal network analysis and has an intuitive explanation. Indeed, to avoid being intercepted, members of a criminal network build their relationships to assure that information flows along the shortest possible paths. In this way, both MN and PC networks configure themselves as small-world networks with a low average path length $\langle d \rangle$ and a large number of connected components $|cc|$. The nodes that intercept most of these shortest paths are those having the largest values of BC, and act as intermediaries to assure the quick flow of information from any source to any target in the graph.

To confirm this intuition, we progressively removed nodes according to their BC and we measured the corresponding variation of $\langle d \rangle$ and $|cc|$ (see Fig. 5.6). These plots indicate that the selected removal of nodes amplifies the average distance between any pair of nodes in the MN and PC networks and, simultaneously, it creates an increasing number of disjoint components. A repressive action aimed at removing high betweenness nodes has, therefore, a devastating impact on network topology because it causes an lcc size drop, as we observed a fast drop in ρ. Also, since the KC prioritized those nodes crossed by a large number of walks of arbitrary length,

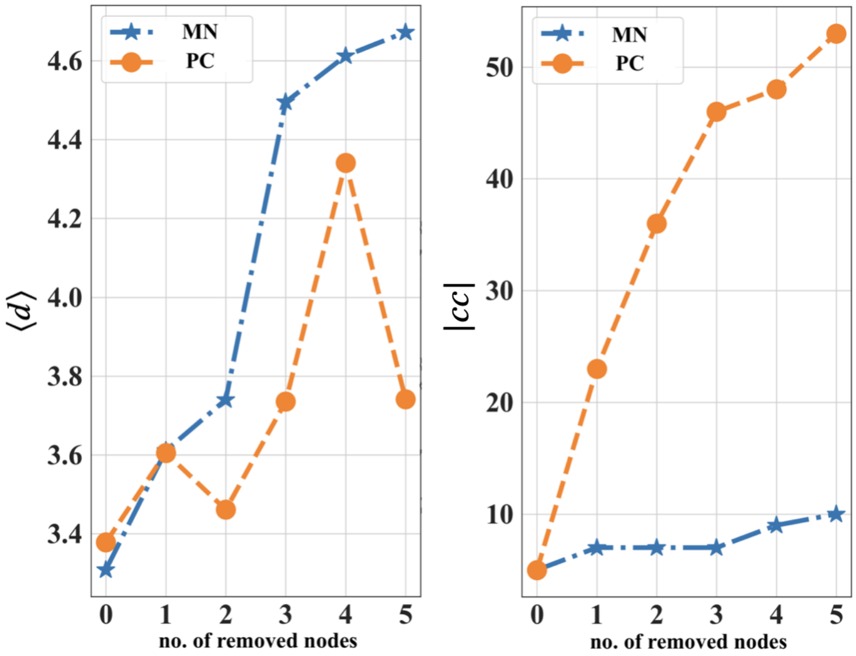

FIGURE 5.6: **Betweenness centrality targeting in the Montagna Meetings (MN) and Phone Calls (PC) networks.** Average path length $\langle d \rangle$ and number of connected components $|cc|$ are represented as functions of the number of removed nodes with high betweenness in the criminal networks.

it was less effective in detecting the nodes acting as intermediaries, and whose removal reduced the lcc size the most.

Intuitively, BC outperforms the other metrics, thanks to its operation on paths, rather than on individual nodes degree. This is particularly effective in criminal networks that are devised in such a way as to minimize the path length, in order to reduce the risk of police interceptions. BC compromises the most influential paths, leading to a faster drop in ρ. This feature is what makes betweenness somehow opposite to KC (whose goal is to explore walks).

CI was the second worst performer after Katz. This was, again, due to its emphasis on node degree instead of path length. CI also showed some differences between the weighted and the unweighted processes, exhibiting a lower ρ drop in the weighed graph. A possible explanation is that the weighted case identifies as influential nodes not only those with higher weights on the incident links, but also the nodes having high-weight only on immediate neighbors. This could reflect a typical situation in criminal networks, whereby the top-leaders avoid direct exposure and mediate all communications through a single trusted individual (or very few of them). On the other hand, this particular aspect is not detectable in the unweighted analysis.

5.3.3 Real-world implications

Our SNA results can be directly translated onto law enforcement actions, considering that we are now able to efficiently identify the top 5% most trusted affiliates (*i.e.*, the ones typically employed as intermediaries between bosses and the other members).

In turn, we can virtually neutralize the clans' internal communication infrastructure by getting the trusted affiliates in custody. Intuitively, whenever arrests can be made in block (raids), that would further impair the ability of the criminal communication network to be re-established. However, we have not studied this specific aspect, due to unavailability of necessary data.

The pre-trial detention order is the final outcome of a time-consuming police investigation. Once the inquiry is underway (and even before it has been completed), the actual network is richer than the one derived from the pre-trial detention order. The investigative network includes extra interactions among suspects, which are removed once the judge deems them to be irrelevant. Thus, the final network derived from the original one is partial and misses the data included in the initial investigation. This explains our limits related to the lack of data.

Furthermore, when LEAs inspect on those kinds of criminal networks, most of the time they have prior knowledge thanks to criminal records, even though they may not have a clear picture of the connections between individuals.

Generally speaking, the aim of a cosca is to conduct illegal activities (which may vary from place to place and are susceptible to local trends), and to ultimately pursue effective financial benefits. For instance, some clans may focus on drugs, rather than organ trafficking, prostitution, finance, or political influence. Quite commonly, clans pursue multiple activities, which makes it even more difficult to reconstruct the labyrinth of criminal communication networks (and perform SNA thereof).

Our datasets emerged directly from a collection of official juridical acts, and focused on a single criminal activity (the securement of public procurement contracts). This involved a network of entrepreneurs, was confined to a specific geographical area, and captured information over a limited time span. The peculiarity of our networks is that the gang was established in relation to a specific event (procurement of a mechanization process), so it was not a pre-existent organization. Thus, our dataset captured a relatively simpler snapshot of the complex entanglement of mafia criminals, which constitutes both a strength, and weakness of our study.

Indeed, if LEAs have prior knowledge, then our approach is even more efficient; otherwise, as in the case of the Montagna networks, two main issues may arise to conduct investigations: noise and different organizational time scales.

By noise, we mean that LEAs could have too much information (*e.g.*, too many interceptions or surveillance logs, some of which are worthless). By different organizational time scales we indicate that criminals already know how to contact a specific criminal for their illicit purposes (*e.g.*, a sniper), in a way LEAs might not be able to identify. Thus, they have to spend more time to reconstruct the inner relationships by exploring the evidences and, as previously asserted, this is a time consuming process.

On the one hand, the scope of our SNA analysis is limited by the significance and breadth of the datasets at hand. A more dynamic analysis of the network could not be done in this case, as for instance, understanding the re-connection ability following events like individual arrests or police raids. Also, we are capturing a single criminal activity in a confined spatiotemporal context. So, it was not possible to detect a broader and more diversified set of communications, such as those taking place in a more complex, multi-activity network. Nor could we detect external communications, such as those involving people who were not directly members of the criminal nets except for entrepreneurs (*e.g.*, politicians, magistrates and businessmen).

On the other hand, the greater specificity of the Montagna networks allowed a cleaner analysis, focused on unveiling some hidden communication mechanisms.

Having reduced the parameters under scrutiny and the complexity of the system, we could pinpoint a simple, yet effective strategy for unsettling the connectivity of the network through a dramatic drop in the *lcc* size. This might have not emerged from the analysis of a more complex network. Also, this simpler framework has allowed us to swiftly test out our hypothesis and to obtain reliable results.

This could have been a challenge on a complex network, especially when multiple criminal activities take place in parallel.

Chapter 6

The multilayer approach

During his lifetime, each individual continuously deal with multiple social networks. He does it with no effort and this does not mean that it is a trivial activity which can be overlooked. The connections between people through multiple types of relational ties represent only one possible view of a problem already known long before the field of SNA was developed. Looking only at a single type of relational tie within a single social network risks either defining a world where different kinds of relationships are ontologically equivalent or overlooking the invisible relationships emerging from the interactions among different types of ties.

For a long time, these interactions have largely been studied within a single-layer perspective and one of the most effective SNA tools to measure social interactions has been the simple graph (see Subsect. 1.1.3).

According to Wasserman and Faust (1994), social networks contain at least three different dimensions: a structural dimension corresponding to the social graph (*e.g.*, actors and their relationships); a compositional dimension describing the actors (*e.g.*, their personal information); and an affiliation dimension (*e.g.*, members of the same family or organization). These three dimensions provide a minimal description needed to understand the full complexity of social structures.

An alternative conceptual approach to dealing with the same set of problems is to think of multiple relationships as a set of connected levels, or layers, forming a single multidimensional social network (Dickison, Magnani, and Rossi, 2016). In fact, a social network with nodes and/or edges can be organized into multiple layers, where each layer represents a different kind of node or edge, a different social context, a different community, a different online social network, and so on. The analysis of multiple layers can provide knowledge that is not present in each layer when layers are considered independently of each other.

Kivelä et al. (2014) reviewed and discussed many of the relevant works on the topic. Then, they tried to unify the literature by introducing a general framework for multilayer networks (Boccaletti et al., 2014; Catanese, 2017; De Domenico et al., 2013, 2015). Such framework can represent the different notions of networks (*e.g.*, single-layer or monoplex networks (De Domenico et al., 2013; Degani, 2016), multiplex networks (Battiston, Nicosia, and Latora, 2014; Nicosia and Latora, 2015; Solé-Ribalta et al., 2014), interdependent networks, networks of networks) by simply introducing cumulative constraints on the general model (Tomasini, 2015).

Multilayer social networks appear in a number of different contexts, where data are characterized by different sizes, different natures (*e.g.*, online, offline, hybrid), and different layer semantics (*e.g.*, contact, communication, time, context, etc.). Many multirelational networks, that is actors connected by multiple types of ties, have been collected during SNA studies. These networks are often characterized by a small size, because they were often collected through offline questionnaires or interviews and they can be very useful in qualitatively checking the behavior and results of new methods (Dickison, Magnani, and Rossi, 2016).

An interesting multirelational network about criminal relationships is described by Bright et al. (2015) who focused on eight types of edges related to the exchange of a particular resource (*e.g.*, drugs, money) in a criminal network with 128 actors. Some networked systems can be better modeled by multilayer structures where the individual nodes develop relationships in multiple layers.

