RMIT UNIVERSITY

Fraud Detection: A Graph Based Anomaly Detection Approach

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

Tahereh Pourhabibi

M.Sc. in Artificial Intelligence, Alzahra University

B.Sc. in Software Engineering, Shahid Beheshti University

School of Accounting, Information Systems and Supply Chain

College of Business and Law

RMIT University

March 2021

Declaration

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the project is the result of work which has been carried out since the official commencement date of the approved research program; any editorial work, paid or unpaid, carried out by a third party is acknowledged; and, ethics procedures and guidelines have been followed.

I acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship.

Tahereh Pourhabibi

16 March, 2021

Acknowledgement

I wish to express my profound appreciation to my supervisory team Professor Booi H. Kam, Dr. Yee Ling Boo, and my external supervisor Associate Professor Kok-Leong Ong (La Trobe University). Their invaluable support, advice, and continuous inspiration enhanced my confidence to accomplish this research. I am indebted to them for their encouragement, and their ability for identifying very fine details, which brought fresh perspective into this research.

Dedication

“To my husband, Mohammad, my best friend and my greatest support.”

Table of Contents

List of Tables

List of Figures

List of Abbreviations

GBAD	graph-based anomaly detection
DSR	design science research
IT	information technology
IS	information system
MDL	minimum description length
OSN	online social network
AML	anti-money laundering
IOF	internal organisational fraud
OCA	online credit application
PR	precision–recall
ROC	receiver operating characteristics
AP	average precision
NMI	normalised mutual information
TPR	true positive rate
FPR	false positive rate
CDF	cumulative distribution function
NDCG	normalised discounted cumulative gain
AUC	area under curve
S	supervised
U	unsupervised
SS	semi-supervised
P	public datasets
SY	synthetic datasets
RW	real-world datasets
FP	false positive
FN	false negative
EM	excess-mass
MV	mass–volume
SNA	social network analysis
SVM	support vector machine
AUROC	area under the receiver operating characteristic curve
AS	asymptotic Surprise
DNE	DarkNetExplorer
KL	kullback–leibler
JI	Jemaah Islamiyah
DI	Darul Islam
LBL	log-bilinear
PMNE	Principled Multilayer Network Embedding
SMNE	Scalable Multiplex Network Embedding
CI	collective influence

Abstract

Advances in communication and digital technologies have created a highly connected world through a plethora of networks, such as social media, e-commerce, industry trading, telecommunication, banking, social communication and insurance. The relentless growth of such networks has provided opportunities for criminals to infiltrate and manipulate them for their own benefits, creating serious threats to physical, social, economic and cyber domains. Given the magnitude of the financial, social and emotional damages these threats could bring, robust fraud detection methods and algorithms are needed to enable law enforcement agencies to detect these potentially destructive activities before they erupt.

Crime is an inherently social behaviour. Understanding the organisation of social networks and their embedded patterns of social relationships is a key step in the analysis of criminal behaviours. In recent years, there has been extensive refinement and development of network analysis methods within criminology. Network analysis, which includes different statistical, mathematical, machine learning techniques, has proven to be capable of providing deep insights into the structural and dynamic characteristics of different types of networks. Such insights could expose information about individuals and their interactions with others within the network, providing valuable data to flag possible embedded anomalies as potential deviant activities.

Graph-based anomaly detection (GBAD) approaches are among such robust and reliable machine learning techniques capable of unearthing relational patterns of social network of individuals and their social ties (network connections). These techniques have been extensively used by researchers and law enforcement experts to detect deviant activities.

The major challenge in the use of GBAD approaches to detecting a deviant behaviour is analysing users' connectivity patterns over time owing to the multiplex nature of human interactions. To avoid being detected, criminals tend to preserve secrecy by spreading their deceptive activities over different time periods and actively concealing their networking information by engaging in different types of activities. This research addresses this challenge in social networks by developing three GBAD-based algorithms to extract structural features from network connectivity patterns to detect deviant activities. It draws on the tenets of five criminological theories–rational choice theory, routine activity theory, crime pattern theory, differential association theory and social disorganisation theory–to provide the substantive base for developing the algorithms using the design science research (DSR) methodology. The efficacy of the proposed algorithms is evaluated using real-world data, and the results are compared with extant state-of-the-art algorithms in fraud detection. The experimental results of the developed algorithms indicate that they generate practically useful solutions in different application contexts.

This thesis makes significant contributions to both theory and practice by providing solutions for detecting suspicious activities in multiplex (or multi-layer) time-evolving networks and covert communities within multi-layer criminal networks. The implementation of the proposed algorithms provides fraud investigators and law enforcement agencies with a promising list of likely suspects to productively start their investigations.

Keywords: Fraud Detection, Feature Extraction, Graph-based Anomaly Detection, Multi-layer Network, Time-evolving Network, Community Detection, Network Embedding.

1 Chapter 1—Introduction

Advances in communication and digital technologies have created a highly connected world (Velampalli and Eberle 2017). The relentless growth of different types of networks, such as social media, e-commerce websites, blogs, industry trading networks, telecommunication networks, banking networks, social communication networks and insurance networks, has led to the generation of an increasing volume of data among them (Velampalli and Eberle 2017), giving opportunities for fraudsters and criminals to manipulate them for their own benefits (Hooi et al. 2017).

These criminal activities lead to serious threats, which impact physical, social, economic and cyber domains (Home Office 2020). Online sexual predators can, for example, access user information in different online social media websites, allowing them to target and interact with vulnerable youngsters (Savage et al. 2014). The social and economic costs of organised crime are estimated to be at least £37 billion per year in the UK alone (Home Office 2020). Given the magnitude of the financial damages these criminal activities impose on society at large, not to mention the immense social and emotional pains they inflict on the victims, robust fraud detection methods and algorithms are required to enable law enforcement agencies to sniff out these potentially destructive activities before they erupt, especially in the era of ‘big data’.

Crime is an inherently social behaviour, and the propensity to commit crime is influenced by individuals’ social ties (Sarnecki 2001). Understanding the organisation of social networks and their embedded patterns of social relationships arising from individual behaviour is thus pivotal to the study of criminal behaviours (McGloin and Kirk 2010; Sarnecki 2001). Network analysis is an interpretive approach that has been proven to be capable of providing deep insights into the structural and dynamic

characteristics of different types of networks, thereby facilitating the understanding of their complex structure, entities, interdependence and vulnerabilities (McGloin and Kirk 2010).

In network analysis, the main attention in recent years has been directed to understanding the interdependence between individual relationships with others rather than individuals' attributes (McGloin and Kirk 2010). This feature makes network analysis particularly well placed to align with the principles of criminological theories that explain the causes and consequences of crime (McGloin and Kirk 2010). This is because network analysis implicitly assumes that associations among individuals are powerful explanatory factors of different social behaviours (McGloin and Kirk 2010). For instance, in investigating the influence of deviant peers on individuals' risk of victimisation (McGloin and Kirk 2010; Zavala et al. 2019), differential association theory (Sutherland 1939) orients us to the influence of relationships some individuals use to impose on others. Stressing the importance of social networks in facilitating the transmission of values, attitudes, techniques and motives for criminal behaviour, differential association theory (Sutherland 1939) contends that exposure to delinquent friends increases the risk of victimisation (Zavala et al. 2019). This explanation asserts the importance of factors, such as associates of a person, the balance of individuals in the network (i.e. whether the individuals within the network are mostly devious or not), the transformation of a deviant behaviour through the relations or links within the network and the quality or strength of the connections (i.e. the more frequent or the stronger the connections, the greater the influence on individuals' behaviours) (McGloin and Kirk 2010). Another example is the analysis of the organisational structure of criminal groups and networks (McGloin and Kirk 2010; Peoples and Sutton 2015) using social disorganisation theory (Shaw and McKay 1942). Studies drawing

on social disorganisation theory (Shaw and McKay 1942) utilised systematic models to identify the social organisation of communities by analysing social networks (Kasarda and Janowitz 1974).

In recent years, there has been considerable work done in refining and developing network analysis within criminology (Bouchard and Malm 2016; McGloin and Kirk 2010). Analysing the connectivity patterns in communication networks could reveal information about individuals and their interactions with others within the network, thus providing valuable data for detecting a deviant behaviour (Hooi et al. 2017; Sarnecki 2001). These interactions, which are represented as interdependencies and relationships between data objects in graphs[1], are analysed using machine learning techniques to detect possible embedded anomalies to be flagged as potential deviant activities (Akoglu et al. 2015).

Graph-based anomaly detection (GBAD) techniques (Velampalli and Eberle 2017), a branch of machine learning techniques, are a set of arithmetical methods that analyse relational patterns of social network of individuals (nodes as actors) and their social ties (network connections) based on mathematical computations (Hulst 2009). These computations result in measurements that quantify the characteristics of network activities, individuals' social roles and positions and their associated social mechanisms (Hulst 2009). These characteristics and measures are analysed to further interpret and detect patterns in social ties within the individuals' network and to identify the impact of the social structures and ties on the functions of actors and networks (Hulst 2009). With the help of the GBAD techniques, the interpreted structural network characteristics are less sensitive to subjectivity, and the risk of missing out important signals or information is reduced (Hulst 2009). GBAD techniques have been

[1] Throughout this thesis, the terms 'network' and 'graph' are used interchangeably.

extensively used to detect deviant activities within networks; moreover, they are recognised by law enforcement experts as robust, reliable and promising anomaly detection methods in recent years (Akoglu et al. 2015; Velampalli and Eberle 2017).

1.1 Research Scope

Over the past few decades, both law enforcement agencies and researchers have paid considerable attention to the application of the GBAD techniques to the processing and intelligent criminal analysis of social networks (McGloin and Kirk 2010). In line with this trend, this research focuses on the analysis of social networks using the GBAD techniques on two major criminal phenomena, namely, cybercrime in online dating social networks and organisation of criminal networks.

These two domains are of particular interest for two reasons. First, the Internet is now an irreplaceable source of information and communication. The widespread use of the Internet has also brought an increasing popularity to online social networks (OSNs), which also provide criminals an opportunity to use them as a medium of operation for cybersex, unsolicited commercial communications, cyber defamation, cyber threats, data theft and data interception. As more criminals interact in cyberspace, there has been an increase in cybercrime incidents, which has not been matched by a corresponding rise in potent technical responses from law enforcement agencies (Hulst 2009; Nouh et al. 2016).

Second, regardless of whether criminals act in the online world or not, the strategic analysis of criminal groups, their operations and activities in cyberspace is an essential and necessary step to disrupt such criminal networks (Leuprecht and Hall 2014). This analysis provides criminal investigators and law enforcement agencies with information related to the strengths and vulnerabilities of the criminal networks relevant

to designing tactical options to demobilise these criminal networks (Leuprecht and Hall 2014).

1.2 Research Problem

Detecting illicit and deviant behaviours in social networks is a significant problem. The GBAD techniques are known to be very practical in identifying such behaviours (Bindu et al. 2017). The success of graph methods, however, depends on the choice of data representation being used (Cresci et al. 2015; Goyal and Ferrara 2018). Generally, feature engineering and graph representation learning (also called graph embedding) techniques aim to embed the structural characteristics of a network into a vector space (or feature space), in which the machine learning models are then built (Goyal and Ferrara 2018). Therefore, defining measures that can best map a social network structure into a vector space is highly important. This method helps preserve the topological and structural characteristics of actors and their network information, which can then be explicitly analysed using machine learning methods to detect anomalies and deviant behaviours (Goyal and Ferrara 2018).

Feature engineering is a useful way of capturing human ingenuity and prior knowledge (Bengio et al. 2013). In this technique, features are designed based on analysts' foreknowledge with regard to the network entities and known suspicious behaviours. These features range from simple attributes, such as in-degree[2], out-degree[3] and reciprocity, to more complex ones, such as clustering coefficients[4] (Bhat and Abulaish 2013). Thus, the learning algorithms in feature engineering are highly dependent on human intervention, creating scalability problems and potentially reducing the accuracy of the approach. In recent years, GBAD researchers have

[2] For a vertex v in a graph, the number of edges adjacent to v is called the *in-degree*.
[3] For a vertex v in a graph, the number of edges leaving v is called the *out-degree*.
[4] The clustering coefficient is a measure of the degree to which the nodes in a graph tend to cluster together.

started developing new methods, such as graph representation learning or graph embedding techniques (Cai et al. 2017), with the aim of building graph structures without any human intervention. These techniques use different methods, such as deep learning (Goyal and Ferrara 2018; Zhong et al. 2016), to quickly construct models and reveal hidden explanatory factors previously unknown to security experts. Therefore, the accuracy of the detection depends on how good these features are and how well they can reflect 'true' structural connectivity (Cai et al. 2017).

Extant research studies on the GBAD methods do not consider the multiplex nature of human interactions while analysing social networks for detecting an illicit behaviour (Pourhabibi et al. 2020). However, real-life interactions within social communities are multi-faceted in nature and comprised multiple relationship types, leading to the formation of multi-layer social networks. To avoid being detected, criminals embrace secrecy and actively conceal their networking information by engaging in different types of activities (i.e. different types of connections within the network). These multi-faceted interactions are more appropriately represented as a multi-layer network (Rosvall et al. 2014; Zhang et al. 2013). Single-layer networks fail to capture the multi-faceted interactions, which could lead to information loss (De Domenico et al. 2015) and distortion of both the network topology and the embedded dynamics (Rosvall et al. 2014), which consequently dampens the chances of detecting a real deviant behaviour.

Further, most research studies using the GBAD methods have considered just one snapshot of the network and disregarded the analysis of changes in connectivity patterns over different timestamps (Bhattacharjee et al. 2017; Lima and Pereira 2015; McGlohon et al. 2009; Moriano and Finke 2014; Pourhabibi et al. 2020; Rashidi 2017; Shah et al. 2016; Tselykh et al. 2016). Evolution is a natural phenomenon in many real

communication networks. These networks, which are known as time-evolving networks, are frequently changing (Ranshous et al. 2015). Millions of nodes and links are added and removed from networks every moment, changing their attributes (Ranshous et al. 2015). Criminals also attempt to spread their illusive activities over time by making new links or changing their existing links (Bhattacharjee et al. 2017; Lima and Pereira 2015; Moriano and Finke 2014; Rashidi 2017). Due to the high dynamicity in real-world networks plus the large volume of links created and destroyed every moment, analysing connectivity patterns and detecting constantly evolving illusive activities remain a major challenge (Bhattacharjee et al. 2017; Lima and Pereira 2015; Moriano and Finke 2014; Rashidi 2017).

Finally, although many criminological theories have provided substantive knowledge about crimes and criminal behaviours, there is a void in fraud detection research to link core criminological principles to the analysis of social networks in analysing a deviant behaviour. Drawing on the tenets of criminological theories, e.g. rational choice theory (Cornish and Clarke 2014), routine activity theory (Cohen and Felson 1979), crime pattern theory (Brantingham and Brantingham 1993), social disorganisation theory (Shaw and McKay 1942) and differential association theory (Sutherland 1939), this thesis aims to address the challenges in fraud detection studies by employing the GBAD techniques and introducing algorithms to analyse users' connectivity patterns in a social network to detect suspicious behaviours.

1.3 Research Questions

This thesis aims to develop algorithms for detecting deviant activities, using the GBAD techniques. Its principal research question is:

How could suspicious activities be accurately and efficiently detected within a network of interconnected users?

The GBAD techniques hold great potential to help detect a deviant behaviour in different domains. In the scope of this research, there are a number of existing commercial tools that support network analysis. Tools such as COPLINK (Chen et al. 2003), LogAnalysis (Ferrara et al. 2014), CrimeNet Explorer (Xu and Chen 2005), GANG (Shakarian et al. 2015) and PAVENET (Rasheed and Wiil 2014) are developed to support law enforcement agencies in criminal network investigations for detecting criminal organisations within network data. Technologies, such as Klout and Twitalyzer, are employed for monitoring users' engagements in different social media (Wani et al. 2018). Such tools measure user engagement by employing different metrics, such as subscriptions, number of active participants and other actions and attitudes provoked by the other users (Drula 2012).

Given the great potential of the GBAD techniques, this thesis develops algorithms to address the above question. It focuses on two main types of deviant behaviour: (i) finding spamming social activities and (ii) organising criminal networks. The prowess of the GBAD fraud detection algorithms is evaluated against two criteria: quality and efficiency of detection. Quality denotes a high level of accuracy in the detection process. A detection mechanism should be able to detect as many true fraudulent cases as possible and raise less false alarms. To evaluate the accuracy of the proposed algorithms, the ground truth data (i.e. the actual incidents of reported fraud) is used as a reference. The final results of the algorithms, which include the list of identified normal and fraudulent cases, are then compared with the ground truth data. Based on the results of this comparison, accuracy is evaluated using some numerical measures, such as area under curve (AUC) (Molloy et al. 2017; Subelj et al. 2011), receiver operating characteristic (ROC) curve (Molloy et al. 2017; Moriano and Finke 2014) and normalised mutual information (NMI) (Ye and Akoglu 2015).

Further, the accuracy depends on how good the network structure is analysed (Cresci et al. 2015). Data scientists attempt to analyse network structures in a way that they can best distinguish suspicious from normal users (Goyal and Ferrara 2018). This process can be performed in one of two ways, namely, using either feature engineering or graph embedding techniques (Cai et al. 2017; Nikolentzos et al. 2017).

Real-world network data are inherently large. Processing a large amount of data to detect a suspicious activity is a very challenging process that should be performed in a scalable way (Chamberlain et al. 2018; Debajit and Samar 2015). In this context, efficiency means less time and memory complexity and is evaluated using numerical measures, such as convergence time (Tian et al. 2015) and run-time (Phua et al. 2009). With these in mind and considering the existing challenges in the application of GBAD methods to fraud detection, the primary research question is categorised into three sub-research questions (SRQs):

SRQ 1. What set of features can be defined and extracted from a network to capture anomalous activities?

Criminals can easily mimic some patterns of legitimate users' behaviours. This characteristic renders the process of characterising them very difficult. However, extracting a set of features that can depict deviant behaviours in a network is very important to improve the detection process (Bhat and Abulaish 2013; Yang et al. 2013). One approach is to use manual feature engineering. With this technique, data scientists could select sets of features to differentiate normal and suspicious activities in a network based on the problem domain (Varol et al. 2017).

The other perspective for extracting structural features is using techniques that do not require manual feature engineering, leading to the second sub-research question:

SRQ 2. How can users' anomalous activities be detected in a network without any manual feature engineering?

One perspective for analysing users' connectivity patterns in a network is using graph embedding techniques to extract the behavioural features from a network without any manual feature engineering (Cai et al. 2017; Goyal and Ferrara 2018). Where no domain knowledge exists about the network and users' behaviours, data scientists have been able to extract structural features using graph embedding techniques and graph representation learning to analyse and detect anomalous interactions (Cai et al. 2017; Goyal and Ferrara 2018). These techniques use mathematical concepts, such as matrix factorisation (Ahmed et al. 2013), or stochastic theories, such as random walk (Perozzi et al. 2014), to extract structural features from a network.

As this research aims to detect anomalous activities in time-evolving networks, another sub-research question is posed:

SRQ 3. How can users' anomalous activities be detected in a time-evolving network?

Most real-world networks are evolving. Not only do users change their relationships and activities over time, fraudsters also attempt to evade detection by redistributing their deceptive activities over time (Rashidi 2017). To detect fraudulent activities, it is necessary to analyse fraudsters' activities over different timestamps to capture any change in their behaviours (Bhattacharjee et al. 2017; Lima and Pereira 2015; Moriano and Finke 2014; Rashidi 2017).

1.4 Algorithm Development Methodology: Design Science Research

This thesis develops algorithms to answer the research questions by applying existing theories and testing and modifying them according to the three-cycle problem-

solving framework prescribed by the design science research (DSR) paradigm (Hevner 2007; Hevner et al. 2004).

First proposed by Hevner et al. (2004), the DSR paradigm is an approach to scientific inquiry in which organisational problems are addressed by introducing ingenious ideas, methods and products in the form of information technology (IT) artefacts (e.g. constructs, models and algorithms). According to Hevner et al. (2004), seven fundamental guidelines should be followed to ensure that an information system (IS) problem is clearly defined, necessary solutions are found, and the required artefacts are deployed. These guidelines are presented in Table 1.1.

Table 1.1. Hevner's guidelines for solving IS problems

Guideline	Description
Guideline 1: Design Artefacts	New artefacts should be created.
Guideline 2: Domain-specific	The novel solutions should address a specific business problem domain and should result in a utility.
Guideline 3: Artefact Evaluation	The quality and efficiency of created artefacts need to be evaluated.
Guideline 4: Research Contribution	The approach must make new clearly defined contributions to the literature by implementing novel artefacts for a new problem domain or introducing methodological advances in existing solutions.
Guideline 5: Research Rigour	The artefact should be clearly defined and evaluated using rigorous methods.
Guideline 6: Research Process	The research process and problem space should be clearly defined.
Guideline 7: Research Communication	The result of DSR must effectively communicate with the technical and managerial audience.

(Modified from source: Hevner et al. (2004, p.83))

To follow the seven-step guideline, Hevner et al. (2004) introduced a three-cycle framework of IS research (Figure 1.1). In this framework, the Relevance Cycle is a bridge between the contextual environment of the project and the design science processes to ensure that business needs are addressed (Hevner 2007; Hevner et al. 2004). The Rigor Cycle bridges the design science activities to the knowledge base by appropriately applying scientific basis, experience and expertise related to the research project (Hevner 2007; Hevner et al. 2004). The central Design Cycle

iteratively builds and evaluates the design artefacts and processes of the research (Hevner 2007; Hevner et al. 2004).

In this framework, the environment defines the problem domain of interest (Hevner 2007; Hevner et al. 2004). In IS research, the environment includes people (i.e. their role, capabilities and characteristics), organisations (i.e. business strategies, culture and business processes) and technology (i.e. development capabilities, communication architectures, applications and infrastructures) (Hevner 2007; Hevner et al. 2004). The business needs or problems related to technology are perceived from the environment (Hevner 2007; Hevner et al. 2004). The researchers then attempt to frame the research activities to address the perceived business needs (Hevner 2007; Hevner et al. 2004).

When business needs are identified, IS research is conducted by developing theories and artefacts and then evaluating the proposed theories using various experimental studies, case studies and process simulation (Hevner 2007; Hevner et al. 2004). Design science addresses the research by building and evaluating the artefacts to meet the business needs (Hevner 2007; Hevner et al. 2004).

The knowledge base provides raw materials related to the problem domain of interest, including foundations (e.g. basic models, theories, instruments and frameworks) and methodologies (e.g. data analysis techniques, data, measures and validation criteria) (Hevner 2007; Hevner et al. 2004). All these materials are used as a knowledge base through which IS research is conducted (Hevner 2007; Hevner et al. 2004).

This thesis develops artefact(s) (i.e. algorithm(s)) to address the research questions. The proposed algorithms are evaluated using different numerical measures, and the final results are compared with existing works.