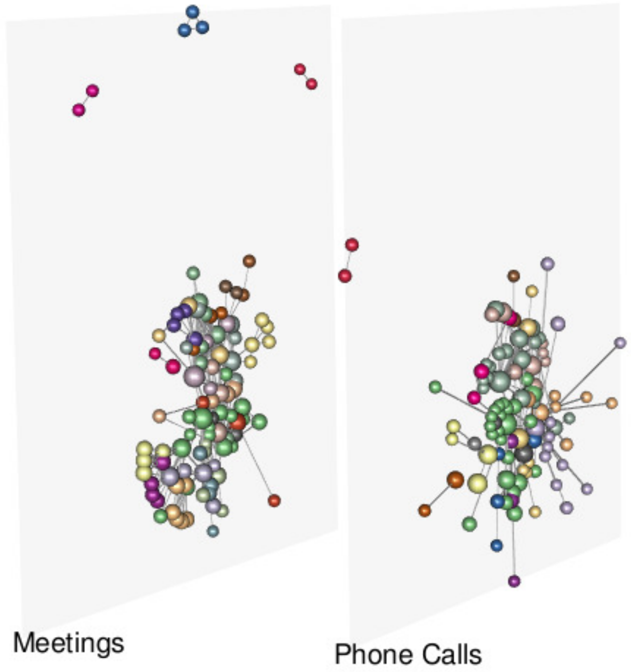

FIGURE 6.1: **The Montagna multilayer network.** The layered visualization is obtained using Muxviz. The color of nodes is given by their community assignment, and the size by their degree.

In Ficara et al. (2021e), a new real multilayer criminal network was built starting from the Montagna *MN* and *PC* networks described in Subsect. 1.3.1. It is an undirected and weighted multilayer network with two layers called Meetings and Phone Calls, 154 nodes and 439 edges. Fig. 6.1 shows the layered visualization obtained using Muxviz (De Domenico, Porter, and Arenas, 2014). The color of nodes is given by their community assignment (*i.e.*, how actors are clustered together) and the size by their degree. The links within layer Meetings refer to the meetings among members of the criminal network, while edges in the layer Phone Calls represent phone communications among distinct phone numbers they use. The weight encodes the number of meetings or phone calls. This network can be identified as an edge-colored multilayer (*i.e.*, a network with multiple types of edges), and more precisely as a multiplex network which does not require all nodes to exist on every layer. Each layer have to share at least one node with some other layer in the network to be multiplex. In this case, the two layers share 47 nodes. Moreover, interlayer edges are only those between nodes and their counterparts in the other layer and no cost is associated to them.

An analysis of suspects' importance was performed for each layer separately, for the aggregate network (obtained summing for each node the edges over all layers in the multilayer network) and the multilayer one which allowed to quantify the importance across the whole series of layers. The degree was used as a simple descriptor to compute the centrality of the actors. This measure just quantifies the number of different meetings or phone calls of each suspect. The top 20 characters are showed ranking them by their degree in each layer, in the aggregate network and in the multilayer network comparing the resulting importance with the role they had in the Sicilian Mafia families which were the protagonists of the Montagna operation.

6.1 Single-layer networks

The concepts presented in Subsect. 1.1.3 can be expressed using an alternative notation, which makes use of tensors and Einstein's notation (De Domenico et al., 2013; Degani, 2016).

Given the canonical basis in the vector space $\mathbb{R}^N$, $\xi = \{e_1, e_2, ..., e_n\}$ where $e_i = (0, ..., 0, 1, 0, ..., 0)^T$ is 1 in the ith component, and 0 otherwise. Given a set of n nodes v_i (where $i = 1, 2, ..., n$ and $n \in \mathbb{N}$), we associate with each node a state that is represented by the canonical vector e_i in the vector space $\mathbb{R}^n$. A node v_i can be related with each other and the presence and the intensity of such relationships in the vector space is indicated using the tensor product (Abraham, Marsden, and Ratiu, 1988) (*i.e.*, the Kronecker product) $\mathbb{R}^n \otimes \mathbb{R}^n = \mathbb{R}^{n \times n}$. Thus, second-order (*i.e.*, rank-2) canonical tensors are defined by $E_{ij} = e_i \otimes e_j^T$ (where $i, j = 1, 2, ..., n$). Consequently, if w_{ij} indicates the intensity of the relationship from node v_i to node v_j, the relationship tensor can be written as:

$$W = \sum_{i=1}^{n} \sum_{j=1}^{n} w_{ij} E_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{n} w_{ij} e_i \otimes e_j^T \,. \tag{6.1}$$

In the context of single-layer networks, W corresponds to an $n \times n$ weight matrix that represents the standard graph of a system that consists of n nodes. This matrix is equivalent to the adjacency matrix A (see Eq. 1.2) and it is an example of an adjacency tensor.

An adjacency tensor can be written using the covariant notation introduced by Ricci and Levi-Civita (1900). In this notation, a row vector $a \in \mathbb{R}^n$ is given by a covariant vector a_α (where $\alpha = 1, 2, ..., n$), and the corresponding contravariant vector a^α (*i.e.*, its dual vector) is a column vector in the Euclidean space. The adjacency tensor W can be represented as a linear combination of tensors in the canonical basis:

$$W^\alpha_\beta = \sum_{i=1}^{n} \sum_{j=1}^{n} w_{ij} e^\alpha(i) e_\beta(j) = \sum_{i=1}^{n} \sum_{j=1}^{n} w_{ij} E^\alpha_\beta(ij) \,, \tag{6.2}$$

where $e^\alpha(i)$ is the αth component of the ith contravariant canonical vector e_i in $\mathbb{R}^n$, and $e_\beta(j)$ is the βth component of the jth covariant canonical vector in $\mathbb{R}^n$, $E^\alpha_\beta(ij) \in \mathbb{R}^{n \times n}$ indicates the tensor in the canonical basis that corresponds to the tensor product of the canonical vectors assigned to nodes v_i and v_j (*i.e.*, it is E_{ij}).

Define the 1-vector $u^\alpha = (1, 1, ..., 1)^T \in \mathbb{R}^n$ whose components are all equal to 1, and let $U^\beta_\alpha = u_\alpha u^\beta$ be the second-order tensor whose elements are all equal to 1 (*i.e.*, a so-called 1-tensor). The degree vector is calculated adding up all the columns of the adjacency tensor defined in Eq. 6.2:

$$k_\beta = W^\alpha_\beta u_\alpha \,. \tag{6.3}$$

It is possible to calculate the degree of node v_i by projecting the degree vector onto the ith canonical vector:

$$k(i) = k_\beta e^\beta(i) \,. \tag{6.4}$$

6.2 Multilayer networks

In this section, the tensor formulation of multilayer networks is reviewed. Following the literature, we use the tensor formulation which represents the natural extension of the adjacency matrix to the case of multilayer networks. Here, we are interested in explaining how to extend the degree formulation to the multilayer case.

Kivelä et al. (2014) define a multilayer network as the most general structure which can be used to represent any kind of network. At the base of this structure, there is the elementary concept of graph, defined in Subsect. 1.1.3. The representation of networks at multiple levels or with multiple types of edges (or with other similar features) requires structures that have layers in addition to nodes and edges. Moreover, the concept of aspect can be defined as a feature of a layer representing one dimension of the layer structure (*e.g.*, the type of an edge or the time at which an edge is present) (Tomasini, 2015). More specifically, an "elementary layer" is an element of one of the possible sets of layers from a specific aspect and the term "layer" refers to a combination of elementary layers from all aspects.

A multilayer network can be defined as a quadruplet $M = (N_M, E_M, N, L)$. $N_M \subseteq N \times L_1 \times \cdots \times L_d$ is the set of the node-layer combinations, that is the set of layers in which a node $v_i \in N$ is present. $E_M \subseteq N_M \times N_M$ is the edge set containing the set of pairs of possible combinations of nodes and elementary layers. N is the set of all nodes independently from the layer. $L = \{L_a\}^d_a = 1$ is the sequence of sets of elementary layers such that there is one set of elementary layers L_a for each aspect a. If $d = 0$, the multilayer network M reduces to a single-layer network. If $d = 1$, then M reduces to a multiplex network.

Using multiple layers, it is possible to represent different types of edges: those among nodes in the same layer, called intralayer edges, and those among nodes in different layers, called interlayer edges. For this reason, the concepts of intralayer and interlayer adiacency tensor are introduced (De Domenico et al., 2013). The intralayer adiacency tensor $C^\alpha_\beta(\widetilde{k}\widetilde{k})$ is defined as the second-order tensor $W^\alpha_\beta(\widetilde{k})$ that indicates the relationships between nodes within the same layer $\widetilde{k}$, where $\alpha, \beta = 1, 2, ..., n$ as defined in Eq. 6.2. The tilde symbol is used to distinguish indices that correspond to nodes from those that correspond to layers. To encode information about relationships between nodes on different layers (*e.g.*, a node v_i from layer $\widetilde{h}$ can be connected to a node v_j in another layer $\widetilde{k}$), the second-order interlayer adjacency tensor $C^\alpha_\beta(\widetilde{h}\widetilde{k})$ is introduced. The interlayer adjacency tensor $C^\alpha_\beta(\widetilde{h}\widetilde{k})$, which corresponds to the case in which a pair of layers represents the same layer $\widetilde{k}$, is equivalent to the intralayer adjacency tensor $W^\alpha_\beta(\widetilde{k})$ of such a layer.

Following a similar approach to the one used to define the adjacency tensor for single-layer networks (see Eq. 6.2), the vector $e^{\widetilde{\gamma}}(\widetilde{k})$ (where $\widetilde{\gamma}, \widetilde{k} = 1, 2, ..., L$) of the canonical basis in the space $\mathbb{R}^L$ is introduced. The greek index indicates the components of the vector while the latin index indicates the kth canonical vector. It is straightforward to construct the second-order tensors that represent the canonical basis of the space $\mathbb{R}^{L\times L}$ as:

$$E^{\tilde{\gamma}}_{\tilde{\delta}}(\tilde{h}\tilde{k}) = e^{\tilde{\gamma}}(\tilde{h})e_{\tilde{\delta}}(\tilde{k})\,. \tag{6.5}$$

The multilayer adjacency tensor (Degani, 2016) can be written from Eq. 6.5, using a tensor product between the adjacency tensors $C^{\tilde{\alpha}}_{\tilde{\beta}}(\tilde{h}\tilde{k})$ and the canonical tensors $E^{\tilde{\gamma}}_{\tilde{\delta}}(\tilde{h}\tilde{k})$. A fourth-order tensor is obtained as:

$$M^{\alpha\tilde{\gamma}}_{\beta\tilde{\delta}} = \sum_{\tilde{h}=1}^{L}\sum_{\tilde{k}=1}^{L} C^{\alpha}_{\beta}(\tilde{h}\tilde{k})E^{\tilde{\gamma}}_{\tilde{\delta}}(\tilde{h}\tilde{k})\,. \tag{6.6}$$

The second-order interlayer adjacency tensor $C^{\alpha}_{\beta}(\tilde{h}\tilde{k})$ can be written when $\tilde{h} = \tilde{k}$ as:

$$C^{\alpha}_{\beta}(\tilde{h}\tilde{k}) = \sum_{i=1}^{n}\sum_{j=1}^{n} w_{ij}(\tilde{h}\tilde{k})E^{\alpha}_{\beta}(ij)\,, \tag{6.7}$$

where $w_{ij}(\tilde{h}\tilde{k})$ are real numbers that indicate the intensity of the relationship between nodes v_i in layer $\tilde{h}$ and node v_j in layer $\tilde{k}$. Then, the fourth-order tensor of the canonical basis of the space $\mathbb{R}^{n\times n\times L\times L}$ is defined as:

$$\xi^{\alpha\tilde{\gamma}}_{\beta\tilde{\delta}}(ij\tilde{h}\tilde{k}) = E^{\alpha}_{\beta}(ij)E^{\tilde{\gamma}}_{\tilde{\delta}}(\tilde{h}\tilde{k}) = e^{\alpha}(i)e_{\beta}(j)e^{\tilde{\gamma}}(\tilde{h})e_{\tilde{\delta}}(\tilde{k})\,. \tag{6.8}$$

Replacing in Eq. 6.6 the expressions obtained in Eq. 6.2 and Eq. 6.8, the multilayer adjacency tensor can be written as:

$$M^{\alpha\tilde{\gamma}}_{\beta\tilde{\delta}} = \sum_{\tilde{h},\tilde{k}=1}^{L}\sum_{i,j=1}^{n} w_{ij}(\tilde{h}\tilde{k})\xi^{\alpha\tilde{\gamma}}_{\beta\tilde{\delta}}(ij\tilde{h}\tilde{k})\,. \tag{6.9}$$

In some cases, it is possible to construct a single-layer network by aggregating multiple networks. Such aggregation is useful in many situations such as the study of temporal networks or social networks. To project a multilayer network onto a weighted single-layer network, the corresponding tensor multiplied by the 1-tensor $U^{\beta\tilde{\delta}}_{\alpha\tilde{\gamma}}$. The obtained projected single-layer network P^{α}_{β} (De Domenico et al., 2013) is:

$$P^{\alpha}_{\beta} = M^{\alpha\tilde{\gamma}}_{\beta\tilde{\delta}}U^{\tilde{\delta}}_{\tilde{\gamma}} = \sum_{\tilde{h}=1}^{L}\sum_{\tilde{k}=1}^{L} C^{\alpha}_{\beta}(\tilde{h}\tilde{k})\,. \tag{6.10}$$

A structure similar to the projected single-layer network is the aggregate or overlay single-layer network (De Domenico et al., 2013) that is obtained from a multilayer network by summing the edges over all layers for each node. The aggregate network ignores the non-negligible contribution of interlayer connections and it is obtained from a multilayer adjacency tensor by contracting the indices corresponding to the layer components as:

$$O^{\alpha}_{\beta} = M^{\alpha\tilde{\gamma}}_{\beta\tilde{\gamma}} = \sum_{\tilde{r}=1}^{L} W^{\alpha}_{\beta}(\tilde{r})\,. \tag{6.11}$$

In the case of an aggregate network, the degree computation is the same of a single-layer network and it is computed like in Eq. 6.3.

On the contrary, the multidegree centrality vector K^{α} (De Domenico et al., 2013) is defined by performing the same projections from the case of single-layer networks using 1-tensors of an appropriate order:

$$K^{\alpha} = \left[M^{\alpha\tilde{\gamma}}_{\beta\tilde{\delta}} U^{\tilde{\delta}}_{\tilde{\gamma}}\right] u^{\beta} = \left[P^{\alpha}_{\beta}\right] u^{\beta} = \left[\sum_{\tilde{h}=1}^{L} \sum_{\tilde{k}=1}^{L} C^{\alpha}_{\beta}(\widetilde{\tilde{h}\tilde{k}})\right] u^{\beta} = \sum_{\tilde{h}=1}^{L} \sum_{\tilde{k}=1}^{L} k^{\alpha}(\widetilde{\tilde{h}\tilde{k}}), \qquad (6.12)$$

where $k^{\alpha}(\widetilde{\tilde{h}\tilde{k}})$ is the degree vector defined in Eq. 6.3 computed on the interlayer adjacency tensor $C^{\alpha}_{\beta}(\widetilde{\tilde{h}\tilde{k}})$.

6.3 The identification of key actors

As already said in Chap. 2, leaders in a criminal network can be identified using a family of measures called centralities aimed at identifying the most important actors in a social network.

Three different approaches can be used to analyze the importance of nodes in a multiplex network using node degree as descriptor:

Approach 1 The two layers of the multilayer network are merged to obtain a single-layer network (*i.e.*, the aggregate network shown in Fig. 6.2). This process, often called flattening, is performed creating a new network with one node for every actor and an edge between two nodes if the corresponding actors are connected in any of the layers. Once the aggregate network is obtained, traditional degree (see Eq. 6.3) can be computed.

Approach 2 The traditional degree (see Eq. 6.3) can be applied to each layer separately. Then, the results are compared.

Approach 3 Multiple layers are considered at the same time, but without treating them as being ontologically different. Measures based on this approach explicitly consider the difference between interlayer and intralayer edges and also make numerical distinctions between different layers (*e.g.*, through weights), but at the end they typically produce single numerical values merging the contributions of the different types of edges (De Domenico et al., 2013, 2015) (see Eq. 6.12).

Table 6.1 gives a summary of the 20 top nodes ranked by their degree in the Aggregate network (*i.e.*, according to Approach 1), in the single layers Phone Calls and Meetings (*i.e.*, according to Approach 2) and in the Multilayer network (*i.e.*, according to Approach 3). The node importance given by their degree is compared with the real roles these nodes have in the Sicilian Mafia families observed during the Montagna operation.

The analysis of node degree was performed for each layer separately, the aggregate and the multilayer networks using Muxviz (De Domenico, Porter, and Arenas, 2014) and Python. The multilayer framework allows to quantify the importance of a node across all the layers. The top 20 nodes ranked by their degree are shown in Fig. 6.3. The results for each layer separately (*i.e.*, Meetings or Phone Calls), shown in the stacked histogram, reveal that the most important actors per layer are nodes 18 and 47. The result from the aggregate network, obtained by summing up all interactions across the whole network while neglecting the layered structure, also identify nodes 18 and 47 as the most central actors. The same result is obtained for the multilayer network, *i.e.*, considering the layered structure. These two nodes are

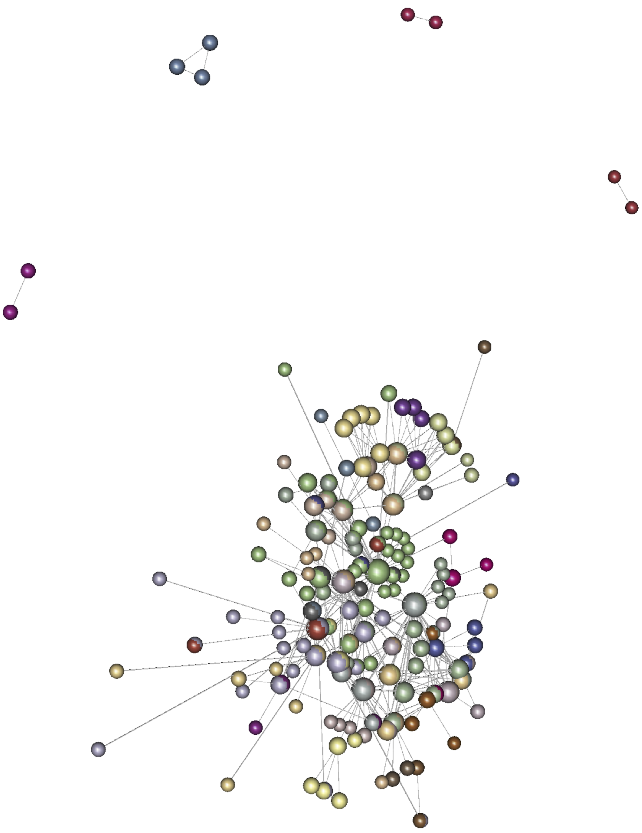

FIGURE 6.2: **The Montagna aggregate network.** The edge-colored multigraph visualization is obtained using Muxviz. The color of nodes is given by their community assignment, and the size by their degree.

effectively important because they are respectively Caporegime of the Mistretta family and deputy Caporegime of the Batanesi family. Using the multilayer framework it was possible to identify two key Caporegimes of the Mistretta family (*i.e.*, nodes 61 and 25). Node 61 was one the twenty most important nodes in the Phone Calls layer but not in the Meetings layer. Node 25 was one the twenty most important nodes in the Meetings layer but not in the Phone Calls layer. So, the importance of these nodes doesn't emerge from the analysis of the single layers but only from the analysis of the Aggregate network and even more of the Multilayer one. The Messaggero (*i.e.*, node 43) who didn't seem so important from the analysis of the single layers was also identified. Then, it was possible to identify some key associates such as pharmacist or entrepreneurs needed in synthetic drug synthesis processes or to facilitate the award of public contracts to companies close to criminal organizations. The identification of these figures can be very useful to define attack strategies to disrupt criminal networks (Cavallaro et al., 2020b; Duijn, Kashirin, and Sloot, 2014; Villani, Mosca, and Castiello, 2019).

This is a preliminary study that shows promising results by identifying nodes which don't seem important from the analysis of the single-layer networks or the aggregate network.

Montagna *MN* and *PC* are two criminal networks based on meetings and phone calls among suspected criminals observed during stakeouts or wiretapped by police during a specific period of time. *MN* possesses a greater number of connections

TABLE 6.1: The 20 top ranked nodes in the Multilayer, Aggregate, Phone Calls and Meetings networks compared with their roles in the Montagna Operation.