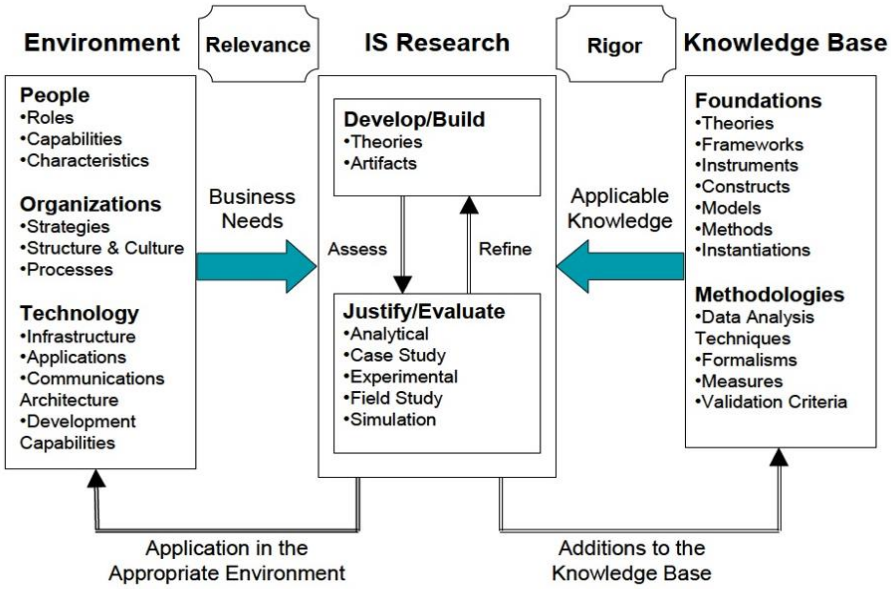

Figure 1.1. IS framework (Source: Hevner et al. (2004, p.80)).

1.4.1 Research Procedure

This research employs Hevner et al.'s (2004) three-cycle framework to develop the required artefacts (algorithms) to answer the research questions. Figure 1.2 presents the different stages of this research organised according to Hevner et al.'s (2004) IS framework (Figure 1.1), preserving relevance and rigor between different stages. The research stages and related processes are described below.

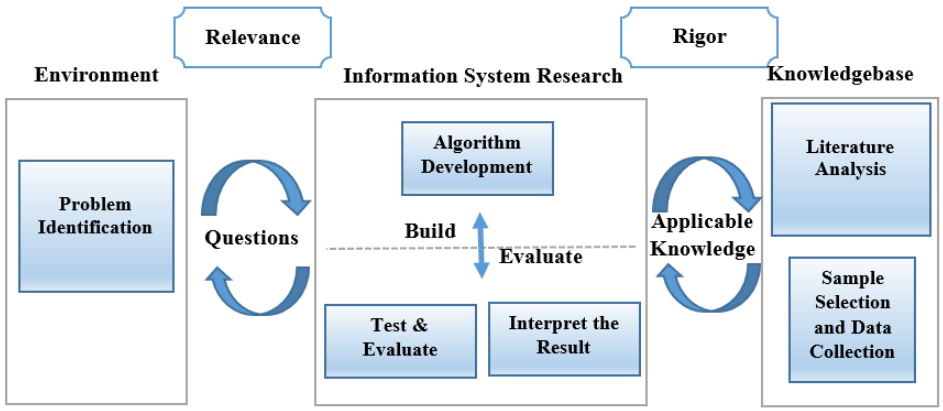

Figure 1.2. Proposed research methodology based on Hevner et al.'s (2004) IS framework.

Environment

The environment section of Hevner et al.'s (2004) framework defines the problem space.

Stage 1—Problem Identification: The first step in this research is the identification of the problems that motivated the research, the research scope and the research questions. This thesis conducts a systematic literature review in the first stage (see Chapter 2). The most significant outcomes of this step are the research 'questions' and 'scope', which are equivalent to 'business needs' in Hevner et al.'s (2004) framework.

Knowledge Base

The knowledge base in Hevner et al.'s (2004) framework includes data, theories and models to conduct the IS research.

Stage 2—Literature Analysis: Once the research questions are identified and the scope is specified, existing research studies are analysed to find answers to the research questions. In this stage, the research will go through the details about different methods, theories and extant algorithms that can be employed to develop new algorithms in response to the research questions.

Stage 3—Sample Selection and Data Collection: Since this thesis develops algorithms to answer the research questions, it is important to collect data samples to test the efficiency and accuracy of the proposed algorithms. One of the main concerns in data collection in this research is privacy and confidentiality issues: organisations and stakeholders are reluctant to share their data for fraud investigations. Therefore, this thesis uses anonymised publicly available data samples with ground truth (i.e. the actual incidents of reported fraud), which are compiled and published by third-party research groups or individuals, e.g. LINQUE[5] and UCINET[6] dark network repositories.

[5] https://linqs.soe.ucsc.edu/data
[6] https://sites.google.com/site/ucinetsoftware/datasets/covert-networks

Information Science Research

The IS section of Hevner et al.'s (2004) framework introduces theories and artefacts and evaluates them using different methods.

Stage 4—Algorithm Development: Based on theories in the context of criminology (see Chapter 3), this thesis develops algorithms to detect anomalous activities in a network by analysing the connectivity patterns in the network. The algorithms are developed based on two GBAD techniques, namely, feature engineering and graph embedding techniques, to analyse and detect deviant behaviours in multi-layer social networks. Here an appropriate programming language (e.g. Python and R) is required for the implementation of the algorithms.

Stage 5—Test and Evaluate: When the algorithms are developed and the experiments are designed, they would be tested using the collected data. Each algorithm goes through several refinements and evaluations. The efficiency of the proposed approaches is evaluated using numerical measures, such as run-time (refer to Table 2.4, Chapter 2). This measure evaluates the execution time of an algorithm. In this case, existing algorithms are used as baseline, i.e. the execution time of the proposed algorithm would be compared with that of existing algorithms on the same dataset to establish time efficiency.

Analysis of time and space complexity can also be another approach to evaluate the efficiency of the proposed algorithms by estimating the required memory space and the time required for the execution of an algorithm (Cook 1983). To measure the accuracy of the proposed approaches, the pre-defined labelled data (e.g. fraud, normal) or the results of previous state-of-the-art approaches (Alzahrani and Horadam 2014; Canu et al. 2015) are used as a reference. The final results, which include the list of identified normal and anomalous cases, are compared with the ground truth (i.e.

actual incidents of fraud that have been reported) to evaluate their accuracy using various measures, such as AUC, ROC curve, modularity and NMI (refer to Table 2.4, Chapter 2).

Stage 6—Interpret the Results: In this stage, the results of the proposed algorithms are interpreted, and their strengths, weaknesses and effectiveness are discussed. To evaluate the results, each chapter includes experiments designed to help the interpretation of the results. Figure 1.3 shows an overview of the designed experiments and their usage.

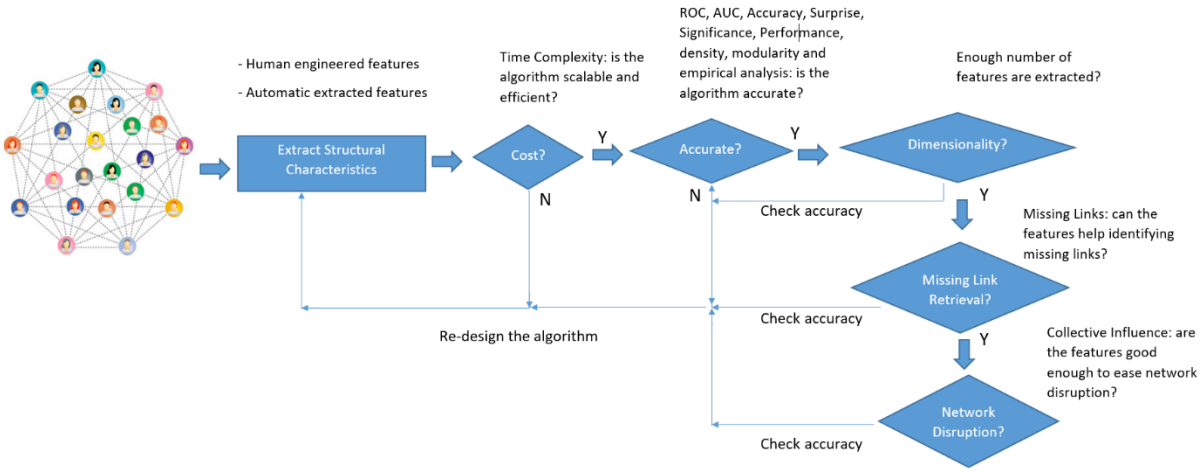

Figure 1.3. Designed experiments for result evaluation and interpretation.

1.5 Research Significance and Expected Contributions

This thesis aims to develop innovative GBAD-based algorithms to analyse the structural connectivity patterns in multi-layer networks with a view to detecting suspicious and deviant behaviours hidden within them. The proposed algorithms are designed to circumvent challenges facing the development of robust GBAD-based fraud detection techniques. The significance of this research comes from its three main contributions.

First, the proposed algorithms are substantiated by five different criminological theories. From a survey of studies using the GBAD approach to develop fraud

detection algorithms up until 2018, none have developed their algorithms based on the tenets of criminological theories. This thesis is among the first to incorporate a theoretical lens from criminology to develop fraud detection algorithms focusing on deviant behaviours in a network. Criminological theories offer an in-depth understanding of anomalous behaviours and provide the conceptual base for developing appropriate algorithms to identify suspicious deviant activities.

Its second contribution is the development of an algorithm that introduces a new set of features that are easy to manually extract for analysing deviant behaviours of cybercriminals in a time-evolving multi-layer online social dating network.

Third, this thesis is devoted to introducing two algorithms that can automatically determine the combination of structural features from multi-layer criminal networks when no prior domain knowledge of the network and anomalous activities are available. Without the need for human intervention, the developed algorithms are expected to automatically reveal a new combination of structural characteristics or features embedded in criminal networks to find criminal communities within such networks. This contribution has a significant practical value; it reduces the dependence of human expert interventions and enables a rapid and efficient detection of criminal groups. Detecting criminal communities within criminal networks would enable law enforcement agencies to dismantle criminal networks and neutralise their threats.

The broader significance of this thesis is its value in the field of anomaly detection in application domains, including OSNs, telecommunication, healthcare, intrusion detection, cyber security and banking anomaly, as well as in improving law enforcement agencies' awareness of issues, such as drug and human trafficking, and extremist organisations' activities in cyberspace (Debajit and Samar 2015). For many

businesses, this problem is too important to ignore, as these events often carry financial and social consequences to their operations.

1.6 Thesis Structure

Chapter 2 consolidates the existing research know-how in analysing inter-dependent data objects in a graph for fraud detection using GBAD. This chapter reviews the state-of-the-art studies on GBAD and identifies key research issues on the applications of the GBAD method. To synthesise existing works, this chapter develops a classification framework, which also serves as an analytic platform in identifying gaps in extant studies. The identified challenges are addressed in Chapters 4–6.

Chapter 3 elaborates the tenets of mainstream theories in criminology to explain different aspects of crime commitment from the perspective of criminology: *why* some people commit crime (i.e. rational choice theory (Cornish and Clarke 2014)), *what* conditions breed crimes (i.e. routine activity theory (Cohen and Felson 1979)), *when and where* crimes happen (i.e. crime pattern theory (Brantingham and Brantingham 1993)) and *how* a deviant behaviour can be detected (i.e. differential association theory (Sutherland 1939) and social disorganisation theory (Shaw and McKay 1942)). This chapter also reviews social network analysis (SNA) as a strong methodological tool, which includes statistical, algebraic and simulation models rooted in the GBAD techniques. As this thesis focuses on *how* to detect criminal acts using the GBAD techniques, Chapter 3 also explains the relationship between network analysis and criminal intelligence by drawing on the tenets of differential association theory (Sutherland 1939) and social disorganisation theory (Shaw and McKay 1942). This explanation builds the theoretical basis for the algorithms developed in Chapters 4–6 to answer the proposed research questions.

Chapter 4 is dedicated to analysing the connectivity patterns in a time-evolving online social dating network to detect a deviant cyber behaviour using feature engineering. Its main objective is to address the first and last proposed sub-research questions: **What set of features can be defined and extracted from a network to capture anomalous activities?** (SRQ 1) **How can users**' **anomalous activities be captured in a time-evolving network?** (SRQ 3). Guided by the tenets of criminological theories reviewed in Chapter 3, Chapter 4 first analyses the commitment of crime in an online social dating network from the perspective of criminology and draws on the principle of differential association theory (Sutherland 1939) to elucidate how suspicious cyber activities may be detected. It then designs four sets of human-engineered features to detect suspicious behaviours in a time-evolving multi-layer social dating network.

Extant learning algorithms in feature engineering designed to interpret suspicious signals of covert criminal activities heavily relying on domain experts' knowledge and are fraught with problems. Not only is the process time-consuming, but the accuracy of the resulting features in detecting suspicious activities is also suspect, not to mention issues of scalability to large-scale networks. To overcome problems associated with human intervention, Chapters 5 and 6 explore new GBAD methods using stochastic theories, graph representation learning (embedding techniques) to discover co-offending groups among criminals within criminal networks (i.e. criminal groups/communities). These two chapters address the second sub-research question: **How can users' anomalous activities be detected in a network without any manual feature engineering?** (SRQ 2).

Chapters 5 and 6 investigate two different approaches to form this new stream of GBAD methods to discover co-offending groups among criminals within criminal

networks (i.e. criminal groups/communities). These two chapters are devoted to addressing the second sub-research question: **How can users' anomalous activities be detected in a network without any manual feature engineering?** (SRQ 2)**.**

Chapter 5 introduces an algorithm that draws on the principles of discrete-time random walks to detect collusive criminal activities in multi-layer criminal networks. The formation of criminal networks is first analysed using the tenets of criminological theories. Then, drawing on the principles of social disorganisation theory (Shaw and McKay 1942), this chapter proposes an approach to find a list of the most important criminals who tend to co-offend together. The proposed approach uses random walk to find the list of criminals who are in touch with each criminal within the network. The Jaccard correlation is then employed to score the similarities among the list of people each pair of criminals is in contact with. The resulting similarity values are then fed into a hierarchical clustering procedure to categorise the criminals into their respective groups by maximising an objective function referred to as asymptotic Surprise (AS) (Traag et al. 2015).

One major concern while developing machine learning algorithms on networks is how the rich topological information of the graph should be incorporated into the machine learning model. In the proposed approach in Chapter 5, once the Jaccard similarities are calculated and fed into the clustering model, no further learning is required. Thus, such information is not optimised during the learning process (Hamilton et al. 2017). This characteristic may reduce the accuracy of the detected communities, especially when the network is very sparse or large.

To overcome this difficulty, Chapter 6 proposes a new algorithm by drawing on a new paradigm of graph-based techniques called network embedding (Goyal and Ferrara 2018; Li et al. 2018; Salim et al. 2020) and applies the algorithm to find covert

communities in multi-layer criminal networks using random walks and a sequence-based network embedding approach. The sequences of criminals and co-offenders extracted are then fed into the network embedding model to extricate the hidden structural characteristics (representations or features) that represent the covert communities.

Finally, Chapter 7 concludes the thesis. It highlights the main contributions and their implications for future GBAD research and fraud detection practices. It also discusses the research limitations and presents an agenda for future research.

2 Chapter 2—Previous Works on GBAD Approaches in Fraud Detection[a]

Graph-based anomaly detection (GBAD) is among the most popular techniques used to analyse the connectivity patterns in communication networks for the detection of suspicious behaviours (Akoglu et al. 2015). Given the different GBAD approaches proposed for fraud detection, this chapter develops a framework to synthesise existing literature on the application of GBAD methods in fraud detection. This chapter aims to identify trends and key challenges that need to be addressed in developing answers to the research questions posed (see Section 1.3).

2.1 Search Methodology

This chapter adopted Booth et al.'s (2011) systematic approach to literature review and followed the three-phase methodology employed by Ngai et al. (2009) and Ngai et al. (2011), as presented in Figure 2.1. A systematic literature review is considered to be the most reliable, transparent and rigorous literature review method for identifying, synthesising and assessing all available evidences to clearly answer the formulated questions (Booth et al. 2011; Mallett et al. 2012). It follows a clearly defined plan with explicitly stated criteria before the review is conduced, which allows it to be replicated by other researchers (Booth et al. 2011; Mallett et al. 2012).

The first phase is 'research definition'. It includes the identification of the research area, formulation of review goals and definition of the research scope. The research area in this review is 'fraud detection' with three main goals: (1) to identify the current

[a] A journal paper developed based on the information presented in this chapter was published: Pourhabibi, T., Ong, K.-L., Kam, B.H., Boo, Y.L., (2020). 'Fraud detection: A systematic literature review of graph-based anomaly detection approaches.' *Decision Support Systems*, Vol.133, pp. 1–15.

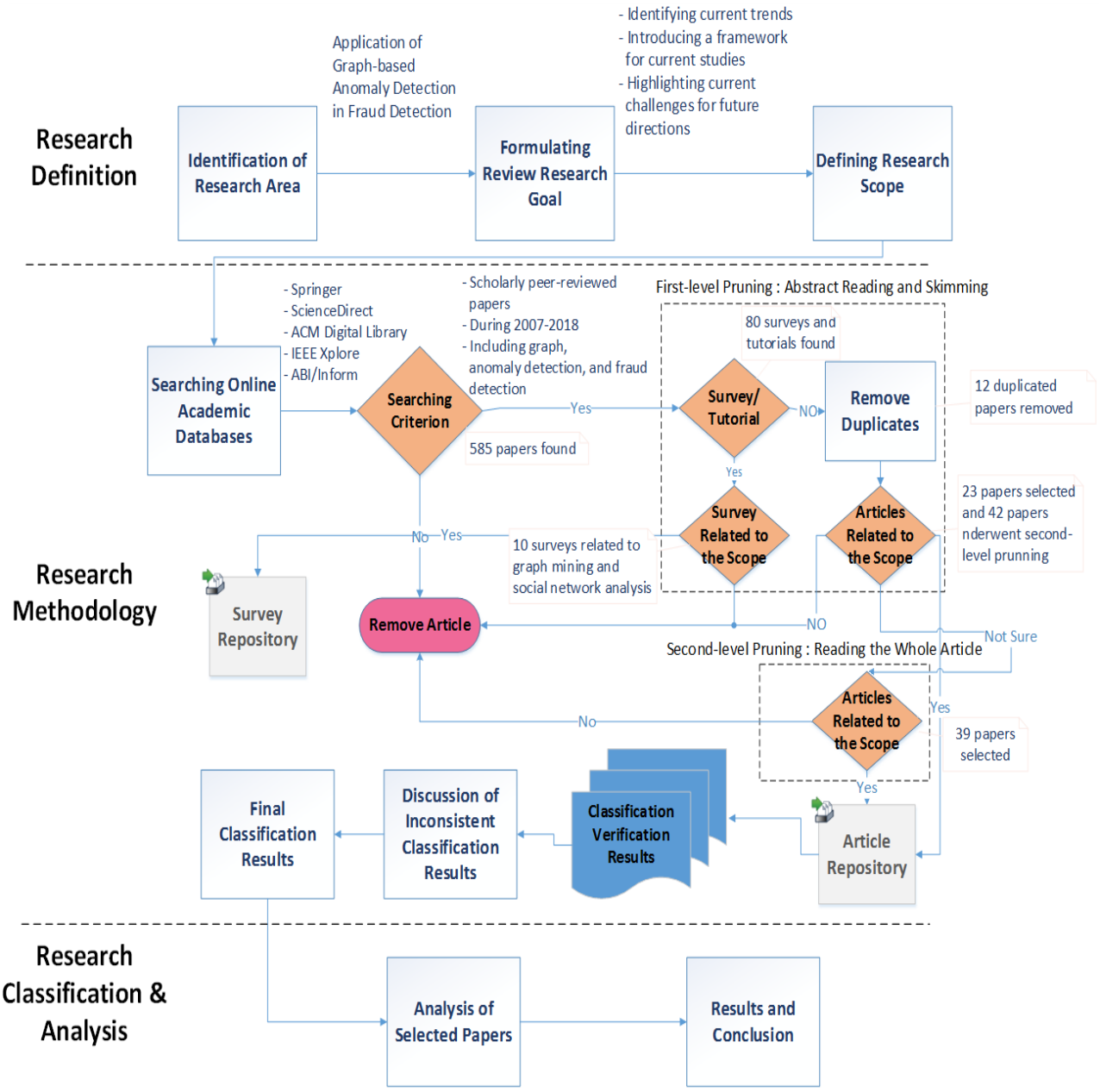

Figure 2.1. Systematic literature review process.

trends, (2) to highlight the current challenges and provide directions for future research and (3) to introduce a classification framework for analysing current studies. The scope covers studies that have employed the GBAD techniques.

The second phase is 'research methodology', which starts with the identification of scientific databases hosting articles related to the selected research context. Five major online scientific databases were selected, namely, ScienceDirect, ACM Digital Library, IEEE Xplore, Springer and ABI/Inform. The literature search process began with the creation of criteria to identify the articles to be included in, or excluded from, the analysis.

Following Ngai et al. (2009), Ngai et al. (2011) and Frost and Choo (2017), four criteria were set: the article must (1) be published in a peer-reviewed academic research journal, (2) be written in English, (3) be published between 2007 and 2018 and (4) have its full text available in at least one of the five databases.

To achieve a more effective and comprehensive search strategy, Boolean expressions were used to combine three terms: ‘graph’, ‘anomaly detection’, and ‘fraud detection’ (i.e. ‘graph’ AND ‘anomaly detection’ AND ‘fraud detection’). A total of 585 papers met the inclusion criteria. Then, the papers were pruned through a two-step process. The first step (‘Abstract Reading and Skimming’) involved reading titles and abstracts, which resulted in the elimination of 428 unrelated papers, white papers and tutorials, 12 duplicated titles and 80 literature review articles. The remaining 65 papers underwent second-level pruning, accomplished by ‘Reading the Whole Article’. This process eliminated another group of 26 unrelated papers, leaving 39 papers for the final analysis.

For the final ‘classification and analysis’ phase, a series of guided questions were applied to sort the 39 papers, similar to the approach adopted by Chan et al. (2017). To ensure the reliability of the classification, each paper was independently reviewed by two authors. Classification discrepancies (e.g. incompatibility in the type of detected anomaly or nature of the input network (see Table 2.3)) were resolved by having the third author read the paper. The guided questions used were as follows:

1. What were the study trends and focus?
2. How did the availability of existing labelled data influence the choice of anomaly detection techniques used in different studies?
3. What were the types of analysed networks?
4. What were the types of detected anomalies?
5. What were the principal graph-based methods used?
6. What were the representation methods used?
7. What were the available research data samples?
8. What were the measures used to evaluate the findings?

9. What were the contributions of the studies, challenges faced during the research and possible future directions?

The first six questions provide six distinct levels of analysis set within the data samples available for experimental studies (Question 7) and the range of measures used for evaluating the findings (Question 8). The eight questions are structured into a hierarchical classification framework to systematically categorise the 39 papers chosen for review (see Figure 2.2). The last question, Question 9, does not constitute part of the classification framework. It is included to remind us to compile the challenges identified by the review studies, including the suggested directions for future research. The next section elucidates the classification framework developed based on the above-proposed questions.