Node		Degree			
Name	**Role**	**Multilayer**	**Aggregate**	**Phone Calls**	**Meetings**
18	Caporegime Mistretta Family	51	41	25	24
47	Deputy Caporegime Batanesi Family	42	29	21	19
27	Caporegime Batanesi Family	29	21	11	16
68	Caporegime Batanesi Family	27	19	10	15
29	Enterpreneur	24	16	9	13
61	Caporegime Mistretta Family	23	19	17	4
45	Soldier Batanesi Family	20	14	6	12
12	Soldier Mistretta Family	19	16	1	16
11	Mafia activity coordinator in Messina	18	15	4	12
22	Pharmacist	18	15	2	14
51	Soldier Batanesi Family	17	11	4	11
25	Caporegime Mistretta Family	16	13	1	13
43	Messaggero	16	11	5	9
48	Soldier Batanesi Family	15	12	1	12
19	External partnership	14	11	3	9
36	Aiding and abetting of a fugitive	14	11	4	8
75	Soldier Mistretta Family	14	12	8	4
89	Soldier Batanesi Family	14	12	N/A	12
54	Enterpreneur	13	7	5	6
5	Sighted with nodes 11 and 12	12	10	N/A	10

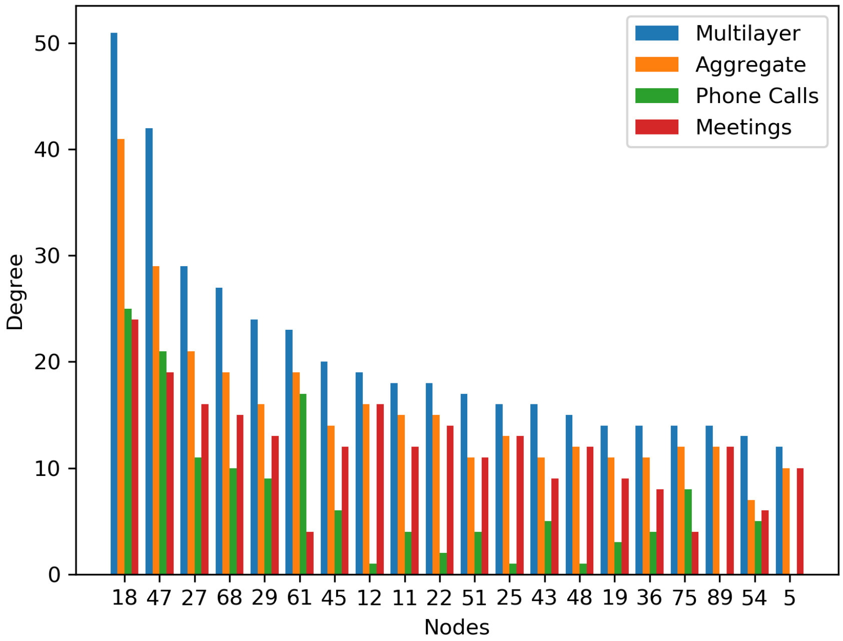

FIGURE 6.3: **Degree in the Montagna multilayer network.** The 20 top ranked nodes by degree are identified in Multilayer (Blue), Aggregate (Orange), Phone Calls (Green) and Meetings (Red) networks.

because LEAs were only able to identify the participants to meetings and not the full extent of their interactions (see Sect. 1.3). In crowded meetings, some participants may have had a very limited (if any) interaction with other participants. In such case, assuming that all participants interacted with each other may considerably overestimate the real number of connections. This is the reason why *MN* is more dense than *PC*.

Moreover, we deal with two criminal networks in which communications are supposed to be reduced to keep the criminal organization safe. If two criminals call each other, it is reasonable to believe that they will not meet. For this reason, it is not recommended to build an aggregated network adding fictitious edges and putting on the same plan phone calls and group meetings. A complete picture can only be obtained by considering the two networks as a whole multilayer network.

The multilayer degree is a simple and introductory tool which already highlights the usefulness of the multilayer approach by bringing out the importance of actors that do not emerge by studying the two networks separately.

We expect that also the study of the shortest paths in the multilayer network will provide useful information about the relationships within the criminal organization. The shortest path distribution on the single-layer networks shows that *PC* has a greater shortest path caused by its lower density with respect to *MN* (see Fig. 1.8).

Conclusions and future work

This thesis paves the way to a new branch of criminal network analysis by providing a new perspective on how SNA methods can help LEAs. Network science and graph theory tools have been applied on real covert networks with the aim to discover new ways to apply SNA on police investigations.

The central part of the study is about two criminal networks (*i.e.*, Meetings and Phone Calls) extracted from the outcome of an anti-mafia law enforcement operation called Montagna against individuals charged for participating in a mafia association. This study is interesting per se as the pre-trial detention order from which two networks was extracted concerns the birth and growth of a branch of the Sicilian Mafia in the North-Eastern part of Sicily, a territory historically under the control of the Palermo and Catania families.

Other seven datasets of real covert networks were analyzed. More specifically, two datasets regard Mafia operations (*i.e.*, Infinito and Oversize), and the remaining ones refer to other dark networks, including street gangs, drug traffics, or terrorist networks (*i.e.*, Stockholm street gangs, Caviar Project, Philippines Kidnappers).

An open issue in the application of SNA to covert network studies has to do with data collection. SNA techniques rely on real-world information, which is used to build the networks. However, data incompleteness and unreliability have been shown to be among the biggest issues in the field, since the collection of complete data is a virtually impossible task, with bias being inevitable too. This is due to the nature of such kind of networks: covert networks should be seen as complex adaptive systems that show unpredictability and covertness in their structures, behaviors and activities.

The risk of biases in the collection of data by LEAs appears to be a major issue in both micro and macro approaches. In the first case, greater volume of data on an individual may suggest either a high level of activity by that actor or major attention by police. Such issue is difficult to untangle, but shows the importance of interpreting findings in light of local operational experience and knowledge. The variable quality in intelligence data, known as the problem of signal and noise, can indeed create a false impression of the situation. Limitations suffered from each data source can be partially addressed by combining different data from different LEA sources. Yet, this method is complex, expensive and time-consuming. In the same manner, in case of macro studies, data are a reflection of LEA knowledge of markets and big criminal or terrorist groups. In this case, the reliability and bias problems show to have a greater impact than micro studies.

Inevitably, however, any LEA source is incomplete, and will always suffer from missing data. This means that, in order to draw meaningful conclusions about the network structure, resilience and dynamics, an understanding of both law enforcement and the criminal environment is necessary.

Moreover, novel information metrics need to be developed to better understand the effects of node manipulation in such networks. Most of the studies are based on static observations of criminal groups. Being the dynamics one of the main features of such networks, more studies should focus on the disclosure of the mechanisms that involve the dynamics of these networks. This is indeed a non trivial task and only a profound integration of different scientific fields could bring the basis and the tools to uncover the complexity of their dynamics.

In particular, the problem of missing edges (*i.e.* the lack of information on the relations between two known criminals) can be solved through the application of link prediction algorithm. LEAs, in fact, may miss a lot of criminal activities such as meetings or phone calls, and therefore relevant plans of a criminal organization.

Graph distances can be used to quantify the impact of incomplete data and to determine what kind of covert network mostly suffers from it. The same distances can be used to compare covert networks with network models. LEAs may need network models to predict and prevent the creation of relationship ties between criminals or to break those ties by arresting one or more of the suspects.

Another problem is the scarcity of data availability in case of micro studies of criminal groups, such as criminal gangs and Mafia. Most of the studies in literature focus indeed on macro studies of terrorist activity. Only future collaborations between academic practitioners and LEAs would eventually open the doors to a greater growth in the amount of available empirical data, which is needed to develop more studies and to fill more gaps.

One of the most common SNA applications to study crime is the use of centrality measures to identify leaders in covert networks. The concept of centrality as importance is debated and strongly depends on the context. Several measures can be used to measuring the centrality of individual nodes such as degree centrality, closeness centrality, betweenness centrality and clustering coefficient. There are only a few metrics to measure centrality of individual edges such as the edge betweenness centrality. All of these metrics are typically studied for graphs of relatively small size. However, in the last few years, the proliferation of digital collection of data has led to huge graphs with billions of nodes and edges. For these reasons, new computationally light alternatives, such as Game of Thieve or WERW-Kpath, could be used and tested on covert network that perfectly reproduce the characteristics of larger networks.

The analysis of the most central actor can be done also following a multilayer approach. Single graphs extracted from the same police investigation can be used to create a multilayer network where each layer represents a different kind of edge. An actor can be central in a certain layer and not be central in an other layer, nor for the multilayer network. It can be useful to compare the study of the single layers with the analysis of multiple layers within a covert network to obtain a more nuanced understanding of the structure of the network, and of the strategic position of actors in the network. In this thesis, the Montagna multilayer network was presented. We are currently working on a new multilayer network with a third layer in which nodes are suspected criminals and edges are the crimes they have committed together. We are using the Python module *uunet.multinet*[1] created by Magnani, Rossi and Vega to analyze this network through actor and layer measures (Ficara et al., 2022c).

SNA allows to understand how a network functions and how it could be broken. Strategies and literature applications for covert network disruption are classified in three approaches: the human capital, the social capital and finally the mixed approach. The first approach consists in weakening a criminal organization by identifying and removing high human capital figures. This includes individuals who provide the organization with their specialized knowledge, skills, competences and expertise. The second approach identifies key actors based on their centrality in terms

[1] Available at: `https://bitbucket.org/uuinfolab/py_multinet/src/master/`

of the network theory. By definition, a social network is based on social ties, so central individuals are indeed evaluated purely upon their social connections within the network. In the mixed approach, nodes to be removed are chosen based on a combination of a SNA metric and the role played within the network. Actors with higher reputation are more prone to present high values of centrality, being more visible in the organization.

Criminal networks are able to withstand disruption and to adapt in face of diverse dismantling attempts. This ability is called network resilience. Resilience is here classified upon the different types of covert networks and in terms of network features such as vulnerability, elasticity and adaptive capacity.

We are currently working on the application of a mixed approach on the Montagna networks which consists in the removal of actors according to the maximal degree, betweenness, closeness, and also according to special skills or knowledge (Ficara et al., 2022b). To this end, it was built a labeled graph where each node possesses a specific role according to the judicial documents of the Montagna operation. Node removal stops when the network is completely disrupted. This kind of study can help to identify the key roles to target during an anti-mafia investigation. Moreover, after having identified the network model that better reproduces a Mafia network, we can proceed to rank nodes in the model, and try to disrupt it removing the nodes having the same rank of the ones with a key role in Mafia networks. In this way, we are trying to create a network model for criminal network disruption using an artificial network with the same characteristics of a Mafia network.

Bibliography

Abraham, R., Marsden, J., and Ratiu, T. (1988). *Manifolds, Tensor Analysis, and Applications: 2nd Edition*. Berlin, Heidelberg: Springer-Verlag. DOI: 10.1007/978-1-4612-1029-0.

Adamic, L. and Adar, E. (2003). "Friends and neighbors on the Web". In: *Social Networks* 25.3, pp. 211–230. DOI: 10.1016/S0378-8733(03)00009-1.

Adger, N. (2000). "Social and ecological resilience: are they related?" In: *Progress in Human Geography* 24.3, pp. 347–364. DOI: 10.1191/030913200701540465.

Agreste, S. et al. (2016). "Network structure and resilience of Mafia syndicates". In: *Information Sciences* 351, pp. 30–47. DOI: 10.1016/j.ins.2016.02.027.