2.2 Classification Framework

Along with the sequence of the nine guiding questions presented in Section 2.1, the proposed classification framework begins with the identification of the domain of interest (i.e. study trends and focus). The other five components of this framework (Questions 2–6) are described below.

2.2.1 Availability of Data Labels

Depending on the available data labels, anomaly detection approaches are classified into three broad categories: (i) supervised, (ii) unsupervised and (iii) semi-supervised (Chandola et al. 2009). Table 2.1 presents the comparison of the characteristics of the three approaches.

Table 2.1. Characteristics of the anomaly detection approaches based on the available data labels

Supervised (Bhattacharyya et al. 2011; Bolton and Hand 2002)	**Unsupervised** (Abdallah et al. 2016)	**Semi-supervised** (Abdallah et al. 2016)
• Require labelled data samples of legitimate and fraudulent samples • Build models based on the patterns revealed in existing data samples • Unable to detect unseen suspicious activities	• Do not need labelled data samples • Able to detect unseen suspicious activities	• Use both labelled and unlabelled samples • Requires a few instances of labelled samples • Able to detect unseen suspicious activities

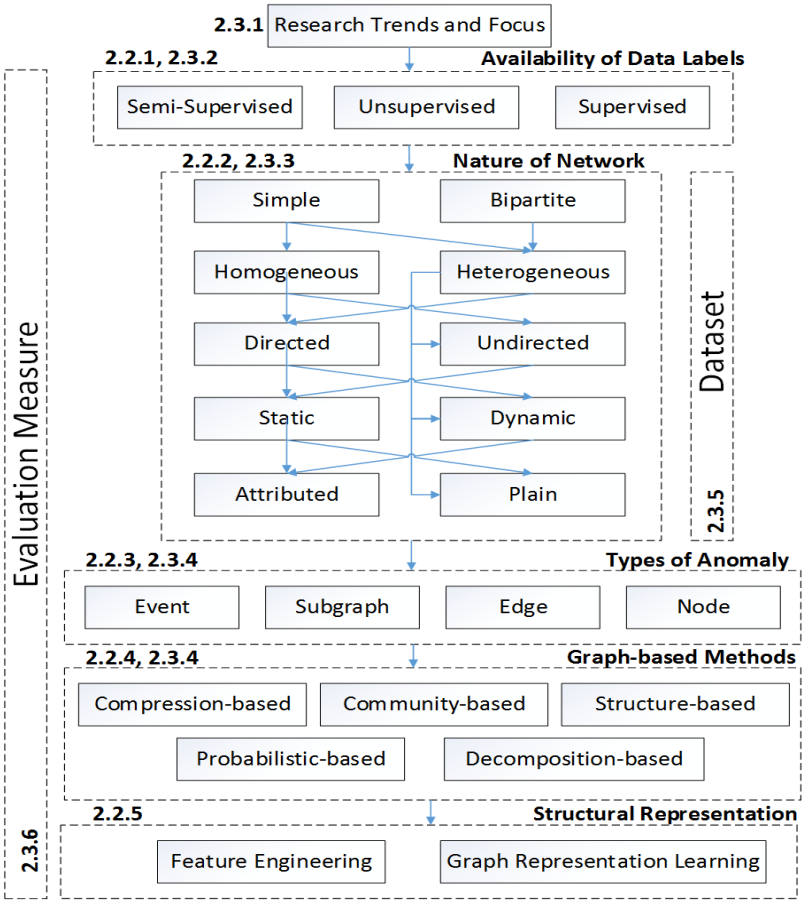

Figure 2.2. Framework for the literature analysis and classification of GBAD fraud detection papers (the numbers refer to the different sections of this chapter).

2.2.2 Nature of the Input Network

With the GBAD approaches, the nature of the input network can influence the process of anomaly detection and the design of the algorithm. As outlined in Table 2.2, these features include the followings: (i) information propagation in the network (such as the direction of links and the time the links were established), (ii) node characteristics (such as node types and node attributes) and (iii) peer influences (such as link structures and link attributes) (Agrawal et al. 2012).

Table 2.2. Characteristics of the different types of input networks

Type of the Input Network	Characteristics
Simple (Kaveh 2013) vs. Bipartite (Kaveh 2013)	- One subset of nodes -Two disjoint subsets of nodes
Homogeneous* (Kaveh 2013) vs. Heterogeneous** (Lee et al. 2013)	- One type of node or link - Different types of nodes or links - Difficult to detect suspicious activities (Fakhraei et al. 2015)
Directed (Kaveh 2013) vs. Undirected (Kaveh 2013)	- Symmetric relations between nodes - Asymmetric relations between nodes
Static (Akoglu et al. 2015; Ranshous et al. 2015) vs. Dynamic (Akoglu et al. 2015; Ranshous et al. 2015)	- A single snapshot of a network (Bindu and Thilagam 2016) - Structure constantly changing over time (Akoglu et al. 2015) - More difficult to analyse anomalies (Akoglu et al. 2015; Bindu and Thilagam 2016; Ranshous et al. 2015)
Attributed (Akoglu et al. 2015; Bindu and Thilagam 2016; Ranshous et al. 2015) vs. Unattributed	- Nodes or links with attributes - Attributes revealing considerable amount of information regarding the network entities and their interactions (Shah et al. 2016) - No attribute assigned to either nodes or links

Note:
* also called simple, simplex or monoplex
** also called multiplex or multilayer networks

2.2.3 Types of Anomalies

Various GBAD approaches have been designed to detect different anomalies. These methods (Bindu and Thilagam 2016; Ranshous et al. 2015) detect anomalies in various networks, such as dynamic or static graphs (attributed or unattributed), by capturing (a) anomalous nodes, (b) edges, (c) sub-graphs and (d) events. Therefore, the type of anomaly is a critical characteristic of the proposed classification framework.

Anomalous nodes are a subset of nodes; every node in the subset has an irregular feature in comparison with the other nodes in the graph. Typically, each node is assigned an anomaly score based on its characteristics (e.g. the ratio of input/output degree and ego net density) (Bindu and Thilagam 2016; Ranshous et al. 2015). Similar to anomalous nodes, anomalous edges are a subset of edges; every edge exhibits an abnormal behaviour, i.e. having scores higher than a specific threshold. This characteristic, in turn, indicates the existence of an anomaly, such as anomalous nodes. Contrarily, the approach to finding an irregular sub-graph is quite different. Typically, sub-graphs are first identified using community detection methods (see Section 2.2.4), and then each sub-graph is assigned an

anomaly score based on intra-graph comparisons (see Noble and Cook (2003) for more information). The last anomaly type is event and change detection. This type of anomaly is exclusively detected in dynamic networks and designed to locate the specific time period(s) in which activities are significantly different from those in the rest of the periods (Ranshous et al. 2015).

2.2.4 Graph Methods

Graph methods include the machine learning algorithm(s) applied to the networks to detect different types of anomalies. Depending on the available data labels, nature of the input network and types of anomalies that are to be discovered in a network, prior studies have captured different anomalies across five approaches, as described in Figure 2.3.

Community-based approaches aim to find densely connected groups of nodes in a graph (usually by analysing their interconnection) and identify nodes and edges that have inter-connections with those communities or clusters. Such nodes act as a 'bridge' between different clusters, and their behaviour exhibits a significant deviation from those of the members of a specific cluster or community (Akoglu et al. 2015; Bindu and Thilagam 2016).

Probabilistic-based methods use the basic concept of probability theory, probability distribution and scan statistics to construct a model of normal behaviour; any deviation from this normal distribution is flagged as an anomaly (Akoglu et al. 2015; Bindu and Thilagam 2016).

Structure-based methods are also useful methods for detecting a community of fraudsters (Hooi et al. 2017; Jiang et al. 2014). Structure-based approaches mainly aim to find special substructures that rarely occur in a graph. These approaches usually exploit a graph topological structure and node/edge attributes (if available) to detect the anomalies (Akoglu et al. 2015; Bindu and Thilagam 2016).

Compression-based approaches are based on minimum description length (MDL) principle. These approaches exploit patterns and regularity in the data to achieve a compact

graph representation by rearranging the network adjacency matrix to minimise the adjacency matrix entropy. In these approaches, anomalies are defined as sub-graphs, edges or nodes that inhibit compressibility (Ranshous et al. 2015).

Decomposition-based approaches have been used to detect suspicious activities in dynamic networks by representing the set of graphs as a tensor like a multidimensional array. Similar to compression-based approaches, decomposition techniques also search for patterns or regularities in data to exploit (Ranshous et al. 2015).

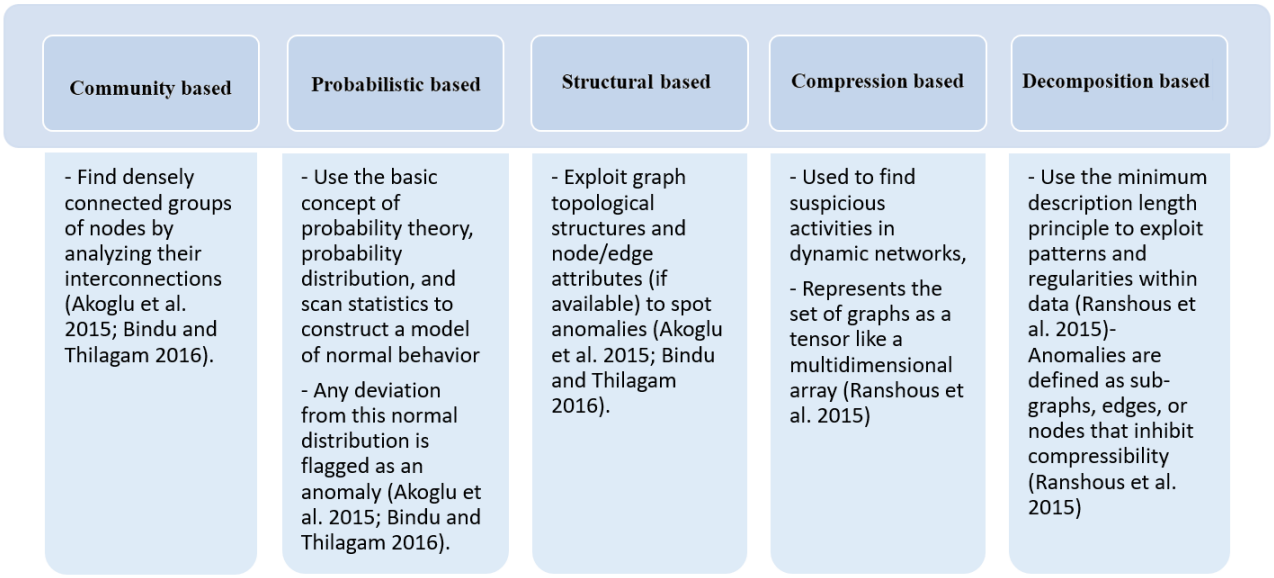

Figure 2.3. Five different types of GBAD.

2.2.5 Structural Representation

The success of GBAD methods depends on the choice of data representation being used (Cresci et al. 2015; Goyal and Ferrara 2018). Generally, feature engineering and graph representation learning (also called graph embedding) techniques aim to embed the structural representation of a graph into a vector space (or feature space), in which the machine learning models are then built (Goyal and Ferrara 2018). Therefore, the definition of measures that can best map a network structure into a vector space is highly important. This method helps preserve the topological and structural characteristics of nodes and network information, which can then be more explicitly analysed using machine learning methods to detect anomalies (Goyal and Ferrara 2018).

Feature engineering is a useful way of capturing human ingenuity and prior knowledge (Bengio et al. 2013). In this technique, features are designed based on analysts' foreknowledge with regard to the network entities and known suspicious activities. These features range from simple attributes, such as in-degree[1], out-degree[2] and reciprocity, to more complex ones, such as clustering coefficients[3] (Bhat and Abulaish 2013). Thus, the learning algorithms in feature engineering are highly dependent on human intervention, creating scalability problems. In recent years, GBAD researchers have started to develop new methods, such as graph representation learning or graph embedding techniques (Cai et al. 2017), that aim to build graph structures without any human intervention. These techniques use different methods, such as deep learning (Goyal and Ferrara 2018; Zhong et al. 2016), to quickly construct models and reveal hidden explanatory factors previously unknown to security experts.

2.3 Findings and Discussions

Using the proposed classification framework (Figure 2.1), the 39 reviewed papers are catalogued into five areas, namely, graph methods, application areas, data label availability, input network and types of anomalies (see Table 2.3). This cataloguing aims to increase the understanding of a particular type of GBAD method while dealing with certain application areas as well as support researchers in exploring which approach or paper to focus on when detecting specific types of anomalies in accordance with the nature of their input network and availability of their data labels. The findings of the review are discussed based on the guiding questions presented in Section 2.1.

[1] For a vertex v in a graph, the number of edges adjacent v is called the *in-degree*.
[2] For a vertex v in a graph, the number of edges leaving v is called the *out-degree*.
[3] The clustering coefficient is a measure of the degree to which nodes in a graph tend to cluster together.

Table 2.3. Cataloguing of graph-based fraud detection •

Graph Methods	Application Areas	Reference	Availability of Data Labels	Nature of the Input Network				Types of Anomalies
Structure-based	**OSN**	(Jiang et al. 2014)	US	SH	ST	D	A	SG
		(Hooi et al. 2017)	US	BH	ST	UD	UA	SG
		(Manjunatha and Mohanasundaram 2018)	US	SH	DY	UD	UA	N
	Insurance	(Branting et al. 2016)	S	SH	ST	D	A	N
		(Seo and Mendelevitch 2017)	US	SH	ST	UD	A	N
	AML	(Bershtein and Tselykh 2013)	US	SH	ST	D	A	SG
		(Fronzetti Colladon and Remondi 2017)	US	SH	ST	D	A	N
Community-based	**OSN**	(Tian et al. 2015), (Ye and Akoglu 2015), (Wang et al. 2018)	US	BH	ST	UD	A	SG
		(Giatsoglou et al. 2015)	US	SH	DY	D	A	SG
		(Bindu et al. 2018)	US	SH	ST	D	A	SG
	AML	(Novikova and Kotenko 2014)	US	SH	ST	D	A	SG
	Banking	(Molloy et al. 2017)	SS	SH	ST	D	A	SG
	Trading	(Li et al. 2012)	US	SH	ST	D	A	SG
	IOF	(Gamachchi and Boztaş 2015)	US	SH	ST	UD	UA	SG
	Online Auction	(Liang et al. 2010)	US	BH	ST	UD	A	SG
		(Bangcharoensap et al. 2015)	SS	BH	ST	UD	A	SG
	Telecom	(Nan et al. 2012)	US	SH	ST	UD	UA	SG
		(Yan et al. 2018)	S	BH	DY	UD	A	SG
	Retail Holding	(Tselykh et al. 2016)	US	SH	ST	D	A	SG
Decomposition-based	**OSN**	(Moriano and Finke 2014), (Liu et al. 2017b)	US	SH	DY	D	A	SG
		(Shin et al. 2017)	US	SH	DY	D	A	N
		(Lamba et al. 2017)	US	SH	DY	D	A	N, SG
Compression-based	**Trading**	(Eberle and Holder 2009), (Eberle and Holder 2007)	US	SH	ST	D/UD	A/UA	SG
	OSN	(Shah et al. 2016)	US	BH/SH	ST	UD	A	N
	Insurance, AML, Banking, Trading	(Huang et al. 2018)	US	BH/SH	ST	UD/D	A	N
Probabilistic-based	**Insurance**	(Carvalho et al. 2017)	US	BH	ST	UD	A	N
		(Subelj et al. 2011)	US	SH	ST	D	A/UA	N, SG
	OSN	(Dai et al. 2012)	US	BH	ST	UD	A	N
		(Wu et al. 2017)	US	BH	DY	UD	UA	N
		(Shehnepoor et al. 2017b)	US, SS	BH	ST	UD	A	N
		(Dang et al. 2017)	US	SH	DY	D	A	SG
	Online auction	(Tsang et al. 2014)	US	BH	ST	UD	A	SG
	OCA	(Phua et al. 2009)	US	SH	DY	D	A	E
	IOF	(McGlohon et al. 2009)	US	SH	ST	D	A	N
		(Bhattacharjee et al. 2017)	US	SH	DY	D	A	SG

● **Note:**
(1) Graph representation learning was only used in decomposition-based methods in the study by Moriano and Finke (2014) and Shin et al. (2017).
(2) Studies that model the input network as a bipartite graph are heterogeneous networks with different types of nodes, and the rest of the studies are homogeneous networks.

(3) None of the reviewed studies worked on anomalous event detection.
Legends:
SH, simple and homogenous; BH, bipartite and heterogeneous;
DY, dynamic; ST, static;
D, directed; UD, undirected;
A, attributed; UA, unattributed;
S, supervised; U, unsupervised; SS, semi-supervised;
N, node; SG, sub-graph; E, edge; EV, event;
OSN, online social network; AML, anti-money laundering; IOF, internal organisational fraud; OCA, online credit application

2.3.1 Research Trends and Focus

Figure 2.4 presents the distribution of the 39 studies analysed from 2007 to 2018 (none of the 39 papers reviewed were published in 2007 and 2008). This finding indicates a growing trend in the application of the GBAD techniques for fraud detection.

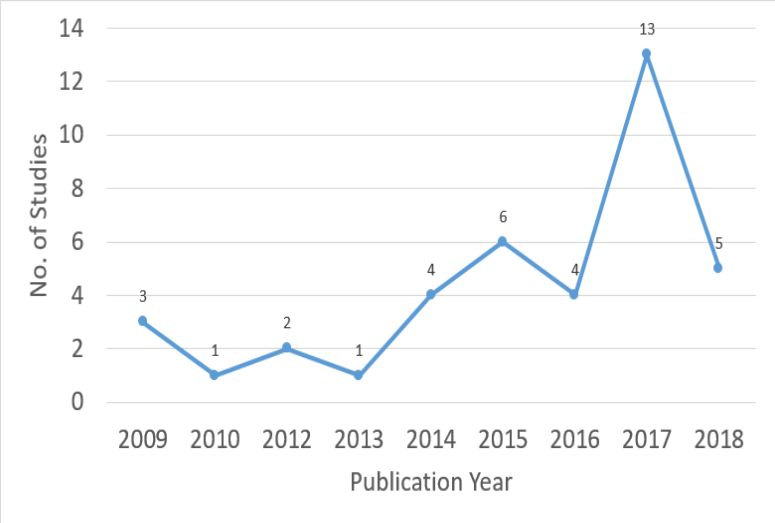

Figure 2.4. Distribution of papers reviewed, 2009–2018.

The analysis suggests that studies using the GBAD methods to detect fraudulent activities generally fall into two major streams: traditional and OSN (Figure 2.5). The traditional stream, with applications in insurance (Carvalho et al. 2017; Molloy et al. 2017; Seo and Mendelevitch 2017), telecommunication (Nan et al. 2012), banking (Molloy et al. 2017; Novikova and Kotenko 2014), online credit applications (OCA) (Phua et al. 2009), anti-money laundering (AML) (Bershtein and Tselykh 2013), retail holding (Tselykh et al. 2016), trading (Li et al. 2012) and internal organisational fraud (IOF) (Bhattacharjee et al. 2017; McGlohon et al. 2009), has heavily relied on GBAD methods to analyse its data.

However, the data utilised in these studies were not explicitly linked together. These studies have used graph data to detect fraud by inferring the links within the data. This growing trend is becoming significant and demonstrates the applicability and importance of the GBAD methods for fraud detection in various applications.

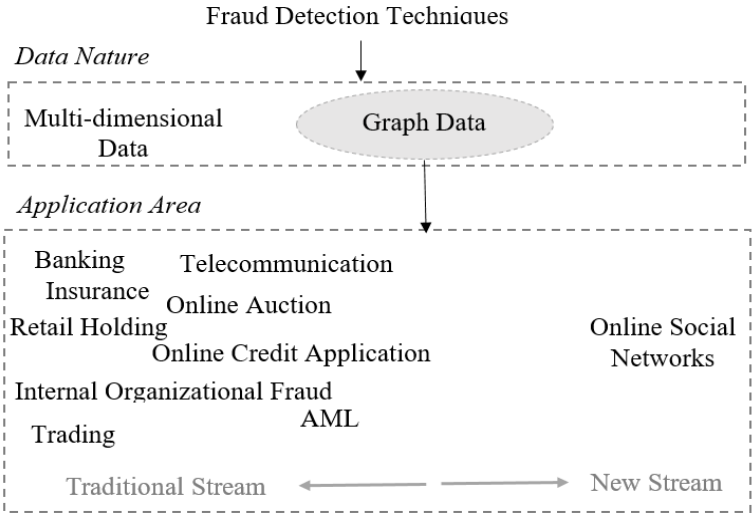

Figure 2.5. Data nature and application areas of the GBAD techniques for fraud detection.

Although research studies using the GBAD methods are still sparse, the efforts devoted to detecting frauds in insurance and banking applications have become prevalent since 2017. Figure 2.6 presents the diversity of research studies employing the GBAD techniques on fraud detection by research area during the selected period. Since 2014, the analysis of OSNs where data are inherently linked to one another in networks (Lima and Pereira 2015; Meng et al. 2016; Moriano and Finke 2014) has also become an emerging stream. This finding indicates the increasing popularity of online social activities. As businesses turn to social media to promote their products and services, they also create an additional opportunity and a fertile channel for fraudsters to conduct malicious activities (Rahman et al. 2017). For example, fake reviewers can earn between $0.5 and $3 for each fake review (Rahman et al. 2017) by demoting or promoting a product, service or business. As the range of online social activities increases, the possibility of different types of fraud occurring in

such networks also increases; thus, filtering any suspicious behaviour is necessary to mitigate the consequences.

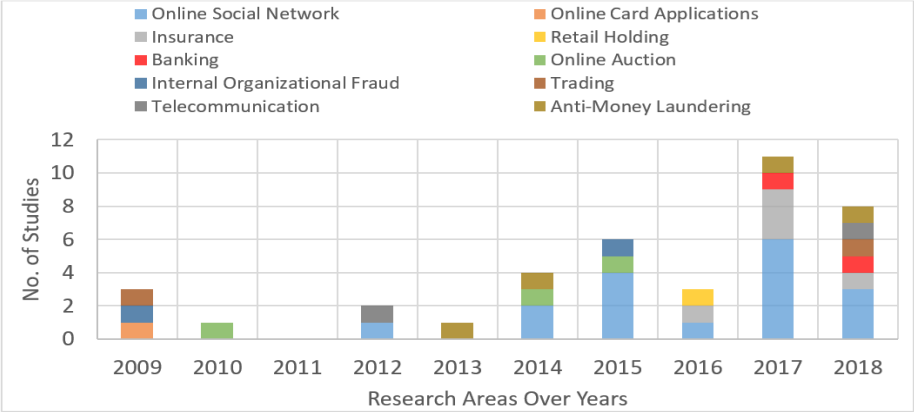

Figure 2.6. Distribution of research studies using the GBAD techniques for fraud detection, 2009–2018.

2.3.2 Availability of Data Labels

From the perspective of data label, approximately 87.2% of the reviewed research studies have exclusively created their models using unsupervised learning techniques. The reason is that data labels are often in short supply or non-existent in many real-world problems, such as fraud detection (Abdallah et al. 2016). Consequently, unsupervised learning techniques have been the focus of many research studies. However, there are exceptions, such as Shehnepoor et al.'s (Shehnepoor et al. 2017b) work, which can be applied in unsupervised and semi-supervised settings (2.6%), as well as the works of Bangcharoensap et al. (2015) and Molloy et al. (2017), which both exclusively used a semi-supervised-based approach. From the review, only 5.1% of the studies used supervised learning methods.

The shortcomings related to supervised and semi-supervised learning techniques, as outlined in Section 2.2.1, may hinder the use of the GBAD approaches in some cases. These methods are among the least commonly used methods found in this review.

2.3.3 Nature of the Input Network

The nature of the input network is a fundamental feature of the GBAD approaches. Therefore, they are unpacked into several units of analysis, which are described in this section.

2.3.3.1 Simple vs. Bipartite

Among the papers that modelled the input network as a bipartite graph, the most represented application is OSN with 20.5% (8 of the 39 papers). The other applications are insurance (5.1%; two papers), auction (7.7%; three papers) and telecommunication fraud detection (2.6%; one paper). This finding can be explained based on the nature of the above application areas, where the connections between users and products or services should be analysed to detect suspicious behaviours (e.g. the number of parties bidding a seller's product in auction fraud, number of ratings to a product in online business websites and claims submitted by a specific insurance provider). The remaining 25 papers analysed user-to-user connections (e.g. the number of messages sent by a specific user to others) to detect suspicious activities, thus modelling their input network as simple graphs.

2.3.3.2 Homogeneous vs. Heterogeneous

The reviewed research papers on OSNs, insurance and auction frauds have extensively considered the analysis of suspicious activities in bipartite networks. These studies model bipartite networks using two different sets of nodes, mainly users and products or users and services. These networks are considered to be heterogeneous networks with different types of nodes (Table 2.3). Among the studies, only two (Bindu et al. 2018; Shah et al. 2016) have considered different types of activities (e.g. different types of links). However, in the study by Bindu et al. (2018), each type of relationship was simulated as a simple network and analysed separately. Another study by Shah et al. (2016) also simulated the input network as a heterogeneous bipartite network. As mentioned in Section 2.3.3.1, 25 papers investigated users' behaviours on simplex networks; they only considered one type of user

activity, thus ignoring the inherent multiplex nature of human interactions in their analysis (Fakhraei et al. 2015). These studies did not consider different types of users' activities in the network to detect suspicious activities (see Section 2.2.2).

2.3.3.3 Directed vs. Undirected

As indicated by the information summarised in Table 2.3, approximately 48.7% of the research studies are solely applied to directed networks, 43.6% are practiced only on undirected networks, and the remaining 7.7% are applied to directed and undirected networks.

Studies modelling their input network as an undirected network mainly explore user-to-product or user-to-service relationships and are mostly bipartite networks (14 of the reviewed papers employed bipartite networks).

2.3.3.4 Static vs. Dynamic

In recent years, dynamic networks have increased in popularity owing to their applications in social networks, insurance and online banking (Bhattacharjee et al. 2017; Moriano and Finke 2014; Phua et al. 2009; Shin et al. 2017). The relentless growth of social networks, in particular, has provided opportunities for fraudsters to infiltrate these networks and spread their illusive activities by frequently establishing new connections with other users or changing their relations with existing users (Pourhabibi et al. 2019). In other words, fraudsters can easily evade current detection mechanisms. Although the importance of analysing dynamic networks for suspected fraud has surged, it is still a promising research area (Bhattacharjee et al. 2017; Moriano and Finke 2014; Phua et al. 2009; Shin et al. 2017). Of the papers reviewed, only 28.2% focused on fraud detection in dynamic networks; the remaining 71.8% (28/39) merely searched for suspicious activities in static networks.

2.3.3.5 Attributed vs. Unattributed

The link and node attributes are essential elements for differentiating users' behaviours in a communication network (Shah et al. 2016). They provide useful information for the

detection of anomalies in a network. Table 2.3 demonstrates that only five papers that were reviewed (12.8%) ignored the importance of attributes. Among those that used attributes to distinguish suspicious activities (87.2%), most employed link attributes, such as interaction strength.

2.3.4 Graph Methods and Types of Anomalies Detected

Depending on the available data labels and nature of the input network, five different GBAD methods were used to detect different types of anomalies in the network among the 39 papers reviewed. Community-based approaches were the most widely used (35.9%), with probabilistic-based methods as the second-most popular approach (25.6%). Around 17.9% of the studies used structural-based techniques, whereas compression-based (10.3% of the studies) and decomposition-based (10.3% of studies) approaches were among the least-used methods (see Figure 2.7).

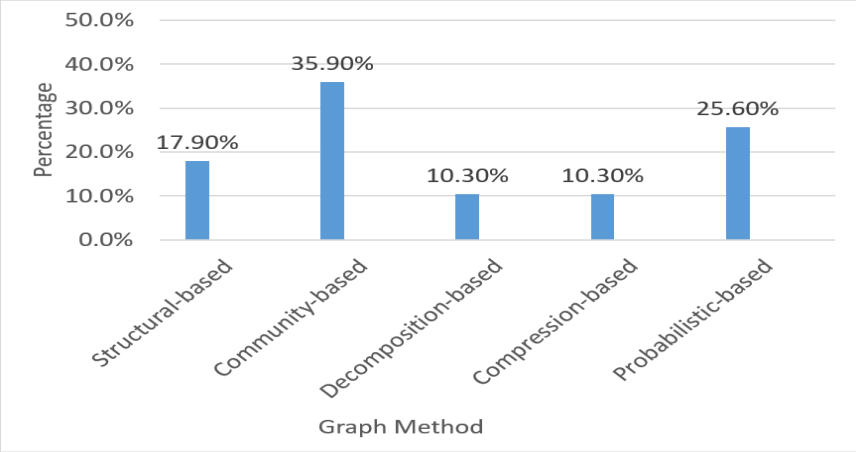

Figure 2.7. Spread of different GBAD methods in the papers reviewed.

Fraud is characteristically manifested as a collective behaviour in networks, as fraudsters attempt to coordinate their behaviours as a group (Pourhabibi et al. 2019). The detection of such illusive user communities (also referred to as groups or clusters) has become a key focus. Table 2.3 demonstrates that around two-thirds of the research studies focused on the identification of anomalous sub-graphs. Among them, the top two GBAD methods, community-based and probabilistic-based methods, exhibited the highest share. Contrarily,

the other three GBAD methods were mostly used to detect the most suspicious nodes or edges within the network.

2.3.5 Dataset

Most of the research studies on fraud detection have used real-world data as their test platforms (Nettleton 2016; West and Bhattacharya 2016). Many have also used synthetic data to simulate specific scenarios (Nettleton 2016; West and Bhattacharya 2016). Owing to privacy considerations, organisations and stakeholders are reluctant to share their fraud information (West and Bhattacharya 2016). This hinders research and affects the reproducibility of the conducted experiments. One possible solution is to use synthetically created data (Nettleton 2016). However, the generation of a realistic dataset presents enormous challenges in terms of topologies, attribute values of nodes and edges, community structures, data distributions and correlations (Nettleton 2016). Furthermore, the similarity between synthetically generated networks and original networks extracted from human behaviour remains unanswered.

Table 2.4 presents an overview of the different publicly available data and datasets used by the studies reviewed. It shows that 87.2% of the studies tested their approach using real-world data (34/39), of which 41.0% are publicly available for research studies (16/39). A third of the 39 studies used synthetic data. Among the studies using publicly available datasets, 81.3% used OSN data (13/16), reflecting their broad availability for anomaly detection research.

Table 2.4. Mapping catalogue for the types of datasets, public data used and evaluation measures

Graph Methods	Application Areas	Reference	Availability of Data Labels	Types of Dataset	Types of Evaluation Measures
Structure-based	**OSN**	(Jiang et al. 2014)	US	P (Twitter, Tencent Weibo), SY, RW	PR curve, run-time, accuracy
		(Hooi et al. 2017)	US	P (Amazon, TripAdvisor, Epinions, WikiVote), SY, RW	F-measure, run-time
		(Manjunatha and Mohanasundaram 2018)	US	RW	PR, F-measure
	Insurance	(Branting et al. 2016)	S	RW	F-measure, ROC

		(Seo and Mendelevitch 2017)	US	P (Medicare-B), RW	Case study
	AML	(Bershtein and Tselykh 2013)	US	No experimental data	No experimental study
		(Fronzetti Colladon and Remondi 2017)	US	RW	Pearson's correlation of features
Community-based	**OSN**	(Tian et al. 2015)	US	SY, RW	Run-time, recall, convergence time
		(Ye and Akoglu 2015)	US	P, SY, RW (Amazon, iTunes)	AUC of PR, NMI
		(Wang et al. 2018)	US	P, RW (Amazon, Yelp)	precision, F-measure, CDF
		(Giatsoglou et al. 2015)	US	P, RW (Twitter)	Power-law analysis
		(Bindu et al. 2018)	US	P, RW (Twitter Honeypot)	TPR, FPR, PR, F-measure
	AML	(Novikova and Kotenko 2014)	US	SY	Visual analytics
	Banking	(Molloy et al. 2017)	SS	RW	ROC
	Trading	(Li et al. 2012)	US	RW (Roget, Stock)	Run-time, case study
	IOF	(Gamachchi and Boztaş 2015)	US	P, RW (CERT)	Case study
	Online Auction	(Liang et al. 2010)	US	RW	NDCG
		(Bangcharoensap et al. 2015)	SS	RW	NDCG
	Telecom	(Nan et al. 2012)	US	RW	CDF
		(Yan et al. 2018)	S	RW	PR, F-measure, ROC
	Retail Holding	(Tselykh et al. 2016)	US	RW	Case study
Decomposition-based	**OSN**	(Moriano and Finke 2014)	US	SY	ROC
		(Liu et al. 2017b)	US	P, RW (Yelp, Amazon, BeerAdvocate)	F-measure, ROC
		(Shin et al. 2017)	US	P, RW (Yelp, Android, YahooM, KoWiki, ENWiki, YouTube)	ROC, detection time
		(Lamba et al. 2017)	US	P, SY, RW (Software Marketplace, Reddit)	PR, F-measure
Compression- based	**Trading**	(Eberle and Holder 2009)	US	SY	Case study
		(Eberle and Holder 2007)	US	SY, RW	Case study
	OSN	(Shah et al. 2016)	US	P, RW (Flipkart)	Precision
	Insurance, AML, Banking, Trading	(Huang et al. 2018)	US	P, SY, RW (German Credit Card, ICIJ Offshore Leaks, COIL2000 insurance)	Accuracy
Probabilistic-based	**Insurance**	(Carvalho et al. 2017)	US	RW	Case study
		(Subelj et al. 2011)	US	RW	AUC
	OSN	(Dai et al. 2012)	US	P, SY, RW (Goodreads, Buzzcity)	Precision
		(Wu et al. 2017)	US	P, RW (Yelp)	PR, F-measure, accuracy, AP, ROC
		(Shehnepoor et al. 2017b)	US, SS	P, RW (Yelp)	AP, AUC
		(Dang et al. 2017)	US	RW	PR, F-measure, accuracy
	Online auction	(Tsang et al. 2014)	US	SY	AUC, TPR, FPR
	OCA	(Phua et al. 2009)	US	RW	Hit rate, TPR
	IOF	(McGlohon et al. 2009)	US	SY, RW	Accuracy, ROC
		(Bhattacharjee et al. 2017)	US	SY, RW (CMU-CERT Insider Threat)	AUC, ROC

Legends:
S, supervised; U, unsupervised; SS, semi-supervised;
P, public datasets; SY, synthetic datasets; RW, real-world datasets;
PR, precision–recall; ROC, receiver operating characteristics; AP, average precision; NMI, normalised mutual information; TPR, true-positive rate; FPR, false-positive rate;
CDF, cumulative distribution function;
NDCG, normalised discounted cumulative gain

2.3.6 Evaluation Measures

As presented in Table 2.4, research studies have employed different mathematical measures to evaluate the outcome of their proposed algorithms. For those with sufficiently available labelled data, the classical criteria based on ROC curve or precision–recall (PR) curve have been used to analyse the performance of the proposed algorithms. ROC curves are commonly used to present the results for binary decision problems in machine learning (Davis and Goadrich 2006; Jeni et al. 2013). However, with highly skewed datasets, ROC does not provide much insight into the data, and PR curves tend to provide a more informative picture of an algorithm's performance. In anomaly detection, the number of negative samples significantly exceeds that of positive examples. Consequently, a substantial change in the number of false positives (FPs) can lead to a small change in the FP rate (FPR) used in the ROC analysis (Davis and Goadrich 2006; Jeni et al. 2013).

Furthermore, precision captures the effect of many negative examples on the algorithm's performance by comparing FPs with true positives rather than with true negatives (Davis and Goadrich 2006; Jeni et al. 2013). F-measure is the second-most commonly used performance measure. This preference over the next measure, i.e. accuracy, comes as no surprise given the nature of fraud problems. Accuracy favours true negative, which is inconsequential in anomaly detection. Instead, a measure that weighs higher on false negative (FN) and FP is of better value in an uneven class distribution. In such cases, the F-measure is preferred as it balances precision and recall, resulting in a better evaluation of an anomaly detection model. Moreover, it is observed that accuracy is only used in five studies (Bhattacharjee et al. 2017; Huang et al. 2018; McGlohon et al. 2009; Tsang et al. 2014; Wu et al. 2017) (see Table 2.4).

Although some measures are preferred over others, no measure is perfect; they can only serve as an approximation to a technique's performance on a specific dataset. Ideally, the evaluation is checked against authentic data sourced from the specific problem, for which

the anomaly detection technique is designed. However, in practice, authentic labelled datasets are in short supply or non-existent (Abdallah et al. 2016). This limitation is further complicated by the need for expert knowledge to create a labelled dataset or evaluate results during model development, which is a time-consuming and expensive process. As a compromise, numerous studies have used a case study analysis on data samples as a proxy of a technique's true capability. Nevertheless, evaluating the performance of anomaly detection algorithms will always be a problem due to insufficient data samples and scenarios. An alternative is to use an ensemble of anomaly detectors along with computer-based knowledge sources (Fanaee and Gama 2014). Lastly, a recent study (Goix 2016) discussed two new approaches, called excess-mass (EM) and mass–volume (MV) curves, to evaluate the performance of anomaly detection approaches on dimensional data without data labels. However, based on the analysis on this chapter, the two approaches have not been employed in anomaly detection on graph data.

Table 2.5. Domain of interest, highlights of the research, challenges faced and future directions

Graph Methods	Application Areas	Reference	Focus of Analysis	Highlights of Approach and Detection Improvements	Challenges (C) and Future directions (D)
Structural-based	OSN	(Jiang et al. 2014)	Detecting synchronised behaviour (suspicious nodes that have an extremely similar behavioural pattern) and rare behaviour (nodes with connectivity patterns very different from the majority) to spot fake followers and fake accounts	- Effectiveness: high accuracy in spotting synchronised behaviours and catching suspicious source-target groups - Scalability: linear complexity with the number of edges - Parameter-free - Oblivious side information	**D:** Incorporate temporal information and other additional features
		(Hooi et al. 2017)	Spotting fraudsters in the presence of camouflage or hijacked accounts to detect fake followers and fake accounts	- Effectiveness: using sufficient condition to detect fraudsters perfectly (e.g. 100% precision and recall) - Scalability: linear complexity with the number of edges	**D:** Incorporate temporal information
		(Manjunatha and Mohanasundaram 2018)	Spotting suspicious behaviours in online social communities	- Scalability: scalable to a large volume of data using big data in-memory cluster computing	**C:** Dependent on a user-selected similarity threshold.
	Insurance	(Branting et al. 2016)	Assessing healthcare fraud risk to detect fraudulent providers	- Effectiveness: F-measure of 0.919 and an ROC area of 0.960	**C:** Lack of providers known to have committed healthcare fraud **D:** Include additional types of information relevant to healthcare fraud prediction
		(Seo and Mendelevitch 2017)	Analysing healthcare fraud to detect fraudulent insurance claims	- Effectiveness: detecting previously unreported anomalies	**C:** Model fuzzy graphs
	AML	(Bershtein and Tselykh 2013)	Detecting patterns of money laundering and financing terrorism	- Incorporating fuzzy concepts	**C:** Use user-defined parameters based on data from past events **D:** Analyse bigger data samples **D:** Include additional control variables, such as age and size of the companies
		(Fronzetti Colladon and Remondi 2017)	Detecting patterns of money laundering to assess risk profiles of clients involved in the factoring business	- Introducing a predictive, rather than just a detective, model for AML - Using a visual analysis of network data for any suspiciousness detection	**C:** Use user-defined parameters that depend on data from past events
Community-based	OSN	(Tian et al. 2015)	Detecting fraud in Internet advertising for crowd fraud detection	- Requiring nearly no human interaction - Scalability: scalable to a large volume of data - Effectiveness: accuracy of over 90%	**C:** Capture fraud from a vast number of attack sources with low fraudulent traffic
		(Ye and Akoglu 2015)	Detecting opinion spammer groups in the existence of camouflage	- Effectiveness: NMI of over 0.94 for various settings and over 0.95 AUC of PR curve on synthetic data and high accuracy on real-world data - Robustness: robust with a variety of parameters, so it requires almost no tweaking of parameters to work correctly	
		(Wang et al. 2018)	Detecting product review spammers	- Effectiveness: outperforming baselines over all databases used in experiments	**C:** Evaluate the annotation of a huge volume of review data manually **C:** Sloppiness in user evaluation
		(Giatsoglou et al. 2015)	Analysing re-tweeting to find fake users in the presence of camouflage	- Introducing RTGEN, a scalable realistic synthetic data generator	**C:** Spot long-term spam activities in the presence of camouflage
		(Bindu et al. 2018)	Analysing tweeting activities for spamming community detection	- Effectiveness: outperforming baseline methods with a precision, recall, F-measure and TP rate of over 0.85 and FP rate of 0.132	**D:** Evaluate the approach based on more realistic data

	AML	(Novikova and Kotenko 2014)	Analysing mobile payments to detect money laundering	- Introducing an interactive visualisation application	**C:** Use limited visualization techniques
	Banking	(Molloy et al. 2017)	Analysing payment transactions for cross-channel frauds	- Effectiveness: reducing FPR by 63%	
	Trading	(Li et al. 2012)	Analysing trading ring patterns to discover cross-account collaborative fraud for market manipulation	- Scalability: several orders of magnitude faster than the baseline	**C:** Correlate user behaviours across multiple trading accounts
	IOF	(Gamachchi and Boztaş 2015)	Analysing enterprise users' web access pattern to detect insider threats	- Introducing an interactive visualisation application	**C:** Rely on some user-defined threshold parameter that should be refined
	Online Auction	(Liang et al. 2010)	Analysing the social graph of online auction users to detect auction fraud	- Effectiveness: detects suspicious nodes as the compared baseline	
		(Bangcharoensap et al. 2015)	Analysing the social graph of online auction users to detect auction fraud	- Effectiveness: outperforming baseline with 5.3% in NDCG - Scalability: parallelise in MapReduce	**C:** Detect the homophilic behaviour of auction fraudsters who frequently bid in auctions hosted by a seller(s) working in the same collusion group
	Telecom	(Nan et al. 2012)	Analysing voice calls to detect fraud in a cellular network	- Effectiveness: detecting 85% of all the victims and the root cause of 78% of fraud calls	**D:** Apply additional (expensive) approaches, e.g. incorporating billing information, manual investigation, user calls history and instant user fraud reports to analyse the detection results to further confirm the fraud activities
		(Yan et al. 2018)	Detecting telecom fraud	- Effectiveness: outperforming baseline methods with a precision, AUC and F-measure of over 0.80 and recall of over 0.74	**C:** Analyse varieties of callers' and callees' behaviours in the telecom network to capture all types of telecom fraud
	Retail Holding	(Tselykh et al. 2016)	Detecting fraudulent transfer pricing when two subsidiaries agree to overprice imports or underprice exports to declare less profit to pay less tax	- Using data visualisation to find hotspots for fraud	**C:** Rely on data quality and availability to reveal internal relations between companies and their affiliated domain users
Decomposition-based	**OSN**	(Moriano and Finke 2014)	Detecting random link attackers	- Effectiveness: low false negatives	**C:** Rely on some historical data for further analysis
		(Liu et al. 2017b)	Detecting suspicious spikes of bursts and drops in the existence of camouflage	- Scalability: sub-quadratic time complexity - Effectiveness: achieving higher accuracy than the competitors	**C:** Aggregate suspiciousness signals from different attributes
		(Shin et al. 2017)	Analysing stream changes in tensors for fake rating detection	- Scalability: a million times faster - Effectiveness: detecting previously unreported anomalies	
		(Lamba et al. 2017)	Analysing dense blocks in tensors to detect bot-like behaviours	- Scalability: linearly scalable with the size of the data - Generalisability: being applied to a variety of domains - Effectiveness: scoring the suspicious entities with high accuracy and detected previously unreported anomalies	
Compression-based	**Trading**	(Eberle and Holder 2009), (Eberle and Holder 2007)	Analysing business transactions and processes to detect deceptive orders	- Effectiveness: minimum or no false positives	**C:** Find anomalies in graph-based data where the anomalous substructure in a graph is part of, or attached to or missing from, a non-anomalous substructure or the normative substructure
	OSN	(Shah et al. 2016)	Analysing user-product ratings to detect rating fraud	- Effectiveness: 0.87 precision over the top 100 results - Scalability: logarithmic scalability with the number of nodes and linear to the number of edges	**C:** Granularity in user behaviour (e.g. different users may rate products in different ways)

	Insurance, AML, Banking, Trading	(Huang et al. 2018)	Analysing financial and trading transaction to detect financial fraud	- Effectiveness: better detection results on sparse graphs - Ability to trace the origin of suspicious activities	**D:** Incorporate temporal information
Probabilistic-based	**Insurance**	(Carvalho et al. 2017)	Analysing the relations between providers (hospitals) and consumers (cities) to detect healthcare fraud committed by hospitals	- Effectiveness: detecting previously unreported anomalies - Visual analysis and manual labelling	**D:** Detect anomalies in big cities with distributed anomalies **D:** Use more precise evaluations because of the limitations of evaluation using visual analysis and manual labelling
		(Subelj et al. 2011)	Detecting automobile insurance fraud	- No requirement for the availability of large data - The imputation of the domain expert's knowledge - Adopted to new types of fraud as soon as they are noticed	**C:** Rely on some user-defined threshold/factor parameters that should be refined
	OSN	(Dai et al. 2012)	Detecting opinion spammers	- Effectiveness: significant performance gains compared with the baselines	**C:** Make a clear split between opinion groups
		(Wu et al. 2017)	Analysing online reviews for fake review detection	- Robustness: robust to data sparsity - Effectiveness: highly outperforms the baselines - Model parameters are refined through a learning algorithm	**C:** Model the distributions of objects' reviews and users' credibility from sparse review data
		(Shehnepoor et al. 2017b)	Analysing online reviews for spam review detection	- Effectiveness: outperforming the existing methods in AUC and AP - Scalability: linearly scalable with the number of edges	**D:** Incorporate product feature for spammer detection **D:** Incorporate meta-path concept for group spammer detection
		(Dang et al. 2017)	Detecting organised spammers in micro-blogging	- Effectiveness: accuracy of 93.6% for all the topics and an F1-score of 82.1% for anomalous topics	**C:** Detect anomalous topics hijacked by spammer groups from numerous trending topics **C:** Detect the hijacked long-term topics that lasted for days **C**: Scalability issue on large data **D:** Detect new evolving types of spammers
	Online Auction	(Tsang et al. 2014)	Analysing the social graph of online auction users and detect auction fraud, including shilling fraud, reputation manipulation and non-delivery fraud	- Effectiveness: ability to detect all three types of fraud (with an AUC of over 0.98, TPR of over 0.97 and FPR of 0.05) that may happen in an auction, whereas the existing methods are tuned to detect just one of those types each - Scalability: linearly scalable with the number of bids	**C/D:** Rely on some user-defined parameters that should be refined
	OCA	(Phua et al. 2009)	Analysing transaction data for credit application fraud detection	- Real-time scoring of incoming transaction streams - Effectiveness: low false alarm rates and achievement of consistent hit rates	**C:** Scalability is a major limitation as there is a trade-off between efficiency (rapid detection time and high scalability) and effectiveness (high hit and low false alarm rates)
	IOF	(McGlohon et al. 2009)	Analysing companies' general ledger to find accounting fraud	- Scalable: linearly scalable with the number of edges - Robustness: robust with a variety of parameters, so it requires almost no tweaking of parameters to work correctly - Effectiveness: high labelling accuracy of up to 97% compared with spectral clustering - Generalisability: can be applied to a variety of domains	**C:** Rely on experts to assess fraudulent behaviours based on the associated risk of each account
		(Bhattacharjee et al. 2017)	Detecting insider threats in a company	- Effectiveness: AUC of 0.9520, 6% improvement of ROC over the best-performing baselines	**C:** Make more genuine alarms over a user profile that usually undergoes some continuous changes over time

2.3.7 Existing Challenges

Table 2.5 presents the main contributions and specific types of fraud across the 39 research studies. It emphasises their problem focus, approaches to finding solutions, challenges faced in the process and recommended directions for future studies. This table provides a quick guide to relevant works using the GBAD approaches to investigate frauds in networks, informing researchers of the range and nature of application problems faced, GBAD baseline approaches to consider and unsettled areas for further investigations. In the preparation of Table 2.5, four key challenges are further identified. This chapter proposes some recommendations and considerations to serve as a scaffold for the future design of fraud detection mechanisms to address these challenges.