Akoglu, L., Tong, H., and Koutra, D. (2015). "Graph based anomaly detection and description: a survey". In: *Data Mining and Knowledge Discovery* 29.3, pp. 626–688. DOI: 10.1007/s10618-014-0365-y.

Albert, R. and Barabási, A.-L. (2000). "Topology of Evolving Networks: Local Events and Universality". In: *Phys. Rev. Lett.* 85 (24), pp. 5234–5237. DOI: 10.1103/PhysRevLett.85.5234.

Athey, N. and Bouchard, M. (2013). "The BALCO scandal: the social structure of a steroid distribution network". In: *Global Crime* 14.2-3, pp. 216–237. DOI: 10.1080/17440572.2013.790312.

Avrachenkov, K., Chebotarev, P., and Rubanov, D. (2019). "Similarities on graphs: Kernels versus proximity measures". In: *European Journal of Combinatorics* 80, pp. 47–56. DOI: 10.1016/j.ejc.2018.02.002.

Ayling, J. (2009). "Criminal organizations and resilience". In: *International Journal of Law, Crime and Justice* 37.4, pp. 182 –196. DOI: 10.1016/j.ijlcj.2009.10.003.

— (2013). "What Sustains Wildlife Crime? Rhino Horn Trading and the Resilience of Criminal Networks". In: *Journal of International Wildlife Law & Policy* 16.1, pp. 57–80. DOI: 10.1080/13880292.2013.764776.

Bader, D. A. and Madduri, K. (2006). "Parallel Algorithms for Evaluating Centrality Indices in Real-world Networks". In: *2006 International Conference on Parallel Processing (ICPP'06)*, pp. 539–550. DOI: 10.1109/ICPP.2006.57.

Baker, W. and Faulkner, R. (1993). "The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry". In: *American Sociological Review* 58.6, pp. 837–860.

Barabási, A.-L. and Albert, R. (1999). "Emergence of Scaling in Random Networks". In: *Science* 286.5439, pp. 509–512. DOI: 10.1126/science.286.5439.509.

Barabási, A.-L. and Pósfai, M. (2016). *Network science*. Cambridge University Press.

Battiston, F., Nicosia, V., and Latora, V. (2014). "Structural measures for multiplex networks". In: *Phys. Rev. E* 89 (3), p. 032804. DOI: 10.1103/PhysRevE.89.032804.

Berlusconi, G. (2013). "Do all the pieces matter? Assessing the reliability of law enforcement data sources for the network analysis of wire taps". In: *Global Crime* 14.1, pp. 61–81. DOI: 10.1080/17440572.2012.746940.

— (2017). "Social Network Analysis and Crime Prevention". In: *Crime Prevention in the 21st Century: Insightful Approaches for Crime Prevention Initiatives*. Ed. by B.

LeClerc and E. Savona. Cham: Springer International Publishing, pp. 129–141. DOI: 10.1007/978-3-319-27793-6_10.

Berlusconi, G. et al. (2016). "Link Prediction in Criminal Networks: A Tool for Criminal Intelligence Analysis". In: *PLOS ONE* 11.4, pp. 1–21. DOI: 10.1371/journal.pone.0154244.

Boccaletti, S. et al. (2014). "The structure and dynamics of multilayer networks". In: *Physics Reports* 544.1, pp. 1–122. DOI: 10.1016/j.physrep.2014.07.001.

Bodin, P. and Wiman, B. (2004). "Resilience and Other Stability Concepts in Ecology: Notes on their Origin, Validity, and Usefulness". In: *ESS Bulletin* 2, pp. 33–43.

Bonacich, P. (1987). "Power and Centrality: A Family of Measures". In: *American Journal of Sociology* 92.5, pp. 1170–1182.

Bonanno, G. (2004). "Loss, Trauma, and Human Resilience: Have We Underestimated the Human Capacity to Thrive After Extremely Aversive Events?" In: *The American psychologist* 59, pp. 20–8. DOI: 10.1037/0003-066X.59.1.20.

Borgatti, S. (2006). "Identifying Sets of Key Players in a Social Network". In: *Computational & Mathematical Organization Theory* 12, pp. 21–34. DOI: 10.1007/s10588-006-7084-x.

Borgatti, S., Everett, M., and Freeman, L. (2002). *UCINET for Windows: Software for social network analysis*.

Bouchard, M. (2007). "On the Resilience of Illegal Drug Markets". In: *Global Crime* 8, pp. 325–344. DOI: 10.1080/17440570701739702.

— (2020). "Collaboration and Boundaries in Organized Crime: A Network Perspective". In: *Crime and Justice* 49. DOI: 10.1086/708435.

Bouchard, M. and Malm, A. (2016). *Social network analysis and its contribution to research on crime and criminal justice*. Oxford Handbooks Online. DOI: 10.1093/oxfordhb/9780199935383.013.21.

Bouchard, M. and Ouellet, F. (2011). "Is small beautiful? The link between risks and size in illegal drug markets". In: *Global Crime* 12.1, pp. 70–86. DOI: 10.1080/17440572.2011.548956.

Brandes, U. (2008). "On variants of shortest-path betweenness centrality and their generic computation". In: *Social Networks* 30.2, pp. 136–145. DOI: 10.1016/j.socnet.2007.11.001.

Bright, D., Greenhill, C., and Levenkova, N. (2013). "Dismantling Criminal Networks: Can Node Attributes Play a Role?" In: *Crime and Networks*. Ed. by C. Morselli. Routledge, pp. 148–162. DOI: 10.4324/9781315885018.

Bright, D. et al. (2015). "Networks within networks: using multiple link types to examine network structure and identify key actors in a drug trafficking operation". In: *Global Crime* 16.3, pp. 219–237. DOI: 10.1080/17440572.2015.1039164.

Bright, D. et al. (2017). "Criminal network vulnerabilities and adaptations". In: *Global Crime* 18.4, pp. 424–441. DOI: 10.1080/17440572.2017.1377614.

Brown, R. and Velásquez, A. (2017). "The effect of violent crime on the human capital accumulation of young adults". In: *Journal of Development Economics* 127, pp. 1–12. DOI: 10.1016/j.jdeveco.2017.02.004.

Bruinsma, G. and Bernasco, W. (2004). "Criminal groups and transnational illegal markets". In: *Crime, Law and Social Change* 41.1, pp. 79–94. DOI: 10.1023/B:CRIS.0000015283.13923.aa.

Burcher, M. (2020). "Social Network Analysis and Crime Intelligence". In: *Social Network Analysis and Law Enforcement: Applications for Intelligence Analysis*. Cham: Springer International Publishing, pp. 65–93. DOI: 10.1007/978-3-030-47771-4_3.

Burcher, M. and Whelan, C. (2015). “Social network analysis and small group ‘dark’ networks: an analysis of the London bombers and the problem of ‘fuzzy’ boundaries”. In: *Global Crime* 16.2, pp. 104–122. DOI: 10.1080/17440572.2015.1005363.

— (2018). “Social network analysis as a tool for criminal intelligence: understanding its potential from the perspectives of intelligence analysts”. In: *Trends in Organized Crime* 21.3, pp. 278–294. DOI: 10.1007/s12117-017-9313-8.

Burt, R. (1992). *Structural Holes: The Social Structure of Competition*. Harvard University Press.

— (2007). *Brokerage and Closure: An Introduction to Social Capital*. Clarendon lectures in management studies. Oxford University Press.

Burt, R., Jannotta, J., and Mahoney, J. (1998). “Personality correlates of structural holes”. In: *Social Networks* 20.1, pp. 63–87. DOI: 10.1016/S0378-8733(97)00005-1.

Calderoni, F. (2012). “The structure of drug trafficking mafias: The ’Ndrangheta and cocaine”. In: *Crime, Law and Social Change* 58. DOI: 10.1007/s10611-012-9387-9.

— (2014). “Identifying Mafia Bosses from Meeting Attendance”. In: *Networks and Network Analysis for Defence and Security*. Ed. by A. Masys. Cham: Springer International Publishing, pp. 27–48. DOI: 10.1007/978-3-319-04147-6_2.

— (2015). “Predicting Organized Crime Leaders”. In: pp. 89–110. URL: http://hdl.handle.net/10807/68084.

Calderoni, F., Brunetto, D., and Piccardi, C. (2017). “Communities in criminal networks: A case study”. In: *Social Networks* 48, pp. 116–125. DOI: 10.1016/j.socnet.2016.08.003.

Calderoni, F. and Piccardi, C. (2014). “Uncovering the Structure of Criminal Organizations by Community Analysis: The Infinito Network”. In: *2014 Tenth International Conference on Signal-Image Technology and Internet-Based Systems*, pp. 301–308. DOI: 10.1109/SITIS.2014.20.

Calderoni, F. and Superchi, E. (2019). “The nature of organized crime leadership: criminal leaders in meeting and wiretap networks”. In: *Crime, Law and Social Change* 72.4, pp. 419–444. DOI: 10.1007/s10611-019-09829-6.

Calderoni, F. et al. (2020). “Robust link prediction in criminal networks: A case study of the Sicilian Mafia”. In: *Expert Systems with Applications* 161, p. 113666. DOI: 10.1016/j.eswa.2020.113666.

Campana, P. (2016). “Explaining criminal networks: Strategies and potential pitfalls”. In: *Methodological Innovations* 9, p. 2059799115622748. DOI: 10.1177/2059799115622748.

Campana, P. and Federico, V. (2013). “Cooperation in criminal organizations: Kinship and violence as credible commitments”. In: *Rationality and Society* 25, pp. 263–289. DOI: 10.1177/1043463113481202.

Campana, P. and Varese, F. (2012). “Listening to the wire: criteria and techniques for the quantitative analysis of phone intercepts”. In: *Trends in Organized Crime* 15.1, pp. 13–30. DOI: 10.1007/s12117-011-9131-3.

Carley, K., Lee, J.-S., and Krackhardt, D. (2001). “Destabilizing Networks”. In: *Connections* 24.3, pp. 79–92.

Carley, K., Reminga, J., and Borgatti, S. (2003). “Destabilizing dynamic networks under conditions of uncertainty”. In: *IEMC ’03 Proceedings. Managing Technologically Driven Organizations: The Human Side of Innovation and Change*. Cambridge: IEEE, pp. 121–126.

Catanese, S. (2017). “New perspectives in criminal network analysis: multilayer networks, time evolution, and visualization”. PhD thesis. University of Catania.

Catanese, S., De Meo, P., and Fiumara, G. (2016). “Resilience in criminal networks”. In: *Atti della Accademia Peloritana dei Pericolanti - Classe di Scienze Fisiche, Matematiche e Naturali* 94.2. DOI: 10.1478/AAPP.942A1.