2.3.7.1 Dealing with Unavailability of Data

Fraud is a highly sensitive topic, and many stakeholders are reluctant to share their information on fraud. One of the major challenges in data sharing in various application areas, such as healthcare, insurance and banking, are regulations that prohibit the transmission and distribution of highly confidential personal and financial data. This challenge poses a major obstacle in fraud detection research in sectors where data contain confidential information. Consequently, numerous fraud detection algorithms resort to mathematical evaluation measures, which appear to be the best in situations where only a few databases are available for research. This issue has also prompted researchers to resort to the use of synthetic datasets with different characteristics to test their solutions. Synthetic network generators generally duplicate a small subset of the original network's properties for specific applications, such as community detection (Akoglu and Faloutsos 2009). Some sets of abnormal samples are usually injected into a predefined normal distribution of data (e.g. power-law networks) to generate

synthetic data for fraud or anomaly detection (Akoglu and Faloutsos 2009). Considering that the proposed algorithm is evaluated over mathematical measures, the overall reliability of the empirical evaluation of a fraud detection model using such synthetically generated data may not reflect well the actual problem and case used (Akoglu and Faloutsos 2009; Awrad Mohammed 2014; Nettleton 2016).

The main challenge in the production of synthetic datasets is to make the generated networks mimic various aspects of human behaviour, including noise and randomness, as how these characteristics are incorporated will determine the realism of the simulated networks (Nettleton 2016). With synthetic data, the dataset characteristics can impact the performance of any new methods developed. When designing new algorithm to detect fraud, attention should be directed to ensure that the simulated data reflect the actual network within which the new algorithm is designed to detect suspicious activities (Awrad Mohammed 2014; Nettleton 2016). Otherwise, the performance of the algorithm evaluated within simulated environments will not reflect real-world networks (Awrad Mohammed 2014).

On real-world datasets, the studies published to support the research community are not without their own challenges. This review notes that some real-world datasets have missing elements or that only part of the dataset is made publicly available. These issues make it challenging for the community to effectively evaluate any new methods developed against a published piece of work that used the full dataset. Without the means to adequately benchmark new algorithms, the progress of research in this area will be slow or limited (Awrad Mohammed 2014).

Data anonymisation can address this issue by hiding confidential information while maintaining the analytical utility of the data (Eze and Peyton 2015). This technique enables data scientists and organisations to engage in a win–win collaboration. Data

scientists will have the chance to analyse data in different areas and share their discoveries with businesses. In turn, businesses can be equipped with new fraud detection methodologies.

However, in some cases, even anonymised data have business value for the party owning them. Unauthorised disclosure of such data may damage the party owning them or other parties affected by their disclosure (Ohm 2009). Here, data confidentiality still matters even after data anonymisation, as clever adversaries can reidentify or deanonymise the information hidden in anonymised data by linking anonymised data to outside information to unearth the true identity of the data subjects (Ohm 2009). While it has not been suggested that all anonymisation techniques fail to protect privacy, some techniques have proven to be difficult to reverse (Ohm 2009). Some researchers reject anonymisation as a privacy-protecting panacea (Ohm 2009).

Nevertheless, this challenge should motivate us to continue exploring, or reexamining, the possibility of adapting synthetic data as an alternative to alleviate the data privacy issue. Synthetic network generators offer a common benchmark, enabling multiple groups of researchers to evaluate their research on the same dataset. However, many algorithms that perform well on synthetically generated networks may perform poorly in real applications (Awrad Mohammed 2014) as real data are often messy, possessing isolated nodes, strange degree distributions and unbalanced class distributions. Thus, many challenges related to synthetically generated networks remain. While it is important to continue developing new and better algorithms, there should also be research on areas that answer the following questions: How good or realistic are the synthetically generated networks? Should there be a measure, or are there other ways to gauge this? How can noise and randomness be incorporated in a synthetically generated networks so that the generated network is close to the type of

network that the designed fraud detection algorithms would be dealing with (Nettleton 2016)? How can the efficiency of different synthetic network generators be evaluated?

2.3.7.2 Keeping Track of Network User Activities Over Different Timestamps

Most real-world networks evolve, and fraudsters leverage their dynamics to evade detection by spreading and altering their activities over time, thus camouflaging their real intent, i.e. their fraudulent activities (Ye and Akoglu 2015). This characteristic renders the detection of fraudsters' behaviours even more challenging. Therefore, core criminal behaviour that can withstand such changes over time should be understood (Ye and Akoglu 2015).

This literature review demonstrates that research on fraud detection in dynamic networks is scarce (see Section 2.3.3.4), leaving a research gap that needs to be urgently filled, particularly with the prevalence of OSNs. This suggests that the future design of fraud detection solutions should consider the use of a time-evolving network structure to continuously track suspicious activities across different time-based snapshots.

Dealing with these time-evolving network structures requires several key considerations (see Table 2.5), one of which is that their solutions need to be scalable to balance the trade-off between efficiency (rapid detection time and high scalability) and effectiveness (high hit and low false alarm rates) (Phua et al. 2009). It is also necessary to ensure that the solution is robust as a time-evolving network structure has data sparsity issues (Wu et al. 2017). Hence, suspicious activities from different attributes and times of evolving network structures should be aggregated (Liu et al. 2017b). As a result, the algorithms developed for such networks need to consider new data characteristics.

2.3.7.3 Investigating the Inherent Multiplex Behaviour of Network Users

This review also finds that many current studies do not consider the intrinsic multiplex nature of human interactions. They tend to investigate users' behaviours in simplex social networks, focusing on just one type of activity. However, capturing different aspects of relations and activities among the same individuals can give more clues to detect suspicious activities (e.g. individuals may have different kinds of activities within an online social media platform, such as making friends, sending messages, reviewing profiles, liking posts and poking). This points to the need to analyse all kinds of activities pertaining to the same individual to uncover any suspicious activity (Fakhraei et al. 2015).

A multiplex network contains multiple layers that share the same sets of nodes, with each layer representing one type of communication among entities. To detect anomalies and suspicious activities in multiplex networks, it is important to study the rich information hidden in individual network layers (Pourhabibi et al. 2019). Analysing just one mode of interaction cannot provide a complete picture of the relationships among network users. Thus, it will be inadequate, if not unrealistic, to focus on a singular view using simplex social networks to detect fraudulent activities. Yet, detecting suspicious activities in multiplex networks remains a relatively unexplored research area.

Given that social interactions in communities comprise different and multiple types of relationship (Fakhraei et al. 2015; Pourhabibi et al. 2019), a pragmatic fraud detection solution or algorithm should acknowledge and consider the varieties and abundance of human interactions that multiplex networks better capture. Neglecting such a multiplicity of human interactions can lead to information loss and may obscure important information from being discovered (Fakhraei et al. 2015; Pourhabibi et al.

2019). Furthermore, such interactions in multiplex networks are digital footprints of potential fraudsters that need to be holistically represented and extracted as important evidence for combating frauds and possibly crimes (Fakhraei et al. 2015; Pourhabibi et al. 2019). Consequently, feature engineering and graph representation learning (also called graph embedding) are reported as the two main families of approaches for extracting and representing the structural features or characteristics of multiplex networks (see Section 2.2.5).

2.3.7.4 Eliminating Human Intervention in Structural Information Extraction

Recently, there has been a surge towards the use of graph representation learning (or graph embedding) techniques to automatically encode the structural information about the network (Cai et al. 2017). The key idea behind these approaches is to learn the mapping of embedded nodes, links or the entire network and transform them into a lower-dimensional vector space to extract important hidden structural features. This is different from traditional approaches, such as feature engineering, which relies on prior knowledge of domain experts to hand-engineer features (e.g. degrees, clustering coefficients). In large and time-evolving networks, feature engineering is time-consuming, expensive and, ultimately, lack scalability as detection models will need to be regularly updated to reflect the fraudster's altered behaviour and activities (Hamilton et al. 2017).

It has been shown that graph representation learning techniques extract structural information from networks without the need for knowledge experts and can be adopted to learn and capture the structural information of time-evolving multiplex networks. As a result of recent developments in deep learning methods (Goyal and Ferrara 2018; Zhong et al. 2016), numerous graph representation learning techniques have been developed to deal with massive network data. These techniques include graph

convolutional networks (Schlichtkrull et al. 2018b), graph attention networks (Veličković et al. 2017) and recurrent networks (Palm et al. 2018). Another reason to consider graph representation learning is that in many of the reviewed literatures, subsequent stages of fraud detection require the topological and structural characteristics of the network to be preserved. For example, many solutions include an anomaly detection stage that uses machine learning tasks (e.g. clustering and classifications), requiring this structural and topological information to operate.

Despite all said, the role of human experts is irreplaceable for the time being. Any detected anomaly will still require the assessment of domain knowledge to make adjustments based on the given complex situations of an application domain. As far as automation goes, algorithms can assist with scoring to create blocking mechanisms (Phua et al. 2009) and block any suspicious fraudulent activities or behaviours by having regular expert input to improve the detection capability (Bhattacharjee et al. 2017).

2.3.7.5 Relation to Criminological Theories

There is a theoretical void among current studies applying the GBAD technique in fraud detection. None of the reviewed studies have made explicit reference to some of the core principles of criminological theories, e.g. differential association theory (Sutherland 1939) and social disorganisation theory (Shaw and McKay 1942), to support their proposed algorithms for the detection of ‘suspicious’ activities or ‘bad’ communities in social networks. Applying principles of criminological theories to substantiate assumptions about criminal behaviours or crime commitment patterns when developing fraud detection algorithms give validity to the techniques in informing appropriate prevention and intervention strategies (Payne et al. 2019). Therefore, this thesis draws on the tenets of criminological theories to develop fraud detection

algorithms based on theoretically substantiated concepts and empirically demonstrated findings.

2.4 Chapter Summary

This chapter sets out to identify, analyse and synthesise various GBAD approaches employed in the research of fraud detection. Using eight questions that separately probe a specific aspect of GBAD-based fraud detection studies to develop a classification framework, this chapter systematically analyses 39 academic papers identified through a systematic literature search. The systematic review unearths three major issues.

First, the current research on GBAD has not drawn on principles from core criminological theories, such as differential association theory (Sutherland 1939) and social disorganisation theory (Shaw and McKay 1942), to detect criminal activities in social networks. Second, the existing literature has not sufficiently addressed the connectivity patterns in time-evolving networks and multi-layer networks when extracting structural features to represent network characteristics and differentiate suspicious from normal users. Third, the learning algorithms in feature engineering are highly dependent on human intervention, which may lead to scalability problems and loss of accuracy in the proposed algorithms. This point is especially important when attempting to detect criminals who form co-offending groups to commit collaborative criminal activities that pose a continuous threat to global society by causing harm to social, technological, environmental and political infrastructure. Members of such covert groups try to hide their actual networking activities by engaging in different ‘cover-up’ activities to reduce the possibility of being identified (Erickson 1981; Warnke 2016). These kinds of cover-up activities render the process of a manual analysis of the network and the design of features by experts more difficult and complicated. Such

a complexity is caused by the fact that the design of features depends on leveraging human intuition to interpret implicit suspicious signals within the network, which requires technical expertise to brainstorm the ideas and implement them, and is limited by creativity, expertise and time. Moreover, the designed features may not be able to single out the suspicious behaviours, leading to a reduced accuracy (Zhu 2019). They may also not be scalable for large networks owing to the complexity of their design, implementation, and extraction (Keikha et al. 2019).

In developing fraud detection algorithms to answer the research questions using the GBAD approach, this research directly addresses the three issues (Table 2.6). First, it analyses the commitment of crime from the perspective of five criminological theories to determine how criminologists approach crime problems and introduce solutions to detect or prevent them. They provide the theoretical foundation for the proposed algorithms presented in Chapters 4–6. Second, to capture the connectivity patterns in time-evolving networks and multi-layer networks, this research uses feature engineering to extract scalable attributes that can preserve network structure to detect deviant users and anomalous activities (See Chapter 4). Third, to reduce dependence on human expert interventions in using feature engineering, two other techniques are used to automatically extract structural characteristics to detect suspicious criminal activities (see Chapters 5 and 6).

Table 2.6. Summary of issues and contribution of this thesis to address them

Issue	Contribution of this thesis	Chapter discussed
Extant GBAD research lacks theoretical foundations for criminal activities detection	Develops the theoretical foundation of the proposed GBAD algorithms	Chapter 3
Connectivity patterns in time-evolving and multi-layer networks insufficiently addressed in extant literature when extracting structural features	All the algorithms developed in this thesis are applicable both in multi-layer networks and monoplex networks	Chapters 4-6
Extant research using GBAD approaches to detect anomalies in networks does not keep track of Network User Activities Over Different Timestamps	human-engineered features or feature engineering of deviant characteristics within a time-evolving network are proposed	Chapter 4
High dependency of learning algorithms in feature engineering on human intervention, resulting in scalability problems and loss of accuracy	Two algorithms are introduced to automatically extract structural features from social networks without human intervention	Chapters 5-6

3 Chapter 3—Theoretical Background

Criminological theories explain crimes and criminal behaviours by posing questions that dig into different aspects of crime commitment, such as causes, patterns and crime prevention: What are the factors contributing to crime occurrence? Why do people commit crime? Why is the likelihood of crime incidence higher in specific suburbs or some specific periods? Why are some people frequently victimised? How could crime and criminals be detected and deviant behaviour prevented? These questions call for an understanding of criminals' motivations and behaviours, crime drivers and commitment patterns, formed by the complexity of criminal events, and target characteristics exhibited in a specific environment (Brantingham et al. 2016; Wortley and Mazerolle 2009; Wortley and Townsley 2016). Criminologists explore responses to such theoretical questions through empirical studies to derive 'rules' and 'theories' that ultimately lead to strategies for crime detection and prevention (Wortley and Mazerolle 2009).

These ultimate crime analysis strategies provide information about crime patterns and trends on which law enforcement agencies could rely to conduct criminal investigations, develop methods and plan preventive and detective strategies (Emig et al. 1980). One possible approach for such analytical practices to explain crime patterns is to analyse environmental and social influences (Wortley and Mazerolle 2009) using SNA.

SNA, a method of examining social structures and processes using networks and graph theory (Wilson 1986), is becoming an essential component in criminal intelligence analysis (Bouchard and Malm 2016). The reason is that crime is relevant to the behaviour of individuals who interact with others within a social system (Bichler and Malm 2015). Social networks reveal the relational patterns among the social units

(individuals or organisations) and the implications displayed by such patterns (Sarnecki 2001). Given the importance of the social environments and social influences in the aetiology of crime and delinquency, network methods are becoming increasingly used to analyse crimes and criminal behaviours (Bouchard and Malm 2016).

This chapter first presents different criminological theories that have been adopted to explain crime, crime drivers and criminal behaviour. These theories broaden insights into how criminologists approach a crime-related problem through the lenses of the criminological theories when applied to different crime contexts. Because this thesis aims to develop algorithms for detecting a deviant behaviour within social networks, this chapter introduces SNA. Including models rooted in the GBAD techniques, SNA provides tactical and strategic detective methods based on theories that explain 'how' to detect a deviant behaviour. Using these theoretical foundations and the tactics explored by SNA, the next three chapters are devoted to developing algorithms using GBAD techniques for detecting a deviant behaviour within social networks.

3.1 Crime Analysis: Criminological Perspective

Criminological theories have provided substantive knowledge on criminals' motivations and behaviours: *why* people commit crimes, *what* conditions should be met *and where and when* a crime is more likely to happen and *how* crimes could be controlled, prevented and detected (Gilmour 2016) (Figure 3.1).

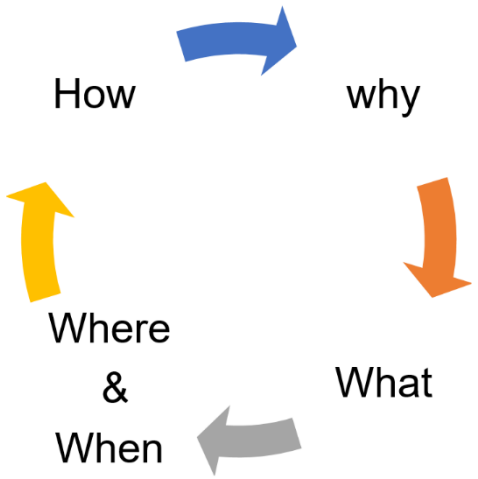

Figure 3.1. Crime analysis: why, what, where and when and how.

Criminological theories are essential facilitators in identifying the viable causes of crime and supporting the detective or preventive mechanisms (Gilmour 2016). This research adopts five theoretical perspectives that are linked to answering the *why, what, where and when* and *how* of criminal motivations and behaviours:

- Rational choice theory (*why*) (Cornish and Clarke 2014),
- Routine activity theory (*what*) (Cohen and Felson 1979),
- Crime pattern theory (*where and when*) (Brantingham and Brantingham 1993),
- Differential association theory (Sutherland 1939) and social disorganisation theory (Shaw and McKay 1942) (*how*).

The aforementioned theories form the theoretical foundation of this research. This research raises understanding about crime and its motivators using the first three theories (why, what, where and when); by focusing on the last two, it finds strategic solutions on how to detect a criminal act. In the following sections, each of these theories is first explained from the perspective of criminology. The discussion then moves to examine SNA as a crime analysis tool and *how* to detect crime under the

tenets of differential association and social disorganisation theories with the help of SNA.

3.1.1 Why: Rational Choice Theory

The rational choice perspective is a utility-based theory in criminology that is aligned with cost–benefit analysis. Rational choice theory (Cornish and Clarke 2014) has different features (Paternoster and Simpson 1993). First, it views the decision to commit a crime as a rational choice, trading off the probable costs and benefits of the action (Paternoster and Simpson 1993). While the rewards of crime can vary from obtaining specific status in the covert community (Perry and Hasisi 2015), fame or honour among criminals (Orehek et al. 2009; Perry and Hasisi 2015), increase in financial utility and religious rewards to regime change or social revolution (Davis and Cragin 2009; Nemeth 2017; van Um 2011), the cost of criminal activity includes, but is not limited to, the possibility and severity of formal and informal legal sanctions, moral costs, loss of legal alternatives to action and loss of self-respect (Paternoster and Simpson 1993).

Second, because the perceptions of the risks and rewards of crime differ, and the kind of information required and used by offenders to commit a crime varies across different crimes, rational choice models of offending are crime-specific (Paternoster and Simpson 1993; Thomas et al. 2020). For example, criminals may have the tendency to specialise in certain types of crime (e.g. property crimes vs. robbery) (Thomas et al. 2020).

Third, the offending decisions in a specific criminal event are influenced by the contextual features of the crime (Paternoster and Simpson 1993). In street crime, for example, the offending decision is influenced by various circumstances, such as vulnerability of the target, ease of escape, existence of security devices or probability

of meeting an armed or resisting victim (Akers 1990; Johnson 2014; Paternoster and Simpson 1993).

On the premises of the rational choice theory, many studies (see, e.g. (Arsovska and Kostakos 2008; Holmes 2009; Kao 2014; Pizarro et al. 2020)) have introduced a rational choice model of criminal activities to delve into different aspects of crimes. For example, by applying rational choice theory, Carson et al. (2020) unveiled the behaviour of eco-movement radicals and their motives. Using this theory, the authors investigated the trade-off between cost and benefit in radical eco-movements: whether the arrest of the activists or environment-threatening (i.e. cost) or environment-protecting actions (i.e. benefit) of the US federal government impact the risk of radical incidents. As a whole, they found that when government actions increase the costs of perpetration, radical movements decline, and when government actions allow benefits to be gained, more eco-incidents occur. Arsovska and Kostakos (2008) examined the rationality of getting involved in illicit arm trafficking. They found that individuals engaged in arm smuggling according to specific needs, and based on those needs, they set specific goals, which can vary from making profit to gaining power. Accordingly, they search for the opportunities, including illegal means, to achieve their goals. These interpretations depend on the person's prior history, not just a particular moment. Moreover, arms can provide individuals with a choice to spare or take lives. Holmes (2009) also found that corporations got involved in corporate crime because, relative to the value of the gains, the punishments meted out to them are minor in comparison. Therefore, relative to the risk taken by corporations, the rewards are bigger (Holms, 2009).

In sum, rational choice theory attempts to establish the motives for criminal acts and answer the question '*why* people commit a crime'. It argues that the rationality

behind any criminal decisions weighs the costs lower than the risks involved. Within the scope of this research, people get involved in cybercrime as compared with the high benefits (e.g. opportunity for sexual abuse, child pornography and phishing), the risk of being caught is low due to the lack of policing in cyber space (Hu et al. 2014). The formation of criminal organisations is also rational, motivated by maximising a utility (e.g. financial, religious and power) (van Um 2011), since the risk of getting caught by local security force and police is typically low (Masucci 2013).

3.1.2 What: Routine Activity Theory

An extension of the rational choice theory is the routine activity theory (Cohen and Felson 1979). Routine activity theory seeks to explain the occurrence of crime by primarily focusing on three elements required for a crime to occur (Figure 3.2): i) a motivated offender with criminal intentions, ii) the presence of a suitable target or victim and ii) the absence of a capable guardian governance in the same time and place (Cohen and Felson 1979).

This theory links the patterns of offensive activities to everyday patterns of social interactions (Brantingham 2010). It suggests that criminals find their potential targets at the intersections of their routine activities with those of their victims (Cohen and Felson 1979). Along their routine activities, people develop strong awareness about their activity space. These activity spaces denote the areas people are most familiar with (Brantingham 2010). This feature indicates that crime is more likely to happen among normal activities and near awareness space (Bichler et al. 2017). Therefore, routine activities of potential criminals generally provide a clue to the location where, and the times when, a crime is more likely to happen.

Figure 3.2. Routine activity theory: three factors for a crime to occur (Modified from source: (Abt 2017, p. 270)).

Among many research studies analysing crimes using this theory, those of Choi et al. (2019), Marcum et al. (2010) and Hutchings and Hayes (2009), for example, demonstrated that routine activity theory is a feasible theoretical framework when applied to cybercrime investigation. One of the findings from these research studies indicates that individuals who extensively use the computer and the Internet in their daily routine activities make suitable cybercrime targets and are more likely to be attacked by motivated cyber offenders. This victimisation is due to the absence of a capable guardian (e.g. the amount of monitoring by a respondent, self-protective measures and law enforcement). This finding supports the tenets of the routine activity theory. Murphy (2019), who studied the dynamics of terrorism and trafficking in South Asia, also found that poor young people are suitable targets of opportunist traffickers and terrorist activists due to poor governance and weak economic structure in South Asia.

Therefore, empirical evidence supports routine activity theory: social and environmental factors make some segments of the population more vulnerable to criminal activities compared with others. The theory prompts criminologists and law-makers to explore the question '*what* conditions would make an ideal breeding ground for a crime to occur'. Cybercriminals are drawn to OSNs, an activity space in the cyber

world with no or minimal policing, so they could easily reach their potential targets (e.g. female, youngsters) and commit their deviant behaviours (Conradt 2012; Karmen 1984; Pourhabibi et al. 2019). Criminal networks also grow due to the lack of guardianships by local security force. Active criminals (i.e. motivated offenders) could easily reach their target accomplices, i.e. criminal counterparts selected from the same awareness or activity space (e.g. those with similar ethnic background, friendship or kinship groups) (Blau 1977).

3.1.3 Where and When: Crime Pattern Theory

Research on environmental criminology suggests that crime is not randomly or evenly distributed in space (Higgins and Swartz 2018). Rather, it tends to occur in clusters and hotspots, in specific locations and time following specific patterns (Higgins and Swartz 2018). Criminology defines these clusters or hotspots as predictable areas where the frequency of occurrence of crime is high (Courtney 2018). Extending from routine activity theory's three elements for a crime to occur, crime pattern theory (Brantingham and Brantingham 1993) focuses on where and when criminal events occur. Crime pattern theory suggests that offenses typically occur in areas that are already known to criminals. As a consequence of engaging in their routine activities (Cohen and Felson 1979), criminals grow their awareness spaces (also known as activity space) (e.g. their home, places of work and recreation and people they know) (Brantingham and Brantingham 1993) and create patterns (in time and space) of their covert activities around their awareness spaces (Eck and Weisburd 1995). Therefore, crimes are more likely to occur in areas where suitable targets overlap the offenders' awareness space (Eck and Weisburd 1995).

Hewitt et al. (2018), for example, used this theory to analyse the characteristics of the places that sex-related crimes are more likely to occur. They found that in

geographical areas with a high percentage of adult females (potential victims), young adult males (motivated offenders) and single individuals (absence of capable guardianship) high rates of sexual crimes were reported. Interestingly, their finding was also in agreement with routine activity theory. Drawing on the realm of this theory, Paraskevas and Brookes (2018) studied human trafficking in the tourism industry. They confirmed that tourist activities are incubators of labour and sexual exploitation in human trafficking, where hotels serve as the activity spaces where offenders and their potential victims converge with hotel employees and managers functioning as the guardians.

Crime pattern theory, therefore, helps increase our understanding of location and time choices of offenders for committing their crime, thus answering the question '*where and when* crimes occur'. Within an online dating social network, cyberspace acts as a virtual space where a crime happens. Within this space, criminals converge with their targets and create patterns through virtual communication with them (Miró-Llinares and Moneva 2020). In forming criminal organisations, these patterns are formed among people who tend to co-offend in the form of clusters within their network (Brantingham and Brantingham 1993; Miró-Llinares and Moneva 2020).

3.1.4 How: Differential Association Theory

Sutherland's (1939) differential association theory in criminology is perhaps the first criminological theory closest to network analytical thought. Sutherland's theory of differential association posits that individuals learn the techniques of committing crimes and acquire the motives, rationalisations and attitudes for criminal behaviour through interactions with others, principally delinquent peers or deviant parents (Hawdon 2012; Levin et al. 2012; Sarnecki 2001). The important features of this theory for explaining criminal activity are the frequency, intensity and durability of interactions,

which can be attributed to links between network members (Hawdon 2012; Levin et al. 2012; Sarnecki 2001). ‘A person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of law’ (Sutherland et al. 1992, pp. 6–7). These definitions are consolidated when high-profile criminals’ contacts with other individuals are established (Sarnecki 2001). Therefore, connections presented more frequently, with longer exposure periods, linked to a more prestigious source or more intense relationships, would receive more weight under the realm of this theory (Matsueda 1988). As presented in Sutherland’s theory (1939), this notion implies that powerful criminal members of a network are more likely those who are (Gallupe and Gravel 2018): i) highly connected, ii) have ties with others and iii) act as a link between disconnected groups.

Drawing on the tenets of this theory, Klein and Cooper (2019), for example, analysed the interactions (e.g. number of sexual partners, frequency of sexual activity and frequency of masturbation) among college students to determine the intensity of cybersex activities. They found that peer associations have a strong influence on individuals’ engagement in deviant cybersex activities. The theory is also adopted to test the connection between drug use and youth crime by Trajtenberg and Menese (2019). In their analysis, they used three proxy measures, namely, presence, intensity and duration of involvement in the crime. They found that the use and exchange of illegal drugs is a key explanatory factor in crime and violence.

In short, this theory posits that criminal behaviour is cultivated through interactions, and by analysing these interactions, criminologists could determine ‘*how* to detect criminal activities’. Accordingly, deviant behaviours within a social network can be detected by analysing the social interactions within the ego’s personal network through

a search for patterns of interaction frequency, duration, priority and intensity (Hanneman and Riddle 2011).

3.1.5 How: Social Disorganisation Theory

Social disorganisation theory hypothesises that a neighbourhood's ecological characteristics (e.g. low economic status, ethnic/racial heterogeneity and residential inequality/mobility) have an important influence on social disorganisation in communities, which ultimately leads to higher crime rates (Parker and Stansfield 2014). Social disorganisation is defined as 'the inability of local communities to realise the common values of their residents or solve commonly experienced problems' (Bursik 1988, p. 12). This indicates that poverty, residential mobility, ethnic heterogeneity and weak social ties would decrease a neighbourhood's capacity to control crime and hence increase the likelihood of crime (Kubrin and Weitzer 2003). In turn, the development of formal and informal social ties, social capital (e.g. social cohesion (Kennedy et al. 1998)) and collective efficiency (e.g. mutual trust among people (Sampson et al. 1998)) promotes the ability of the community to socially control or impede delinquency (Parker and Stansfield 2014). Worrell et al. (2013) contend that growth in social control (i.e. strong ties among communities) will reduce crime and disorder, as presented in Figure 3.3.

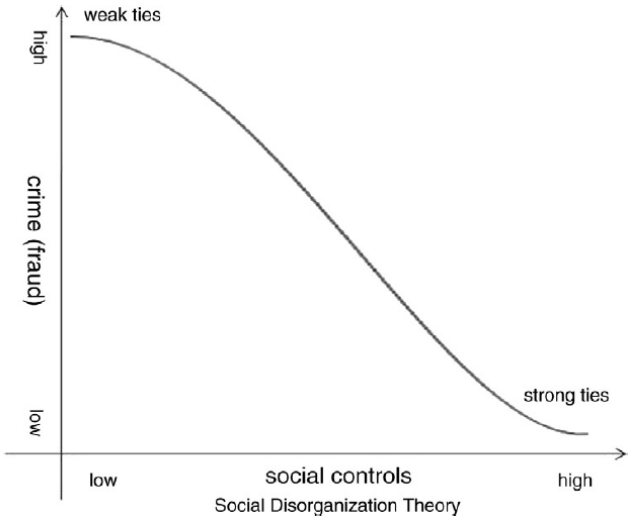

Figure 3.3. Social control and crime as explained by social disorganisation theory (Source: (Worrell et al. 2013, p.133)).

Carter et al. (2020), for example, adopted social disorganisation theory and routine activity theory to explore the role that different ecological and socio-demographic variables (e.g. median household income, renter percentage, multifamily housing count, homeownership and percentage of African-American residents) play in predicting patterns of property and vehicle crime incidents. Their findings reveal that the hotspots of crimes typically emerge in high-traffic areas (e.g. higher renter-occupied housing, commercial areas and areas with high residential turnover) of the city bordering low-income areas. Another study by Kajeepeta et al. (2020) adopted the principles of this theory to prove that place-based interventions have an immense influence on reducing crime incidents in urban settings. They reported that in neighbourhoods with higher bar densities, the percentage of violence is higher. Therefore, by increasing social control or social awareness (e.g. through the increased presence of police or their neighbours) in such areas, it would be possible to reduce the occurrence of such crimes.

Using the framework of this theory, criminologists can determine places or communities prone to persistent crime occurrences. This outcome can be a useful

theoretical foundation for the development of policing strategies to identify such crime-prone communities or people and answer the question '*how* to detect criminal activities'. Within a dark network, the presence of dense portions is a sign that criminals are creating high-density social ties. The identification of those portions thus helps detect criminals and disrupt their criminal activities (Carrington 2011).

3.2 Social Network Analysis as a Crime Analysis Strategy

The criminological theories attempt to explain crime patterns and motives by analysing environmental and social influences (Wortley and Mazerolle 2009). Such analysis ultimately leads to the development of crime detection and prevention strategies (Emig et al. 1980), which could be applied in SNA.

Network analysis was first introduced by Sparrow (1991) as a potential tool to assist law enforcement agencies in criminal investigations. However, it was almost a decade after Sparrow's (1991) proposal that SNA started to become popular in criminal intelligence studies following Krebs' (2002) investigation of the 9/11 attack using SNA.

SNA includes a theoretical perspective and a set of methodological techniques (Carrington, 2005). As a theoretical perspective, it considers the interdependence and relations (e.g. trading patterns, friendship and co-offending) among social actors (e.g. individuals, organisations, websites, cities and neighbourhoods). SNA views the social world as patterns among the interacting units and the implications displayed by those patterns (Carrington, 2005). The relationships and interdependencies in the social world are reflective of the processes and consequences of interacting behaviours (Haynie and Soller 2014).

From a methodological perspective, SNA refers to a class of techniques rooted in graph theory called GBAD approaches (Velampalli and Eberle 2017), which extends

to other models, including statistical, algebraic, simulation and agent-based models, and has been used extensively in studying relational patterns (Carrington, 2005).

In criminal investigations, SNA has significantly contributed to understanding the root causes of deviant behaviour and crime. For example, it has been widely used for profiling organised crimes (Basu and Sen 2021; Calderoni et al. 2020; Duijn and Sloot 2015; Saidi et al. 2017), financial crimes (Didimo et al. 2014) and cybercrimes (Han et al. 2019; Singh et al. 2020) as well as identifying key players in criminal events (Lee et al. 2020), among others. Essentially, the utility of SNA to law enforcement comes from the fact that knowing who a person is associated with can aid in predicting that person's future decisions (Overland Park 2018). Therefore, SNA provides practical guidance for crime prevention and detection efforts (Overland Park 2018).

The next two sections present two principal tenets of SNA analysis applied to crime and deviant behaviour (Carrington 2011): i) peer influence and ii) co-offending. Under each principle, this chapter further elaborates how network analysis strategies are drawn from the principles of criminological theories to explain '*how* criminal acts can be detected' (see Sections 3.1.4 and 3.1.5).

3.2.1 Peer Influence On Delinquency

One of the most popular uses of SNA in criminology is analysing the influences that personal networks have on adults' delinquency, which is called peer influence (Carrington 2011). Many criminological studies have focused on the analysis of social relationships to examine the roles that peers play in criminal activities (see e.g. (Eriksson et al. 2016; Lee et al. 2020; Liu et al. 2014; Philippe 2017; Stevenson 2017)). Peers can be defined as friends (Lee et al. 2020; Liu et al. 2014), family members (Eriksson et al. 2016), people that spend time together in prison (Stevenson 2017) and co-offenders (Philippe 2017). The scope for peer influences and the underlying

influence mechanisms may also vary by crime type (Lindquist and Zenou 2019). However, the common element among these studies is that they all have demonstrated that peer influence and becoming delinquent stemming from repeated contacts with close peers, an inherently social phenomenon, imply a process of social interaction. They also suggest that the source of crime and delinquency is located within the very intimate social networks of individuals (Baerveldt et al. 2008; Gallupe et al. 2015; Gerstner and Oberwittler 2018; Grund and Densley 2014; Haynie 2001; Haynie et al. 2014; Haynie and Osgood 2005; Jose et al. 2016; Kreager et al. 2011; Rees and Pogarsky 2011; Sarnecki 1990; Schaefer 2012; Weerman 2011; Young 2011). Carrington (2011) argues that these social communications can be investigated using SNA. Baerveldt et al.(2008), for example, analyses a friendship network to demonstrate that one of the best predictors of crime involvement among adolescents is exposure to delinquent peers. Gallupe et al. (2015) suggest that adolescents who exhibit a high capacity for delinquency have higher social status and are more popular (i.e. have high centrality). Gerstner and Oberwittler (2018) also employed network data analysis to determine the extent to which adolescents get involved in delinquent activities in the absence of adult supervision and how dependent this behaviour is on the delinquent inclinations of their peers.

The theories of delinquency, such as differential association theory (Sutherland 1939), are rooted in a framework in which the interactions between individuals and their social environment are a key component in analysing crime and delinquency. As explained in Section 3.1.4, differential association theory focuses on the frequency, strength and intensity of social interactions with others and contends that delinquency is learned within close relationships (Bouchard and Malm 2016; Haynie and Soller 2014): the more cohesive the network, the more robust the association between peers

and delinquency (Bouchard and Malm 2016; Haynie and Soller 2014). This theory states that the behaviour of one's personal network affects one's ego's behaviour and attitudes, and these effects can be depicted by the characteristics of the network. The concepts advanced by this theory can be operationalised using the SNA method. 'The intimate personal groups' (Carrington 2011, p. 237), in which crime is learned, are simple ego's personal network which can be measured using various metrics, such as frequency, duration, priority and intensity (Hanneman and Riddle 2011). Further, ego's social integration, which is defined as the social cohesion among the neighbours along with their inclination to involve in a common good, can be measured by modularity or density within a group (i.e. discovering partitions of the network with higher density or partitioning the network into clusters where members in each cluster have the maximum number of interactions with each other but minimum connections with members in other clusters (Luan et al. 2019)) or the average degree between a pair (Carrington 2011).

3.2.2 Co-offending: Crime as a Group Activity

Crime is an inherent group activity (Gravel and Tita 2017), and co-offending is the actual involvement of an individual in an illegal behaviour with others (Reiss and Farrington 1991, p. 361). A large portion of very serious criminal activities is perpetrated by co-offending individuals as organised groups of criminals (Lindquist and Zenou 2019), including street gangs (Grund and Densley 2012; McGloin 2005; Papachristos 2009; Sierra-Arévalo and Papachristos 2015), secret societies (Erickson 1981), criminal enterprises (Campana and Varese 2012; Morselli 2009), illegal drug market (Berlusconi et al. 2017; Malm and Bichler 2011; Morselli et al. 2017; Natarajan 2006) and terrorist groups (Krebs 2002).

Co-offenders tend to engage in collective activities with ‘similar’ others (Papachristos 2013). This homophily feature, reflective of the idiom ‘birds of a feather stick together’ (Glueck and Glueck 1950, p. 361), can be explained in a criminal context in two different ways (Grund and Densley 2014).

The first explanation is that individuals tend to form social relationships with similar others. As such, the literature on co-offending demonstrates that co-offenders exhibit strong propensities towards homophily characteristics, e.g. age (Carrington 2014b; Sarnecki 2001), gender (Carrington 2011; Sarnecki 2001; van Mastrigt and Carrington 2014), place of residency, criminal experience and ethic homophily (Grund and Densley 2014; Sarnecki 2001).

These similarities lead to the second explanation: there is a psychological preference for criminals to select similar people as accomplices or co-offenders to achieve a common illegal goal (Carrington 2014a; Faust and Tita 2019; Grund and Densley 2014). Offenders’ selection of co-offenders is not a random process (Cornish and Clarke 2014) but follows a rational decision-making process where co-offenders are systematically selected from a large pool of potential accomplices (Tremblay 1993). In addition, most of the offenders already know their co-offenders from the conjunction of their routine activity space, as the routine activity theory indicates (Cohen and Felson 1979). Therefore, Tremblay’s (1993) extension of routine activity theory explicitly connects co-offending selection to SNA (Carrington 2014a), which is the offenders’ desire to connect to similar other with whom they can form i) the strongest possible ties (who looks to be more trustworthy) (Carrington 2014a) and ii) ‘weak but useful ties so as to increase the scope and value of crime opportunities’ (Tremblay 1993, p. 26). In other words, co-offending decisions are networked decisions (Bouchard and Malm 2016), and the emergence of the network paradigm in

criminology had a great impact on the way law enforcement agencies and criminologists approached organised crime, gangs and illicit networks. Once each offender is mapped to a pool of potential accomplices as a social network, the analyst can start understanding the selection mechanisms, and the flow of the influences among co-offenders more precisely (Bouchard and Malm 2016).

Among the criminological theories, social disorganisation theory (Shaw and McKay 1942), which explains the formation of criminal communities, hypothesises that community structures characterised by instability and heterogeneity, contrary to similarity and homophily (first explanation) and weak social ties (second explanation), can foster illicit activities and crime (Shaw and McKay 1942) (see section 3.1.5). Co-offending groups having a similar nature in that sparse and unstable networks are composed of weak connections, which implies that co-offenders have a tendency to evade detection (Tremblay 1993). Furthermore, as hypothesised by social disorganisation theory, the absence of a regulatory system reduces the ability to formally or informally control the behaviour of individuals. This may increase the opportunities for individuals to engage in deviant activities (Shaw and McKay 1942). Due to the lack of regulation and monitoring by local law enforcement agencies, individuals within co-offending groups may influence their network to engage in deviant behaviours (Monk et al. 2018). Reiss (1986), however, raised a paradox: high crime groups often seem to be both organised and disorganised simultaneously. In other words, due to their deliberate attempts to form weak ties with peers, which results in a sparse network (disorganised), criminal groups also exhibit a high density of social ties in some parts of the network (organised) due to their failure to conceal their covert activities (Waring and Weisburd 2000). The presence of such covert communities

(dense portions) within a network can be measured by modularity or density within a group (Carrington 2011).

3.3 Chapter Summary

This chapter reviews different aspects of criminal activities through the perspective of five criminological theories to discuss why people engage in deviant behaviours (rational choice theory), what conditions are conducive for a crime to occur (routine active theory), where and when a crime is more likely to happen (crime pattern theory) and how law enforcement agencies can detect, prevent and control a criminal event (differential association theory and social disorganisation theory).

Since this research uses SNA rooted in graph theory (GBAD techniques) as an approach to develop fraud detection algorithms and detect a deviant behaviour, the discussion also extends to two principal concepts of SNA in crime detection and elaborates on theories that explain 'how' to detect a deviant behaviour using SNA. More specifically, it highlights how *differential association theory* explains the influence of criminal peers on their intimate network, followed by a discussion on how *social disorganisation theory* helps explain the formation of criminal groups in social networks. In short, this chapter has raised an understanding about different aspects of crime analysis and how criminologists analyse a deviant behaviour and introduce solutions to detect or prevent crime. In addition, it explains how these theories are related to the scope of this research and demonstrates that the basic tenets of differential association theory and social disorganisation theory are closely linked to SNA. Drawing upon the premises of these two theories, this thesis develops fraud detective strategies using the GBAD techniques in the next three chapters.

4 Chapter 4—Discovering Spammers in an Online Dating Social Network: A Feature Extraction Approach [a]

The increasing popularity of social networks has offered opportunities to collect a huge amount of information about their users, such as their characteristics, habits and friends (Stringhini et al. 2010). This valuable information and ease of access to other users within social networks provide a platform for delinquent users, also known as 'spammers', to behave maliciously and cause inconvenience to others (Fakhraei et al. 2015; Hu et al. 2014). Particularly, spammers frequently attempt to reach their prospective victims by sending unsolicited messages. Spammers usually mimic some patterns of legitimate users' behaviour, making the process of spotting them very difficult (Fakhraei et al. 2015; Hu et al. 2014). Furthermore, a growing number of social networking websites have provided their users with different types of interactions (e.g. tweets, mention, like, wink and poke), resulting in a multiplex network of interactions (Fakhraei et al. 2015). In these networks, malicious users evade detection by frequently changing the nature of their activities (e.g. message passing, sending friendship requests, poke and Like) (Fakhraei et al. 2015). This feature makes it challenging to analyse users' interactions to capture anomalous behaviours.

Many studies on the detection of spamming activities, e.g. (Benevenuto et al. 2010; Gao et al. 2010; Shehnepoor et al. 2017a; Wang 2010; Yang et al. 2013; Zheng et al. 2015), do not consider the intrinsic multiplex nature of human interactions. They tend to investigate users' behaviours in simplex social networks by focusing on one type of activity and the content of their messages to detect and filter spammers. Sophisticated

[a] A conference paper developed based on the information presented in this chapter was published: Pourhabibi, T., Boo, Y. L., Ong, K. L., Kam, B., & Zhang, X. (2019), 'Behavioral Analysis of Users for Spammer Detection in a Multiplex Social Network', AUSDM 2018, Springer Singapore, viewed 16 February 2019, <https://doi.org/10.1007/978-981-13-6661-1_18>.

spammers may cleverly manipulate their spam messages to bypass traditional content-based spam filters but would find it difficult to hide their interactions in a network to avoid detection (Fakhraei et al. 2015; Hooi et al. 2017).