Catanese, S. et al. (2014). “Detecting criminal organizations in mobile phone networks”. In: *Expert Systems with Applications* 41.13, pp. 5733–5750.

Cavallaro, L. et al. (2020a). *Criminal Network: The Sicilian Mafia. “Montagna Operation”*. Zenodo. DOI: 10.5281/zenodo.3938818.

— (2020b). “Disrupting resilient criminal networks through data analysis: The case of Sicilian Mafia”. In: *Plos One* 15.8, pp. 1–22. DOI: 10.1371/journal.pone.0236476.

Cavallaro, L. et al. (2021). “Graph Comparison and Artificial Models for Simulating Real Criminal Networks”. In: *Complex Networks & Their Applications IX*. Ed. by R. Benito et al. Cham: Springer International Publishing, pp. 286–297. DOI: 10.1007/978-3-030-65351-4_23.

Charette, Y. and Papachristos, A. (2017). “The network dynamics of co-offending careers”. In: *Social Networks* 51, pp. 3–13.

Chen, H.-c. et al. (2004). “Crime data mining: a general framework and some examples”. In: *Computer* 37.4, pp. 50–56. DOI: 10.1109/MC.2004.1297301.

Chen, P. and Popovich, P. (2002). *Correlation: parametric and nonparametric measures*. Sage university papers series. No. 07-139. Sage Publications.

Coleman, J. (1990). *Foundations of Social Theory*. Harvard University: Belknap Press.

Cornish, D. (1994). “The Procedural Analysis of Offending and its Relevance for Situational Prevention”. In: *Crime Prevention Studies*. Vol. 3. New York: Criminal Justice Press, pp. 151–196.

Curry, D. (2011). “Gangs, crime, and terrorism”. In: *Criminologists on terrorism and homeland security*, pp. 97–112.

de Andrade, R. et al. (2021). “Energy disruptive centrality with an application to criminal network”. In: *Communications in Nonlinear Science and Numerical Simulation* 99, p. 105834. DOI: 10.1016/j.cnsns.2021.105834.

De Domenico, M., Porter, M. A., and Arenas, A. (2014). “MuxViz: a tool for multilayer analysis and visualization of networks”. In: *Journal of Complex Networks* 3.2, pp. 159–176. DOI: 10.1093/comnet/cnu038.

De Domenico, M. et al. (2013). “Mathematical Formulation of Multilayer Networks”. In: *Phys. Rev. X* 3 (4), p. 041022. DOI: 10.1103/PhysRevX.3.041022.

De Domenico, M. et al. (2015). “Ranking in interconnected multilayer networks reveals versatile nodes”. In: *Nature Communications* 6.1, p. 6868. DOI: 10.1038/ncomms7868.

De Meo, P. et al. (2012). “A novel measure of edge centrality in social networks”. In: *Knowledge Based Systems* 30, pp. 136–150. DOI: 10.1016/j.knosys.2012.01.007.

De Meo, P. et al. (2013). “Enhancing community detection using a network weighting strategy”. In: *Information Sciences* 222, pp. 648–668. DOI: 10.1016/j.ins.2012.08.001.

— (2014). “Mixing local and global information for community detection in large networks”. In: *Journal of Computer and System Sciences* 80.1, pp. 72–87. DOI: 10.1016/j.jcss.2013.03.012.

Decker, S. and Pyrooz, D. (2011). “Gangs, terrorism, and radicalization”. In: *Journal of Strategic Security* 4.4, pp. 151–166.

Degani, E. (2016). *Monoplex to Multiplex networks analysis generalization: formalization, description and implementation of the commonest measures via a statistical package*. BSc thesis. University of Padua.

Dehghanniri, H. and Borrion, H. (2021). "Crime scripting: A systematic review". In: *European Journal of Criminology* 18.4, pp. 504–525. DOI: 10.1177/1477370819850943.

Dickison, M., Magnani, M., and Rossi, L. (2016). *Multilayer Social Networks*. Cambridge University Press. DOI: 10.1017/CBO9781139941907.

Donnat, C. and Holmes, S. (2018). "Tracking network dynamics: A survey using graph distances". In: *The Annals of Applied Statistics* 12.2, pp. 971–1012. DOI: 10.1214/18-AOAS1176.

Duijn, P., Kashirin, V., and Sloot, P. (2014). "The Relative Ineffectiveness of Criminal Network Disruption". In: *Scientific Reports* 4.1, p. 4238. DOI: 10.1038/srep04238.

Duijn, P. and Klerks, P. (2014). "Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement". In: *Networks and Network Analysis for Defence and Security*. Cham: Springer International Publishing, pp. 121–159. DOI: 10.1007/978-3-319-04147-6_6.

Duijn, P. and Sloot, P. (2015). "From data to disruption". In: *Digital Investigation* 15. Special Issue: Big Data and Intelligent Data Analysis, pp. 39–45. DOI: 10.1016/j.diin.2015.09.005.

Duxbury, S. and Haynie, D. (2019). "Criminal network security: An agent-based approach to evaluating network resilience*". In: *Criminology* 57.2, pp. 314–342. DOI: 10.1111/1745-9125.12203.

Emmert-Streib, F., Dehmer, M., and Shi, Y. (2016). "Fifty years of graph matching, network alignment and network comparison". In: *Information Sciences* 346-347, pp. 180 –197. DOI: 10.1016/j.ins.2016.01.074.

Erdös, P. and Rényi, A. (1959). "On Random Graphs I". In: *Publicationes Mathematicae Debrecen* 6, p. 290.

Erickson, B. (1981). "Secret Societies and Social Structure". In: *Social Forces* 60.1, pp. 188–210.

Everton, S. (2012). *Disrupting Dark Networks*. Structural Analysis in the Social Sciences. Cambridge University Press. DOI: 10.1017/CBO9781139136877.

Farley, J. (2003). "Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making)". In: *Studies in Conflict & Terrorism* 26.6, pp. 399–411. DOI: 10.1080/10576100390242857.

Faust, K. and Tita, G. (2019). "Social Networks and Crime: Pitfalls and Promises for Advancing the Field". In: *Annual Review of Criminology* 2.1, pp. 99–122. DOI: 10.1146/annurev-criminol-011518-024701.

Ferrara, E. et al. (2014). "Visualizing criminal networks reconstructed from mobile phone records". In: *CEUR Workshop Proceedings* 1210.

Ficara, A. et al. (2020). "Social Network Analysis of Sicilian Mafia Interconnections". In: *Complex Networks and Their Applications VIII*. Ed. by H. Cherifi et al. Cham: Springer International Publishing, pp. 440–450. DOI: 10.1007/978-3-030-36683-4_36.

Ficara, A. et al. (2021a). "Correlation analysis of node and edge centrality measures in artificial complex networks". In: *Proceedings of Sixth International Congress on Information and Communication Technology*. Ed. by X.-S. Yang et al. Cham: Springer International Publishing. DOI: 10.1007/978-3-030-81854-8_2.

— (2021b). "Correlations Among Game of Thieves and Other Centrality Measures in Complex Networks". In: *Data Science and Internet of Things: Research and Applications at the Intersection of DS and IoT*. Ed. by G. Fortino et al. Cham: Springer International Publishing, pp. 43–62. DOI: 10.1007/978-3-030-67197-6_3.

Ficara, A. et al. (2021c). "Criminal networks analysis in missing data scenarios through graph distances". In: *PLOS ONE* 16.8, pp. 1–18. DOI: 10.1371/journal.pone.0255067.

Ficara, A. et al. (2021d). "Game of Thieves and WERW-Kpath: Two Novel Measures of Node and Edge Centrality for Mafia Networks". In: *Complex Networks XII*. Ed. by A. Teixeira et al. Cham: Springer International Publishing, pp. 12–23. DOI: 10.1007/978-3-030-81854-8_2.

Ficara, A. et al. (2021e). "Multilayer Network Analysis: The Identification of Key Actors in a Sicilian Mafia Operation". In: *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*. Ed. by D. Perakovic and L. Knapcikova. Cham: Springer International Publishing, pp. 120–134. DOI: 10.1007/978-3-030-78459-1_9.

Ficara, A. et al. (2021f). "Social network analysis: the use of graph distances to compare artificial and criminal networks". In: *J Smart Environ Green Comput* 1, pp. 159–172. DOI: 10.20517/jsegc.2021.08.

Ficara, A. et al. (2022a). *Covert Network Constructing, Disruption and Resilience: A survey*. (submitted).

Ficara, A. et al. (2022b). *Human and social capital strategies for Mafia network disruption*. (submitted).

Ficara, A. et al. (2022c). *The whole is greater than the sum of the parts: a multilayer approach on criminal networks*. (submitted).

Freeman, L. (1978). "Centrality in social networks conceptual clarification". In: *Social Networks* 1.3, pp. 215–239. DOI: 10.1016/0378-8733(78)90021-7.

Gambetta, D. (1993). *The sicilian mafia*. Cambridge: Harvard University Press.

— (1996). *The Sicilian Mafia: The Business of Private Protection*. Cambridge: Harvard University Press.

Gambetta, D. and Reuter, P. (1995). "Conspiracy among the many: the Mafia in legitimate industries". In: *The Economic Dimensions of Crime*. Springer, pp. 99–120. DOI: 10.1007/978-1-349-62853-7_5.

Gerdes, L., Ringler, K., and Autin, B. (2014). "Assessing the Abu Sayyaf Group's Strategic and Learning Capacities". In: *Studies in Conflict & Terrorism* 37.3, pp. 267–293. DOI: 10.1080/1057610X.2014.872021.

Gilbert, E. (1959). "Random Graphs". In: *Ann. Math. Statist.* 30.4, pp. 1141–1144. DOI: 10.1214/aoms/1177706098.

Goodman, L. (1961). "Snowball Sampling". In: *The Annals of Mathematical Statistics* 32.1, pp. 148–170. DOI: 10.1214/aoms/1177705148.

Gottschalk, P. (2009). "Value configurations in organised crime". In: *Policing and Society* 19.1, pp. 47–57. DOI: 10.1080/10439460802457701.

Gould, R. and Fernandez, R. (1989). "Structures of Mediation: A Formal Approach to Brokerage in Transaction Networks". In: *Sociological Methodology* 19, pp. 89–126.

Grassi, R. et al. (2019). "Betweenness to assess leaders in criminal networks: New evidence using the dual projection approach". In: *Social Networks* 56, pp. 23–32. DOI: 10.1016/j.socnet.2018.08.001.

Grover, A. and Leskovec, J. (2016). "node2vec: Scalable Feature Learning for Networks". In: *Proc. of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. San Francisco, CA, USA: ACM, pp. 855–864. DOI: 10.1145/2939672.2939754.