The detection and characterisation of these cybercriminals have a significant influence on the quality of user experiences and could promote the healthy use and development of OSNs (Hu et al. 2014). As discussed in Chapter 1, one approach to detect and analyse suspicious activities in a network is to use manual feature engineering. With this technique, data scientists could choose sets of features to differentiate normal and suspicious activities in a network based on the problem domain (Varol et al. 2017).

Drawing on the principles of the criminological theories discussed in Chapter 3, this chapter first analyses crime (i.e. spamming activities) in an online dating website. Through the tenets of differential association theory, it then introduces four different sets of human-engineered features to detect a suspicious behaviour in a time-evolving multiplex dating social network. As explained in Section1.4, this chapter follows the proposed framework in Figure 1.2, which is adapted from Hevner et al.'s (2004) IS framework (Figure 1.1) to address the first and last proposed sub-research questions:

- **SRQ 1.** What set of features can be defined and extracted from a network to capture anomalous activities?
- **SRQ 3.** How can users' anomalous activities be captured in a time-evolving network?

The following sections describe the proposed approach following the sequence of Hevner et al.'s (2004) IS framework in Figure 1.1 (see Section1.4).

4.1 Background Theories: Crime Analysis

This section explores the spamming activities in an online social dating website as a cybercrime act from the perspective of criminological theories. It discusses *why*

people get involved in cybercrime and, in particular, spamming activities in online dating social networks? *What* are the required conditions for spammers to reach their potential victims and commit a crime? *Where and when* spammers commit their criminal acts? And finally, it goes through the criminological theories that help answer *how* to detect criminal activities?

Why. *Rational choice theory* (Cornish and Clarke 2014) postulates that offenders make rational decisions that lead them to perceive more benefits when engaged in particular criminal activities against the risks arising from their behaviours (Paternoster and Simpson 1993).

With regard to spamming activities in online dating social networks, there may be several primary benefits for cybercriminals. For example, sexual predators attempt to interact with potentially vulnerable victims to find their targets online and abuse them (Savage et al. 2014). There are also special types of spammers who launch various attacks, such as spreading ads to generate sales, disseminating child pornography, phishing and befriending victims to grab their victims' personal information (Hu et al. 2014). While the benefits associated with trying to reach new victims by sending unsolicited messages in OSNs are high, the risk of being detected and caught is relatively low (Pourhabibi et al. 2019).

As OSNs provide their users with different types of interactions, offenders are more likely to evade the filtering security measures by frequently changing the nature of their interactions (Agrawal et al. 2014). Furthermore, offenders can continue their online offensive activities anonymously without any apprehension of being identified in OSNs (Pourhabibi et al. 2019). There are also inconsistencies in the application of laws against cybercriminals (Choi 2008; Hinduja and Schafer 2009). Further, the behaviour of victims themselves is also an important factor that reduces the risk that spammers

perceive (Choi 2008; McQuade 2006). In OSNs, victims consider themselves partially responsible and fear to look stupid for being victimised; therefore, they do not report their victimisation to police (Choi 2008; McQuade 2006). Given the low risk of being detected coupled with significant benefits, the behaviour of spammers in OSN supports the tenets of rational choice theory (Choi 2008; McQuade 2006).

What. *Routine activity theory* (Cohen and Felson 1979) contends that crime happens in the intersection of shared activity spaces of offenders and potential targets under a lack of guardianship (McQuade 2006). According to this theory (see Section 3.1.2), exposure to motivated offenders, deviant behaviour, and access to the potential target increase the risk of committing crime. Contrarily, the presence of guardianship acts as a preventive factor (Spano and Freilich 2009).

The 'deviant place factor' concept could be applied to 'cyberspace' when a cybercrime occurs (Conradt 2012; Karmen 1984). Although cyberspace lacks a physical location (Conradt 2012; Karmen 1984), offenders and their potential victims temporarily intersect within a network which acts as a proxy for physical activity space (Reyns et al. 2016). Motivated offenders (e.g. cybercriminals) are drawn to OSNs because of two major reasons (Conradt 2012; Karmen 1984; Pourhabibi et al. 2019): prevalence of potential targets (e.g. youngsters or females willing to meet people online (Yar 2005)) and absence of guardianship (e.g. OSNs allow users to create multiple accounts, continue their activities anonymously or easily get away and disappear from the virtual environment (Yar 2005)). Therefore, victims who are looking for love expose themselves to potential cybercriminals in online dating social networks that lack guardianships, furnishing conducive conditions for cybercrime to occur according to routine activity theory (Conradt 2012; Karmen 1984) (see Figure 4.1).

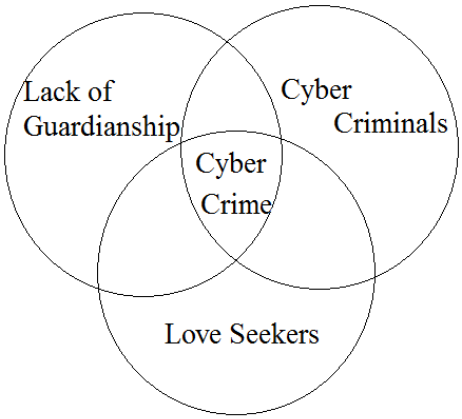

Figure 4.1. Routine activity theory: three factors for cybercrime in online dating social networks.

Where and When. *Crime pattern theory* (Brantingham and Brantingham 1993) assumes that crimes usually occur in specific patterns, at particular times and places (Hartel et al. 2010; Park et al. 2012). This theory suggests that crimes are dependent on the 'nodes' and 'paths' commonly used by the offender (Benson et al. 2009). In a spamming offense in an online dating social network, the nodes are the users seeking to find online friends and even other cybercriminals looking for potential targets. The paths used to navigate between these nodes include the procedures (e.g. message passing, like, and poke) and networks (e.g. friendship) used to establish connections with these users. Cybercriminals create patterns of their movement and activities while navigating through these paths to reach their victims (at the course of their routine activities) (Hartel et al. 2010). In short, crimes do not randomly or uniformly occur in time and space. They happen in clusters and hotspots which are the anomalous concentration of excessive deviant behaviours in specific places and at specific time periods; these are repeat offenders and victims (Brantingham and Brantingham 1993; Miró-Llinares and Moneva 2020). Therefore, online dating social networks are viewed as cyberspace where normal users or criminals converge (Miró-Llinares and Moneva 2020). Within this space, users are linked through virtual connections (e.g. message passing, friendship and followership), and cybercrime is concentrated among certain

users (nodes) and in certain time intervals (Miró-Llinares and Moneva 2020). Knowledge of such malicious users in the social network, when publicised, can alert users to spot suspected offenders who are out to prey on easy targets (Hartel et al. 2010; Park et al. 2012).

How. *Differential association theory* (Sutherland 1939) states that an excess exposure to a deviant behaviour by prestigious criminals may lead to learning and involvement in a crime. The focus of this theory is, therefore, to find patterns of frequency, intensity and durability of interactions within a network (Herath and D'Arcy 2015). Therefore, from the lens of differential association theory, criminals are most likely to be highly connected owing to their goals to influence more individuals and get involved with others for longer periods of time or more frequently (Gallupe and Gravel 2018). The type of relationships and the activities individuals engage in significantly influence the likelihood of crime (Choi et al. 2017). As such, searching and finding such patterns in social communications could lead to the detection of criminals.

In an online dating social network, spamming activities are exerted through connections (e.g. message passing, friendship request) that cybercriminals make with others (Herath and D'Arcy 2015; Venkatesh and Brown 2001). This chapter introduces an approach on how to detect cybercriminals within an online social dating website. Accordingly, to find cybercriminals, this chapter introduces four sets of mathematical features to rate the intensity of users' activity patterns within their 'intimate personal groups' (e.g. ego's personal network) (Carrington 2011) quantitatively as suggested by differential association theory (see Section 3.2.1). This leads to finding potential delinquents who persistently attempt to influence other criminals (e.g. by transferring the skills of cybercrimes) and harass their victims.

4.2 Problem Formulation

Multiplex networks are usually defined in different distinct layers, such that each layer exhibits a different kind of relationship between a common set of network nodes (Liu et al. 2016). In each layer, underlying nodes share the same relationship type (Liu et al. 2016). Therefore, to distinguish different types of edges between each pair of nodes and simulate different layers in a network, a 'relation type' label is assigned to each edge. This label denotes the type of relationship between each pair of nodes (Liu et al. 2016). Figure 4.2 presents a sketch of a multiplex network with two different types of relations presented by layers *a* and *b*, whereas the two layers share the same sets of nodes.

Any directed time-stamped multiplex social network is denoted as graph G where $G = \cup_{i=1}^{R} G_i$, where $i \in R$ is a relation type and $G_i = (V_i, E_i, R_i, T_i)$ is a sub-graph of G. For each sub-graph G_i, E_i denotes a directed relation of type R_i created between each pair of vertices from the vertex set V_i at timestamp T_i (Fakhraei et al. 2015; Schlichtkrull et al. 2018a).

The problem of finding potential delinquents is to predict if any user in a multiplex social network, denoted by vertices in graph G, is a normal user or spammer, considering his/her interactions in multiple layers of the network. For this purpose, this chapter aims to investigate each user's behaviour in his/her neighbourhood graph by extracting some features and then mapping all users to a class from [Spammer, Normal] set.

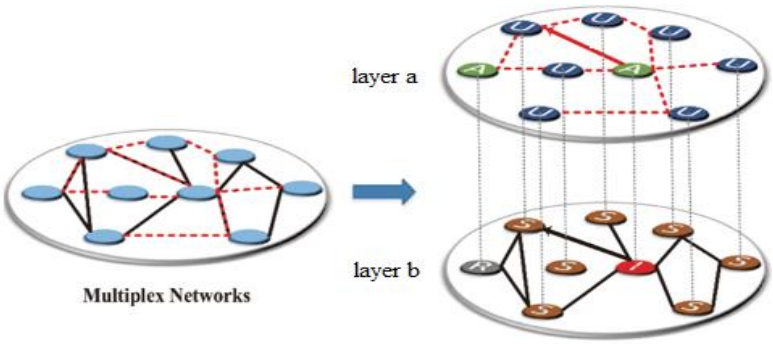

Figure 4.2. Sketch of a multiplex network with two different types of links, each shown in a separate layer, *a* and *b* (Modified from source: (Liu et al. 2016, p. 4)).

4.3 Algorithm Development

The proposed approach to detect spammers in a large time-evolving multiplex social network relied on the interactions of users in the network. As discussed in Section 4.1, drawing on the principles of differential association theory, this chapter defines four sets of easy-to-calculate features to find patterns of intensity, durability and frequency to detect spammers: profile-based features, behaviour-based features, bursty features and sequence-based features. Profile-based features are user demographic information usually obtainable from their registration with a social network. These features look for similar demographic patterns in the connections. The other three feature sets designed to detect any suspicious activities within the intimate personal connections are described below.

4.3.1 Behaviour-Based Features

To extract the behavioural characteristics of users in their interaction network, the proposed algorithm relies on the premise that spammers can usually control their activities to easily evade detection systems (Karim and Zilles 2014). However, it would be much more difficult for spammers to control their neighbours' activities. The quality of the neighbourhood, therefore, is considered as a key factor for the identification of spammers and non-spammers (Karim and Zilles 2014).

For this purpose, the proposed approach relied on the analysis of spammers' behaviour in the popular social media, mainly Twitter, and extracted a set of behaviour-based features to capture the community structure (collusive behaviour) of spammers. These features were inspired by follower–followee and friendship relationships in Twitter to find patterns of frequency and intensity. By mapping the follower–followee pattern, a set of easy-to-calculate behaviour-based features are extracted to find the patterns of frequency within the intimate personal connections as follows:

- Bidirectional link ratio (Bhat and Abulaish 2013; Yang et al. 2013) is the total number of users who are in a bidirectional relation with a user to his total friends:

$$bilink = \frac{N_{bilink}}{N_{friends}} \quad (4\text{-}1)$$

- Average Neighbours' Followers (Yang et al. 2013) is the total number of friends' followers to the total number of friends:

$$Avg_{neig} = \frac{N_{friends\ followers}}{N_{friends}} \quad (4\text{-}2)$$

- Followings to Median Neighbours' Followers (Yang et al. 2011, 2013) is the number of total friends to the median of friends' followers:

$$f = \frac{N_{friends}}{Median(N_{firends\ followers})} \quad (4\text{-}3)$$

- Average activities of friends (Chu et al. 2012) is the total number of friends to the total number of friends' relations:

$$avg_{frnd_{activites}} = \frac{N_{friends\ relations}}{N_{freinds}} \quad (4\text{-}4)$$

- Follower to Following Ratio (FoF) (Chu et al. 2012) is the total number of a user's followers to the total number of his/her friends:

$$fof = \frac{N_{followers}}{N_{friends}} \quad (4\text{-}5)$$

- Total follow in/out ratio (Yang et al. 2011) is the number of total relations made with a user to the total relations a user makes:

$$io = \frac{N_{in-\ relations}}{N_{out-relations}} \quad (4\text{-}6)$$

- Spamicity (Eom et al. 2016; Karim and Zilles 2014) is thus computed as:

$$SP = \frac{1 + N_{out-relations}}{1 + (N_{in-relations} + N_{out-relations})} \quad (4\text{-}7)$$

- Reputation (Wang 2010) is expressed as:

$$Rep = \frac{1 + N_{followers}}{1 + (N_{followers} + N_{friends})} \quad (4\text{-}8)$$

- Average Neighbour Reputation (Karsai et al. 2018) is:

$$avg_{Rep} = Avg(Rep_{friends}) \quad (4\text{-}9)$$

4.3.2 Bursty Features

Bursty behaviour or burstiness is defined as an intermittent increase or decrease in the frequency of events (García-Pérez et al. 2015). Within a social network, an event is defined as a social activity (i.e. any kind of interaction with other users) (Ubaldi et al. 2017). When social interactions happen in the form of a large number of very rapidly occurring interactions in a short period of time, it can be inferred that a burst of events is happening, which may be suspicious (Ubaldi et al. 2017). The following three measures are utilised to capture the burst of users' activities, including their intensity, durability and frequency. Intensity and frequency can be measured using B-measure and median activity rate, whereas median activity time reflects the durability of user activities:

- *B-measure* (Kim and Jo 2016) is calculated as:

$$\mathrm{B} = \frac{\delta - \mu}{\delta + \mu} \quad (4\text{-}10)$$

  where μ denotes the average number of user activities per day, and δ denotes the standard deviation of user activities. $\mathrm{B} \in [-1,1]$ correlates the burstiness, as $\mathrm{B} = 1$ is the most burst signal, $\mathrm{B} = 0$ is neutral, and $\mathrm{B} = -1$ shows a completely regular signal.
- *Median activity* rate (Bhat and Abulaish 2013; Bindu et al. 2018; Yang et al. 2013) measures the median number of users' interactions per day. This measure reflects the speed (i.e. frequency) at which a user interacts with others.
- *Median activity time* is defined as the median of users' inter-time activity (Bhat and Abulaish 2013; Bindu et al. 2018; Yang et al. 2013). This measure

evaluates the duration of interactions a user has with others and how often a user interacts with others.

4.3.3 Sequence-Based Features

In multiplex social networks, spammers are frequently switching between different relation types and sending spamming messages to different users (Jiang et al. 2016). Two different sets of sequence-based features are proposed to capture these patterns of temporal behaviour: relative abundance and distinct neighbourhood ratio.

- *Relative Abundance:*
  Inspired from gene sequence analysis (Kariin and Burge 1995), for each user u_i who is creating a discrete sequence of *n* relations in timestamps T_i ($i = 1,2,\dots,n$), relative abundance ($RA_{ij} \in [0,1]$) is defined as:

$$RA_{ij} = \frac{P_{ij}}{P_i P_j}, (i,j) \in n \qquad (4\text{-}11)$$

  where P_i and P_j denote the frequency of the occurrence of activity i and j, respectively, and P_{ij} denotes the joint probabilities of activity i and j. If one sequence is completely stochastic and the activities are mutually independent, then theoretically, $P_{ij} = P_i P_j$ and the value of RA_{ij} is one. Spammers tend to frequently communicate with random users to find their potential victims (Jiang et al. 2016). Therefore, for spammers, the value of RA_{ij} tends to one ($RA_{ij} \rightarrow 1$). But normal users' activities are not normally stochastic, RA_{ij}, and tend to zero ($RA_{ij} \rightarrow 0$).
- *Distinct Neighbours Ratio:*
  For each user u_i who is sending messages to a discrete sequence of *n* users in timestamps T_i ($i = 1,2,\dots,n$), the distinct neighbours ratio ($DN_{u_i} \in [0,1]$) is defined as:

$$DN_{u_i} = \frac{N_{Ds}}{S} \qquad (4\text{-}12)$$

  where N_{Ds} denotes the number of different users in user u_i's neighbouring sequence, and S denotes the total number of users in this sequence. If the neighbouring sequence of a user is completely stochastic and the users who a user is related to are mutually independent, then theoretically, $N_{Ds} = S$ and the

value of DN_{u_i} is one. Again, for spammers who randomly make connections with other users (Jiang et al. 2016), the value of DN_{u_i} tends to one ($DN_{u_i} \rightarrow 1$). While for normal users who normally communicate with a limited list of users (e.g. their friends), DN_{u_i} tends to zero ($DN_{u_i} \rightarrow 0$).

4.3.4 Proposed Process Framework

To speed up the process of feature extraction, data were collected cumulatively (e.g. in a daily manner and during night runs) to form different layers of the multiplex network. The process of behaviour and bursty feature set extraction is simulated in Microsoft SQLServer 2016. Most of the massive real-world network data are stored in relational data management system databases for easy updating and accessing (Jindal et al. 2015; Liu et al. 2010) (e.g. SQL, Oracle and Vertica). Therefore, implementing these features in SQLServer will be very helpful in the productivity and performance of the proposed approach (Jindal et al. 2015). Then, behaviour-based features (f_{BH}) and bursty features (f_B) were extracted for each layer $l \in L$ separately. The sequence-based features (f_S) were also extracted in parallel with bursty and behaviour-based features using a designed Python engine. User demographic profile features (f_P) were extracted from user profile information. Finally, all features were combined to form a feature vector F:

$$F = [f_{B1}, f_{B2}, \dots, f_{Bl}, f_{BH1}, f_{BH2}, \dots, f_{BHl}, f_S, f_P] \quad (4\text{-}13)$$

Figure 4.3 presents the proposed framework for data storage, feature extraction and classification.

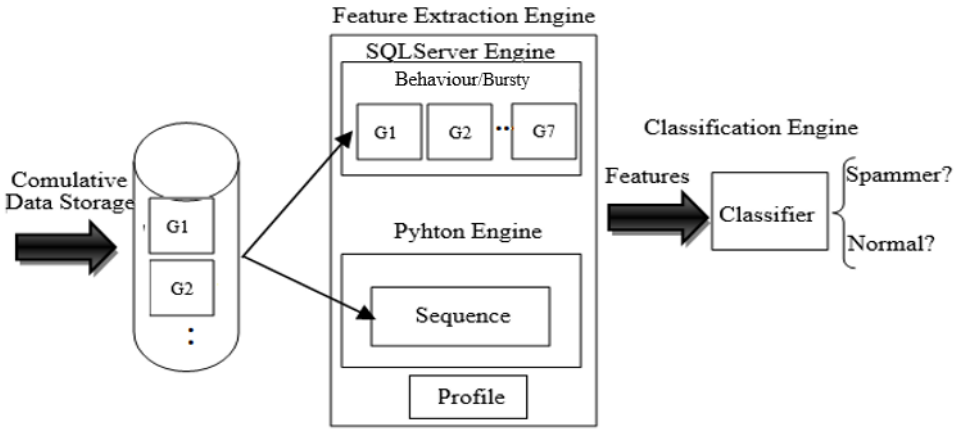

Figure 4.3. Process framework for the proposed approach.

4.4 Knowledge Base

4.4.1 Dataset Description

The experimental data is presented in Table 4.1. This dataset is a labelled data collected from a social networking website called Tagged.com. It is a dating website that connects users through various methods (e.g. mention, like, dislike, wink and poke) to make new connections with other users. The original dataset was first used by Fakhraei et al. (2015) who published their data for research studies. However, due to security concerns, parts of relations from the original data were removed. Besides, the spammer labels have been updated with the release of the published data. The dataset includes over 5.6 million users, of which 336,953 are labelled as spammers. This imbalance distribution of fraudulent users compared with legitimate ones makes the process of classification challenging as common classification algorithms tend to produce more errors when the class distribution is imbalanced (Perera 2013).

Table 4.1. Dataset description

Data Features	Description
Users	Over 5.6 million labelled users 5,270,494 normal users and 336,953 spammers
Relations	858,247,099 relations from 7 different type of relations anonymised to $r_i, i \in [1,7]$

4.4.2 Baseline Methods

This proposed algorithm adopted Fakhraei et al.'s (2015) approach as a baseline. Fakhraei et al. (2015) used a set of graph-based, profile-based and sequence-based features to detect spammers in a multiplex social network. Their graph-based features included PageRank (Page et al. 1999), graph colouring (Jensen and Toft 1994), number of connected components (Skiena 1990), number of triangles (Polak 2016) and k-core centrality measure (Alvarez-Hamelin et al. 2005), in-degrees and out-degrees.

In their sequence-based feature set, Fakhraei et al. (2015) used two different types of features. The first sequence-based feature was called sequential *k*-gram. To calculate this feature, they considered $k = 2$ and calculated the occurrence of any two different relation types in the sequence of users' activities. The second sequence-based feature was defined as a probability of spamicity for each user's activity sequence. This spamicity was extracted using Tree Augmented Naive Bayes (Fei and Geoffrey 2010), relying on the label of the existing data. However, they found that this spamicity did not improve the accuracy of classification. Moreover, this feature relies on the availability of data labels. Nevertheless, the proposed algorithm in this chapter introduces features that do not rely on predefined data labels. Therefore, this spamicity feature is omitted from the sequence-based feature set of the baseline while accomplishing the experiments. The rest of the features, namely, graph-based, profile-

based and sequence k-gram features, are extracted as described in the baseline study by Fakhraei et al. (2015).

4.4.3 Classification Algorithms

To calculate the performance of the extracted features in differentiating normal users from spammers, it is required to apply a classification algorithm on the extracted features. To do so, as suggested by Fakhraei et al. (2015), three different classification algorithms are employed to classify users into Spammers or Normal users: support vector machine (SVM) (Cortes and Vapnik 1995), random forest regression (Liaw and Wiener 2002) and gradient-boosted decision trees (Ye et al. 2009).

SVM (Cortes and Vapnik 1995) is a classification machine learning model for separating the classes in the data domain by constructing the best decision boundaries within the data. Random forest regression (Liaw and Wiener 2002) is an ensemble learning technique that uses a combination of multiple decision trees and a technique called bagging to combine the classification results of multiple decision trees in the determination of the final output rather than just relying on the judgment of individual decision trees. Gradient-boosted decision trees (Ye et al. 2009) classifier is also similar to the random forest regression approach, which is built over a combination of several decision trees. The differences between the two approaches are the way that the decision trees are built and how the classification results are combined.