Gunderson, L. and Holling, C. (2001). *Panarchy: Understanding Transformations in Human and Natural Systems*. Island Press.

Hagberg, A., Schult, D., and Swart, P. (2008). "Exploring Network Structure, Dynamics, and Function using NetworkX". In: *Proceedings of the 7th Python in Science*

Conference. Ed. by G. Varoquaux, T. Vaught, and J. Millman. Pasadena, CA, USA, pp. 11–15.

Handmer, J. and Dovers, S. (1996). "A Typology of Resilience: Rethinking Institutions for Sustainable Development". In: *Industrial & Environmental Crisis Quarterly* 9.4, pp. 482–511. DOI: 10.1177/108602669600900403.

Hardy, J. and Bell, P. (2020). "Resilience in sophisticated financial crime networks: a social network analysis of the Madoff Investment Scheme". In: *Crime Prevention and Community Safety* 22.3, pp. 223–247. DOI: 10.1057/s41300-020-00094-7.

Hartle, H. et al. (2020). "Network comparison and the within-ensemble graph distance". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 476, p. 20190744. DOI: 10.1098/rspa.2019.0744.

Hastie, T., Tibshirani, R., and Friedman, J. (2009). *The elements of statistical learning: data mining, inference, and prediction*. Springer Science & Business Media.

Heber, A. (2009). "The networks of drug offenders". In: *Trends in Organized Crime* 12, pp. 1–20. DOI: 10.1007/s12117-008-9055-8.

Holling, C. (1961). "Principles of Insect Predation". In: *Annual Review of Entomology* 6.1, pp. 163–182. DOI: 10.1146/annurev.en.06.010161.001115.

Holme, P. and Kim, B. J. (2002). "Growing scale-free networks with tunable clustering". In: *Phys. Rev. E* 65 (2), p. 026107. DOI: 10.1103/PhysRevE.65.026107.

Hric, D., Peixoto, T., and Fortunato, S. (2016). "Network structure, metadata, and the prediction of missing nodes and annotations". In: *Physical Review X* 6.3, p. 031038. DOI: 10.1103/PhysRevX.6.031038.

Hutchins, C. and Benham-Hutchins, M. (2010). "Hiding in plain sight: criminal network analysis". In: *Computational and Mathematical Organization Theory* 16.1, pp. 89–111. DOI: 10.1007/s10588-009-9060-8.

Ianni, F. and Reuss-Ianni, E. (1990). "Network Analysis". In: *Criminal Intelligence Analysis*. Ed. by Paul Andrews, Jr and M. Peterson, pp. 67–84.

Jaccard, P. (1912). "The Distribution of the Flora in the Alpine Zone". In: *New Phytologist* 11.2, pp. 37–50. DOI: 10.1111/j.1469-8137.1912.tb05611.x.

Jamour, F., Skiadopoulos, S., and Kalnis, P. (2018). "Parallel Algorithm for Incremental Betweenness Centrality on Large Graphs". In: *IEEE Transactions on Parallel and Distributed Systems* 29.3, pp. 659–672. DOI: 10.1109/TPDS.2017.2763951.

Jupp, V. (2012). *Methods of Criminological Research*. Taylor & Francis.

Kang, U et al. (2011). "Centralities in Large Networks: Algorithms and Observations". In: *Proceedings of the 11th SIAM International Conference on Data Mining, SDM 2011*, pp. 119–130. DOI: 10.1137/1.9781611972818.11.

Katz, L. (1953). "A new status index derived from sociometric analysis". In: *Psychometrika* 18.1, pp. 39–43. DOI: 10.1007/BF02289026.

Keeley, B. (2007). *Human Capital*. OECD Publications and Information Centre, p. 150. DOI: 10.1787/9789264029095-en.

Kendall, M. and Gibbons, J. (1990). *Rank Correlation Methods*. Charles Griffin Book. E. Arnold.

Kenney, M. (2007). *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. Penn State University Press.

Kim, M. and Leskovec, J. (2011). "The network completion problem: Inferring missing nodes and edges in networks". In: *Proc. of the SIAM International Conference on Data Mining (SDM 2011)*. Mesa, Arizona, USA: SIAM, pp. 47–58. DOI: 10.1137/1.9781611972818.5.

Kivelä, M. et al. (2014). "Multilayer networks". In: *Journal of Complex Networks* 2.3, pp. 203–271. DOI: 10.1093/comnet/cnu016.

Kleemans, E. and van de Bunt, H. (1999). “The social embeddedness of organized crime”. In: *Transnational Organized Crime* 1999.5, pp. 19–36.

Klein, M. and Maxson, C. (2006). *Street Gang Patterns and Policies*. Oxford University Press. DOI: 10.1093/acprof:oso/9780195163445.001.0001.

Klerks, P. (2003). “The Network Paradigm Applied to Criminal Organisations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands”. In: *Connections* 24, pp. 53–65.

Koutra, D., Vogelstein, J., and Faloutsos, C. (2013). “DELTACON: A Principled Massive-Graph Similarity Function”. In: *Proceedings of the 2013 SIAM International Conference on Data Mining*, pp. 162–170. DOI: 10.1137/1.9781611972832.18.

Krebs, V. (2002). “Mapping Networks of Terrorist Cells”. In: *Connections* 24.3, pp. 43–52.

Kulig, J. et al. (2013). “Community Resiliency: Emerging Theoretical Insights”. In: *Journal of Community Psychology* 41.6, pp. 758–775. DOI: 10.1002/jcop.21569.

Lauchs, M., Keast, R., and Chamberlain, D. (2012). “Resilience of a corrupt police network: the first and second jokes in Queensland”. In: *Crime, law and social change* 57.2, pp. 195–207.

Leicht, E., Holme, P., and Newman, M. (2006). “Vertex similarity in networks”. In: *Physical review. E, Statistical, nonlinear, and soft matter physics* 73.2, p. 026120. DOI: 10.1103/PhysRevE.73.026120.

Lengnick-Hall, C. and Beck, T. (2005). “Adaptive Fit Versus Robust Transformation: How Organizations Respond to Environmental Change”. In: *Journal of Management* 31.5, pp. 738–757. DOI: 10.1177/0149206305279367.

Liben-Nowell, D. and Kleinberg, J. (2003). “The Link Prediction Problem for Social Networks”. In: *Proceedings of the Twelfth International Conference on Information and Knowledge Management*. CIKM ’03. New York, NY, USA: Association for Computing Machinery, 556–559. DOI: 10.1145/956863.956972.

Lin, N., Cook, K., and Burt, R. (2001). *Social Capital: Theory and Research*. Sociology and economics: controversy and integration: an Aldine de Gruyter series of texts and monographs. Piscataway: Transaction Publishers.

Luers, A. et al. (2003). “A method for quantifying vulnerability, applied to the agricultural system of the Yaqui Valley, Mexico”. In: *Global Environmental Change* 13.4, pp. 255–267. DOI: 10.1016/S0959-3780(03)00054-2.

Lusseau, D. et al. (2003). “The bottlenose dolphin community of Doubtful Sound features a large proportion of long-lasting associations”. In: *Behavioral Ecology and Sociobiology* 54.4, pp. 396–405. DOI: 10.1007/s00265-003-0651-y.

Madduri, K. et al. (2009). “A faster parallel algorithm and efficient multithreaded implementations for evaluating betweenness centrality on massive datasets”. In: *2009 IEEE International Symposium on Parallel Distributed Processing*, pp. 1–8. DOI: 10.1109/IPDPS.2009.5161100.

Malm, A. and Bichler, G. (2011). “Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets”. In: *Journal of Research in Crime and Delinquency* 48, pp. 271–297. DOI: 10.1177/0022427810391535.

Malm, A., Bichler, G., and Walle, S. (2010). “Comparing the ties that bind criminal networks: Is blood thicker than water?” In: *Security Journal* 23, pp. 52–74. DOI: 10.1057/sj.2009.18.

Mastrobuoni, G. and Patacchini, E. (2012). “Organized Crime Networks: an Application of Network Analysis Techniques to the American Mafia”. In: *Review of Network Economics* 11. DOI: 10.1515/1446-9022.1324.

Mastrobuoni, G., Patacchini, E., et al. (2010). "Understanding organized crime networks: Evidence based on federal bureau of narcotics secret files on american mafia". In: *Carlo Alberto Notebooks* 152, pp. 1–58.

McCarthy, B. and Hagan, J. (2001). "When Crime Pays: Capital, Competence, and Criminal Success*". In: *Social Forces* 79.3, pp. 1035–1060. DOI: 10.1353/sof.2001.0027.

McDowell, D. (2008). *Strategic intelligence: a handbook for practitioners, managers, and users*. Vol. 5. Scarecrow Press.

McGloin, J. (2005). "Policy and Intervention Considerations of a Network Analysis of Street Gangs*". In: *Criminology & Public Policy* 4.3, pp. 607–635. DOI: 10.1111/j.1745-9133.2005.00306.x.

McLaughlin, A. and Bader, D. A. (2018). "Accelerating GPU Betweenness Centrality". In: *Commun. ACM* 61.8, 85–92. DOI: 10.1145/3230485.

Mocanu, D. C., Exarchakos, G., and Liotta, A. (2018). "Decentralized dynamic understanding of hidden relations in complex networks". In: *Scientific Reports* 8.1, p. 1571. DOI: 10.1038/s41598-018-19356-4.

Morone, F. and Makse, H. (2015). "Influence maximization in complex networks through optimal percolation". In: *Nature* 524.7563, pp. 65–68. DOI: 10.1038/nature14604.

Morselli, C. (2001). "Structuring Mr. Nice: Entrepreneurial opportunities and brokerage positioning in the cannabis trade". In: *Crime, Law and Social Change* 35.3, pp. 203–244. DOI: 10.1023/A:1011272411727.

— (2008). *Inside Criminal Networks*. Studies of Organized Crime. Springer New York.

— (2010). "Assessing Vulnerable and Strategic Positions in a Criminal Network". In: *Journal of Contemporary Criminal Justice* 26.4, pp. 382–392. DOI: 10.1177/1043986210377105.

Morselli, C., Giguère, C., and Petit, K. (2007). "The efficiency/security trade-off in criminal networks". In: *Social Networks* 29.1, pp. 143–153. DOI: 10.1016/j.socnet.2006.05.001.

Morselli, C. and Petit, K. (2007). "Law-Enforcement Disruption of a Drug Importation Network". In: *Global Crime* 8.2, pp. 109–130. DOI: 10.1080/17440570701362208.

Morselli, C. and Roy, J. (2008). "Brokerage Qualifications In Ringing Operations*". In: *Criminology* 46.1, pp. 71–98. DOI: 10.1111/j.1745-9125.2008.00103.x.

Munro, P. (2011). "People smuggling and the resilience of criminal networks in Indonesia". In: *Journal of Policing, Intelligence and Counter Terrorism* 6.1, pp. 40–50. DOI: 10.1080/18335330.2011.553180.

Murphy, K. (2012). *Machine Learning: A Probabilistic Perspective*. Vol. 58. MIT Press.

Natarajan, M. (2000). "Understanding the structure of a drug trafficking organization: a conversational analysis". In: *Crime Prevention Studies* 11, pp. 273–298.

— (2006). "Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data". In: *Journal of Quantitative Criminology* 22.2, pp. 171–192. DOI: 10.1007/s10940-006-9007-x.

Natarajan, M. and Belanger, M. (1998). "Varieties of Drug Trafficking Organizations: A Typology of Cases Prosecuted in New York City". In: *Journal of Drug Issues* 28.4, pp. 1005–1025. DOI: 10.1177/002204269802800410.

Newman, M. (2001). "The structure of scientific collaboration networks". In: *Proceedings of the National Academy of Sciences* 98.2, pp. 404–409. DOI: 10.1073/pnas.98.2.404.

— (2010). *Networks: an Introduction*. Oxford University Press.

Newman, M. (2018). "Estimating network structure from unreliable measurements". In: *Phys. Rev. E* 98 (6), p. 062321. DOI: 10.1103/PhysRevE.98.062321.

Newman, M. and Watts, D. (1999). "Renormalization group analysis of the small-world network model". In: *Physics Letters A* 263.4, pp. 341–346. DOI: 10.1016/S0375-9601(99)00757-4.

Nicosia, V. and Latora, V. (2015). "Measuring and modeling correlations in multiplex networks". In: *Phys. Rev. E* 92 (3), p. 032805. DOI: 10.1103/PhysRevE.92.032805.

Norris, F. et al. (2008). "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness". In: *American Journal of Community Psychology* 41.1-2, pp. 127–150. DOI: 10.1007/s10464-007-9156-6.

Oliver, K. et al. (2014). *Covert networks: structures, processes and types*. Unpublished manuscript, University of Manchester.

Page, L. et al. (1999). *The PageRank Citation Ranking: Bringing Order to the Web.* Technical Report 1999-66. Stanford InfoLab.

Pandey, B. et al. (2019). "A comprehensive survey of edge prediction in social networks: Techniques, parameters and challenges". In: *Expert Systems with Applications* 124, pp. 164–181. DOI: 10.1016/j.eswa.2019.01.040.

Paoli, L. (2002). "The paradoxes of organized crime". In: *Crime, Law and Social Change* 37.1, pp. 51–97. DOI: 10.1023/A:1013355122531.

— (2004). "Italian Organised Crime: Mafia Associations and Criminal Enterprises". In: *Global Crime Today: The Changing Face of Organised Crime* 6.1, pp. 19–32. DOI: 10.1080/1744057042000297954.

— (2008). *Mafia brotherhoods: Organized crime, Italian style*. Oxford University Press. DOI: 10.1093/acprof:oso/9780195157246.001.0001.

Papachristos, A. and Smith, C. (2012). "The Small World of Al Capone: The Embedded and Multiplex Nature of Organized Crime". In: *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2159899.

Peixoto, T. (2018). "Reconstructing Networks with Unknown and Heterogeneous Errors". In: *Phys. Rev. X* 8 (4), p. 041011. DOI: 10.1103/PhysRevX.8.041011.

Peterson, M. (1994). *Applications in Criminal Analysis: A Sourcebook*. Westport: Greenwood Press.

Pfefferbaum, B. et al. (2007). "Building Resilience to Mass Trauma Events". In: *Handbook of Injury and Violence Prevention*. Ed. by L. S. Doll et al. Boston: Springer US, pp. 347–358. DOI: 10.1007/978-0-387-29457-5_19.

Piccardi, C. et al. (2016). *Oversize network*. DOI: 10.6084/m9.figshare.3156067.v1.

Pina e Cunha, M. and Vieira da Cunha, J. (2006). "Toward a complexity theory of strategy". In: *Management Decision* 44, pp. 839–850. DOI: 10.1108/00251740610680550.

Raab, J. (2003). "Dark Networks as Problems". In: *Journal of Public Administration Research and Theory* 13, pp. 413–439. DOI: 10.1093/jpoart/mug029.

Ratner, B. (2009). "The correlation coefficient: Its values range between +1/-1, or do they?" In: *Journal of Targeting, Measurement and Analysis for Marketing* 17.2, pp. 139–142. DOI: 10.1057/jt.2009.5.

Regunta, S. C. et al. (2021). "Efficient parallel algorithms for dynamic closeness and betweenness centrality". In: *Concurrency and Computation: Practice and Experience*, e6650. DOI: 10.1002/cpe.6650.

Reuter, P. and Haaga, J. (1989). *The organization of high-level drug markets: An exploratory study*. Rand Santa Monica.

Ricci, G. and Levi-Civita, T. (1900). "Méthodes de calcul différentiel absolu et leurs applications". In: *Mathematische Annalen* 54.1, pp. 125–201. DOI: 10.1007/BF01454201.

Robins, G. (2009). “Understanding individual behaviors within covert networks: the interplay of individual qualities, psychological predispositions, and network effects”. In: *Trends in Organized Crime* 12.2, pp. 166–187. DOI: 10.1007/s12117-008-9059-4.

— (2015). *Doing social network research: Network-based research design for social scientists*. Sage.

Robinson, D. and Scogings, C. (2018). “The detection of criminal groups in real-world fused data: using the graph-mining algorithm “GraphExtract””. In: *Security Informatics* 7.1, p. 2. DOI: 10.1186/s13388-018-0031-9.

Ross, S. (2017). *Introductory statistics*. Academic Press.

Rostami, A. and Mondani, H. (2015a). *Network complexity data*. DOI: 10.6084/m9.figshare.1297161.v1.

— (2015b). “The Complexity of Crime Network Data: A Case Study of Its Consequences for Crime Control and the Study of Networks”. In: *Plos One* 10.3, pp. 1–20. DOI: 10.1371/journal.pone.0119309.

Rothenberg, R. (2002). “From whole cloth: Making up the terrorist network”. In: *Connections* 24.3, pp. 36–42.

Schwartz, D. and Rouselle, T. (2009). “Using social network analysis to target criminal networks”. In: *Trends in Organized Crime* 12.2, pp. 188–207. DOI: 10.1007/s12117-008-9046-9.

Singh, S., Verma, S., and Tiwari, A. (2020). “A novel method for destabilization of terrorist network”. In: *Modern Physics Letters B* 34.27, p. 2050298. DOI: 10.1142/S021798492050298X.

Solé-Ribalta, A. et al. (2014). “Centrality Rankings in Multiplex Networks”. In: *Proceedings of the 2014 ACM Conference on Web Science*. WebSci ’14. New York, NY, USA: Association for Computing Machinery, 149–155. DOI: 10.1145/2615569.2615687.

Soundarajan, S., Eliassi-Rad, T., and Gallagher, B. (2014). “A Guide to Selecting a Network Similarity Method”. In: pp. 1037–1045. DOI: 10.1137/1.9781611973440.118.

Spapens, T. (2011). “Interaction between criminal groups and law enforcement: the case of ecstasy in the Netherlands”. In: *Global Crime* 12.1, pp. 19–40. DOI: 10.1080/17440572.2011.548955.

Sparrow, M. (1991). “The application of network analysis to criminal intelligence: An assessment of the prospects”. In: *Social Networks* 13.3, pp. 251–274. DOI: 10.1016/0378-8733(91)90008-H.

Spearman, C. (1904). “General Intelligence, Objectively Determined and Measured”. In: *The American Journal of Psychology* 15.2, pp. 201–292. DOI: 10.2307/1412107.

Squartini, T., Mastrandrea, R., and Garlaschelli, D. (2015). “Unbiased sampling of network ensembles”. In: *New Journal of Physics* 17.2, p. 023052. DOI: 10.1088/1367-2630/17/2/023052.

Strang, S. (2014). “Network Analysis in Criminal Intelligence”. In: *Networks and Network Analysis for Defence and Security*. Ed. by A. Masys. Cham: Springer International Publishing, pp. 1–26. DOI: 10.1007/978-3-319-04147-6_1.

Tantardini, M. et al. (2019). “Comparing methods for comparing networks”. In: *Scientific Reports* 9.1, p. 17557. DOI: 10.1038/s41598-019-53708-y.

Tomasini, M. (2015). *An Introduction to Multilayer Networks*. DOI: 10.13140/RG.2.2.16830.18243.

Tremblay, P., Talon, B., and Hurley, D. (2001). “Body Switching and Related Adaptations in the Resale of Stolen Vehicles. Script Elaborations and Aggregate Crime

Learning Curves". In: *The British Journal of Criminology* 41.4, pp. 561–579. DOI: 10.1093/bjc/41.4.561.

Valente, T. et al. (2008). "How Correlated Are Network Centrality Measures?" In: *Connections (Toronto, Ont.)* 28.1, pp. 16–26.

van der Hulst, R. (2009). "Introduction to Social Network Analysis (SNA) as an investigative tool". In: *Trends in Organized Crime* 12.2, pp. 101–121. DOI: 10.1007/s12117-008-9057-6.

Varese, F. (2006). "The structure of a criminal network examined: The Russian Mafia in Rome". In: *Oxford Legal Studies Research Paper* 21.

Villani, S., Mosca, M., and Castiello, M. (2019). "A virtuous combination of structural and skill analysis to defeat organized crime". In: *Socio-Economic Planning Sciences* 65.C, pp. 51–65. DOI: 10.1016/j.seps.2018.01.002.

Wasserman, S. and Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Structural Analysis in the Social Sciences. Cambridge: Cambridge University Press. DOI: 10.1017/CBO9780511815478.

Watts, D. and Strogatz, S. (1998). "Collective dynamics of 'small-world' networks". In: *Nature* 393.6684, pp. 440–442. DOI: 10.1038/30918.

Williams, P. (2001). "Transnational criminal networks". In: *Networks and netwars: the future of terror, crime, and militancy* 1382, p. 61.

Wills, P. and Meyer, F. G. (2020). "Metrics for graph comparison: A practitioner's guide". In: *PLOS ONE* 15.2. Ed. by P.-Y. Chen, e0228728. DOI: 10.1371/journal.pone.0228728.

Wilson, R. and Zhu, P. (2008). "A study of graph spectra for comparing graphs and trees". In: *Pattern Recognition* 41.9, pp. 2833 –2841. DOI: 10.1016/j.patcog.2008.03.011.

Xu, J. and Chen, H. (2008). "The Topology of Dark Networks". In: *Communications of the ACM* 51.10, 58–65. DOI: 10.1145/1400181.1400198.