4.4.4 Experimental Setup

To execute the classification algorithms, a 10-fold cross validation approach is used. For SVM algorithm the maximum number of iterations is set to 10, penalty is set to 1.0 and the convergence threshold is 0.01. For gradient-boosted decision trees, the

number of iterations is set to 10 and for random forest regression algorithm maximum depth is 3 and number of iteration is set 10.

4.5 Results and Discussion

4.5.1 Comparison of Evaluation Metrics

This section will discuss the performance of the proposed approach in terms of feature extraction time, performance and feature importance.

Feature Extraction Time. Regardless of the difference between the type of features in this study and baseline, the implementation of features in relational databases is highly efficient as the features in this study took 2.25 (h) to be extracted. Compared with the baseline features implemented in a graph database and took 5.27 (h) to be extracted in the proposed experimental setup, the proposed approach in this study has a higher productivity. Sequence-based features in both studies also require one pass through the whole relations.

Performance. To calculate the performance of the proposed features in classifying users into two classes [Spammer, Normal], three different classification algorithms are used: SVM (Cortes and Vapnik 1995), random forest regression (Liaw and Wiener 2002) and gradient-boosted decision trees (Ye et al. 2009).

The three different classifiers are employed to classify data using a ten-fold cross-validation method. To validate the performance of the classification algorithms on the different sets of features introduced in this chapter, the average results of the experiments are separately reported according to each distinct feature set as well as a combination of all features (see Figure 4.4(a–c)).

The most appropriate metric for measuring the performance of the classifiers on the proposed features on this highly imbalanced dataset (i.e. the high ratio of fraudulent users compared with the legitimate ones in the dataset) is the PR curve (Saito and

Rehmsmeier 2015). A high precision relates to a low FPR, whereas a high recall relates to a low FN rate. Figure 4.4(a) presents the comparison of the average result of area under precision–recall curve (AUPR) of the three classifiers on different sets of features. Among all three classification algorithms, the gradient-boosted decision trees classifier yields the best results of AUPR when all feature sets are used for classification. This result indicates that gradient-boosted decision trees algorithm leads to better classification results (i.e. low FN and low FPR) when applied to a combination of all features. SVM has a high AUPR when profile-based or sequence-based features were utilised, although it does not perform well when applied to bursty and behaviour-based features. Even when a combination of all features was used for classification, SVM performs worse than the other two classifiers. Random forest regression has a better performance on a combination of all features, although it could not classify data when each set of features were distinctively used.

The other performance metric that indicates how much the features are capable of distinguishing between two classes is the area under the receiver operating characteristic curve (AUROC). A higher AUROC indicates that the classification algorithm can better categorise users using the extracted sets of features (Zou et al. 2007): spammers are classified as spammer, whereas normal users are classified as normal. Figure 4.4(b) also demonstrates that the gradient-boosted decision trees classifier gives a better performance over the other three classification algorithms over each set of features alone as well as the combination of all features.

Accuracy is also a measure that evaluates the closeness of the detected class and true class for each user in the dataset, yet it is a poor measure for imbalanced data (Trajković 2008). As presented in Figure 4.4(c), gradient-boosted decision trees and SVM exhibit higher accuracy values compared with the other feature sets. Although

accuracy is not alone a reliable measure here, referring to the results of AUPR and AUROC, among the three classification algorithms, the gradient-boosted decision trees algorithm is a better classifier in categorising users in the selected dataset using the proposed features.

Therefore, to compare the performance of the proposed features in differentiating users (i.e. normal users from spammers) against the features introduced by the baseline, the gradient-boosted decision trees algorithm is used as the reference classification algorithm. The results of the three performance metrics against the two methods are compared in Figure 4.4(c). The results indicate that the proposed sets of features in this chapter can better differentiate between the two classes of users when compared with the features proposed by the baseline method.

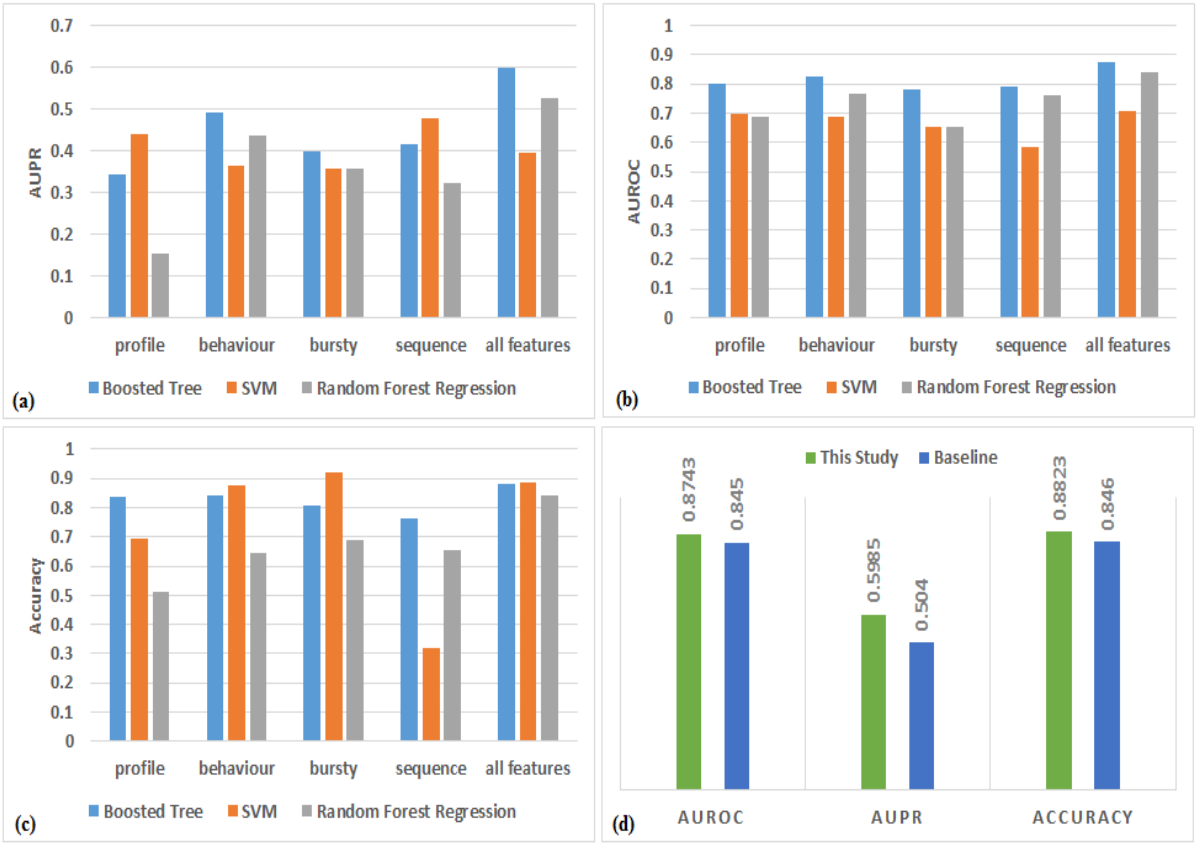

Figure 4.4. (a–c) AUPR, AUROC and accuracy results of the three classifiers using different sets of features proposed in this chapter. (d) Average AUPR, AUROC and accuracy of a combination of all features compared with baseline features using the gradient-boosted decision trees classifier.

Feature Importance. To identify the key features and accumulate the dimensionality, an unsupervised Laplacian score (He et al. 2005) feature selection approach is applied to the full framework of features in this study. The Laplacian score is a feature selection approach that seeks the features in the dataset that best reflect the underlying manifold structure (He et al. 2005). This approach creates a nearest-neighbour graph based on the similarities between each data point in the dataset and its k-nearest neighbours ($k = 10$). Each data point x_i in the dataset is considered a node in this graph, and the weights between the nodes are calculated as:

$$w_{ij} = \begin{cases} e^{\frac{-\left\|x_i - x_j\right\|^2}{t}}, if\ nodes\ i,j\ are\ connected \\ 0 \qquad\qquad , otherwise \end{cases} \tag{4-14}$$

For the r^{th} feature, $f_r = [f_{r1}, f_{r2}, \dots, f_{rn}]$ is the value of feature r in n data samples. The Laplacian score for the r^{th} feature is then calculated as:

$$L_r = \frac{\hat{f}_r^T L\, \hat{f}_r}{\hat{f}_r^T D\, \hat{f}_r} \tag{4-15}$$

$$\hat{f}_r = f_r - \frac{f_r^T D\, \mathbf{1}}{\mathbf{1}^T D\, \mathbf{1}} \tag{4-16}$$

$$\mathbf{1} = [1,1,\dots,1]^T \tag{4-17}$$

$$D = diag(W\mathbf{1}) \tag{4-18}$$

$$L = D - W \tag{4-19}$$

Once the Laplacian values of all the features are calculated, they are sorted in descending order, and features with maximum scores are selected as the final features. Figure 4.5(a) presents the overall Laplacian score value of different feature sets introduced in this chapter. This experiment highlights the importance of different sets introduced in this chapter and helps select the best features to reduce the dimensionality of feature space and training time of the classifiers. As presented in Figure 4.5(a), the proposed sequence-based features have the highest share of

Laplacian score, and bursty features are the second-most important sets of features, whereas the behaviour and profile features are the least important in this data. Figure 4.5(b) presents the comparison of the training time and AUPR for the selected features with different Laplacian score thresholds. The features with a Laplacian score larger than 0.005 have the least possible training time while keeping the near-maximum AUPR.

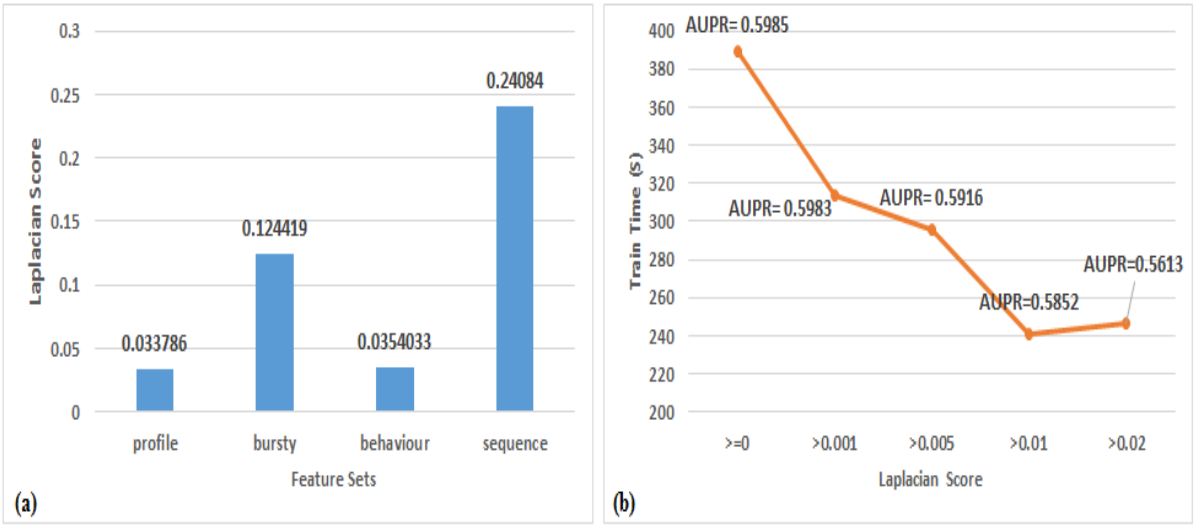

Figure 4.5. (a) Overall average Laplacian score of different feature sets. (b) Overall average AUPR and training time over selected features with various Laplacian score thresholds.

4.6 Chapter Summary

This chapter is devoted to finding spammers and cybercriminals in an online dating social network. Its main concern is to address the first and last proposed sub-research questions: **What set of features can be defined and extracted from a network to capture anomalous activities? (SRQ 1). How can users' anomalous activities be captured in a time-evolving network? (SRQ 3).** It draws on the tenets of criminological theories to investigate the lifecycle of crime on online dating social networks. To identify cybercriminals, this chapter has introduced a feature engineering-based approach to find suspicious activities in a time-evolving multiplex

social network using four sets of features, which the differential association theory postulates as typical of criminal social interaction patterns: patterns of intensity, frequency and durability in the social relationships within the network. The proposed features included a set of profile-based features, a set of lightweight behaviour-based features, a set of bursty features and a set of sequence-based features inspired by gene sequence analysis. The experimental results further indicated that the proposed feature sets had empirically less time complexity while achieving higher AUPR and AUROC as well as Accuracy compared with the baseline approach. The behaviour-based and bursty features can be easily captured in relational databases, which are used in their raw form by many real-world systems.

The drawback of the feature engineering approach is that its dependence on human intervention may create scalability issues in real-world problems. This pitfall is an especially important issue to consider when criminals work together and form a criminal network to reach a 'common good'. In such scenarios, criminals embrace secrecy and actively conceal their networking information by getting engaged in various activities to avoid being detected. Detecting such covert communities is a vital step in dismantling the threat of criminal groups. However, because criminals tend to conceal their activities, the design of features that are able to interpret the implicit signals of suspicious activities would be more complicated and more dependent on the analyst's creativity and expertise. The process is also time-consuming. In some scenarios, the designed features are less able to identify suspicious activities or are not scalable to large-scale network, leading to accuracy and scalability issues. Therefore, the next two chapters are devoted to finding such criminal communities to address the second sub-research question: **How can users' anomalous activities be detected in a network without any manual feature engineering? (SRQ 2).** In

each of the following two chapters, a new method of recently developed GBAD research is introduced to explore the relationships among the criminals and find the co-offending groups among them without any human interventions.

5 Chapter 5—Discovering Covert Communities in Criminal Networks: A Random Walk-Based Approach [a]

Dark networks are covert social networks (Erickson 1981) that are usually incomplete as they are not easily observable (Duijn 2017). Members of these networks would actively conceal their network information by engaging in activities (e.g. friendship, kinship and economic transactions) that distract their true intentions, which prevents them from being discovered by law enforcement agents (Erickson 1981; Warnke 2016). They also hide their impermissible activities by disguising their interactions with people and events (Duijn 2017). As a result, the data on criminals and their networks are typically incomplete with missing links and nodes or contain incorrect information because of criminals' fraud (e.g. fake identity), data entry error or inconsistent information sourced from different legal databases (Hosseinkhani et al. 2012).

Crossley et al. (2012) define a covert network as having individuals who (i) commit illegal acts that are kept secret until the crime has been committed and (ii) seek to remain anonymous afterwards. Given the different types of covert networks, definitions vary (Crossley et al. 2012; Erickson 1981). However, this chapter adopts Crossley et al.'s (2012) definition as it is well aligned with the application problem proposed here, i.e. terrorist networks, where the focus is on individuals and how they conceal their involvement in criminal acts (Broccatelli 2017).

In terrorist networks, individuals are connected *via* different human interactions (Xu and Chen 2004), such as friendship, kinship and economic transactions. These

[a] A journal paper developed based on the information presented in this chapter was published: Pourhabibi, T., Ong, K.-L., Kam, B.H., Boo, Y.L., (2021), 'DarkNetExplorer (DNE): Exploring Dark Multi-layer Networks beyond the Resolution Limit', *Decision Support Systems*, no. 113537.

relationships can be easily captured as a multi-layer network (also known as multiplex network), where all layers share the same users (nodes) but have different edges for each relationship type (Pourhabibi et al. 2019). As a result, multi-layer networks contain rich topological information about individuals and their ties, but their complex structure renders discovering communities difficult (Pourhabibi et al. 2019), especially covert ones in dark multi-layer networks. As mentioned above, this is because these networks are incomplete or contain erroneous data. Therefore, in the case of terrorist networks, they lead to challenges in: (i) identifying key leaders in the network, (ii) understanding influence and relations, (iii) pinpointing vulnerabilities and (iv) disrupting and mitigating harmful activities (Saxena et al. 2018; Troncoso and Weber 2020).

As criminals embrace secrecy and attempt to hide their networking information to evade being identified by law enforcement agencies, detecting covert communities is a vital step in dismantling the threat of criminal groups. This chapter first explores the formation of criminal networks under the premises of criminological theories elaborated in Chapter 3. Using the principles of social disorganisation theory, it then introduces a machine learning approach to investigate how covert communities within multi-layer criminal networks could be detected to address the second proposed sub-research question:

- **SRQ 2. How can users' anomalous activities be detected in a network without any manual feature engineering?**

The following sections describe the proposed approach in the context of Hevner et al.'s (2004) IS framework (see Figure 1.1 in Section 1.31.4).

5.1 Background Theories: Crime Analysis

This section explores the organisation of criminal networks from the perspective of criminological theories. It explains *why* people engage in collusive criminal activities

and form criminal networks? *What* are the required conditions for the establishment and growth of such networks? *Where and when* do criminal networks form? *How* to detect the collusive structures within criminal networks?

***Why*.** Criminals seek similar co-offenders to engage in collusive activities to reach a common goal (e.g. terrorist attack, arm and drug trafficking) (Papachristos 2013). As claimed by *rational choice theory* (Cornish and Clarke 2014), there is a rationality for the formation of co-offending groups, such as street gangs (Grund and Densley 2012; McGloin 2005; Papachristos 2009; Sierra-Arévalo and Papachristos 2015), secret societies (Erickson 1981), illegal drug market (Berlusconi et al. 2017; Malm and Bichler 2011; Morselli et al. 2017; Natarajan 2006) and terrorist groups (Krebs 2002).

Terrorists, for example, are instrumentally rational and politically motivated (van Um 2011). They attempt to maximise their expected political utility (e.g. independent state, financial gain, religious reward, regime change or social revolution) regarding specific political grievances (Davis and Cragin 2009; Nemeth 2017; van Um 2011). Street gangs and drug traffickers are also rational beings: they attempt to maximise the utility of alternative actions by growing a criminal network. These utilities include collecting private information about their partner's intentions and abilities (van Um 2011), access to illegal goods' suppliers and or clients, such as drugs or gun, and illegal services, such as sex (Masucci 2013).

Accordingly, considering the rationality and benefits behind the formation and growth of criminal networks, there is often very poor guardianship by local security forces, making the risk and cost of criminals getting caught low (Masucci 2013). Moreover, if actors involved in a criminal network were to be discovered, there would be a substantial risk for other members. Therefore, secrecy plays a significant role in covert networks, and network members attempt to maintain weak ties as much as

possible (Burt 2005). Keeping weak ties within the network forms a disorganised, sparse, unstable and heterogeneous network (Burt 2005), which amplifies the lack of regulation or monitoring by law enforcement agencies. Therefore, as stated by rational choice theory (Monk et al. 2018), criminal insurgencies take root and evolve gradually within such ungoverned space (Masucci 2013).

What. Drawing onto Cohen and Felson's (1979) routine activity theory, the convergence of three elements in time and space can have an influence on crime rate: motivated offenders, suitable targets and absence of capable guardians against a violent behaviour.

Within criminal networks, the capable offenders are the 'active' criminals who are looking to host negative social, behavioural and cognitive outcomes (Peterson et al. 2004), i.e. terrorists in a terrorist network and traffickers in a drug trafficking network. The guardians may be the ordinary citizens (Cohen and Felson (1979), police, military or counter-terrorism forces (Bigot 2017; Masucci 2013). Finally, the targets are the criminal counterparts who are selected from the same *awareness* or *activity space*, which is of the same ethnic background, friendship or kinship groups, studied in the same school, worked in the same organisation or served their sentence in the same prisons (Blau 1977). This selection mechanism results in opportunities for offenders to associate with like-minded individuals and connect and develop strong ties and high degrees of trust, thereby forming a network of criminals for committing deviant behaviours (Blau 1977).

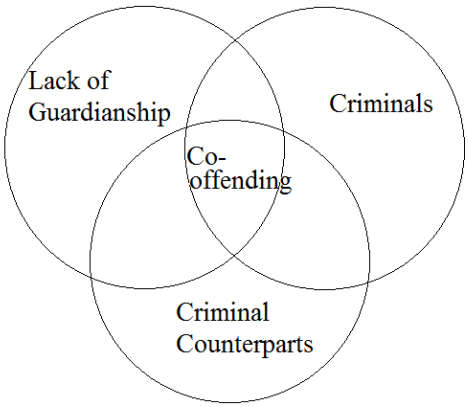

Figure 5.1 Routine activity theory: Three factors for criminal network formation.

***Where and When*.** Environmental criminologists believe that there are patterns of crime and patterns within co-offending that would ultimately help law enforcement agencies to better predict, analyse and control the offenders, as and where the crime occurs (Bright et al. 2020). Criminals do not commit crime alone. They choose their co-offenders from a pool of people whom they already know through their routine activities (Cohen and Felson 1979), such as from a network of friends, family and acquaintances who influence their co-offending behaviour, decision-making and exposure to criminal opportunities (Bichler and Malm 2019). While offenders try to reach their network of familiar people within their awareness space in the co-offending selection procedure, they shape their linkage and relationship patterns.

To examine the co-offending pattern within a criminal network from the perspective of crime pattern theory (Brantingham and Brantingham 1993), the focus would be on the population of the offenders who co-offend, their frequency of co-offending and persistent relation with specific offenders (Pourheidari and Croisdale 2010).

How. *Social disorganisation theory* (Shaw and McKay 1942) proposes that the lack of governance on criminal networks increases the opportunity for criminals to recruit individuals to commit crime (Monk et al. 2018). As noted by Burt (2005), criminal networks have a disorganised structure that hinders focused monitoring by law

enforcement agencies. Engaging in deviant behaviour, however, may lead to the formation of cohesive social ties within the network (Waring and Weisburd 2000), which can be readily detected by searching linkage patterns within the network (Carrington 2011). This characteristic helps detect covert communities within criminal networks, which would enable law enforcement agencies to take appropriate actions to disrupt criminal organisations or select important targets for policing and interventions (Monk et al. 2018).

Accordingly, to find the important targets for policing, this chapter introduces a machine learning algorithm to find portions of the criminal networks with higher densities of social ties.

5.2 Problem Formulation

The main focus of this chapter is to introduce a machine learning approach to identify criminal clusters within a dark multi-layer network. Jeub et al. (2017) argue that one way to discover the topological and dynamic properties of multi-layer networks, including covert communities, is to study the behaviour of a discrete-time random walk on the network. This is because a random walker that jumps from one node to another gets ‘trapped’ in denser regions of the network for longer periods, thus exposing anomalies and allowing the discovery of covert communities (Jeub et al. 2017; Kuncheva and Montana 2015). This explanation resembles the principles of social disorganisation theory (Shaw and McKay 1942): engagement in deviant activities may lead to cohesive social ties within the network (Waring and Weisburd 2000), which can be detected by an in-depth analysis of relational patterns within the network (Carrington 2011).

This chapter takes advantage of this behaviour to explore (or 'walk' through) the network both within and between layers based on some pre-set transition probabilities (Kuncheva and Montana 2015), an approach called a 'multiplex random walk'. The proposed approach aims to find clusters with nodes that mostly reside in the network hubs, which are known to play a key 'brokerage' role in (i) the flow of information and resources throughout the dark networks or in (ii) mediating between unconnected actors (Cunningham et al. 2013). According to Sageman (2004), these nodes in the hubs are where the leaders are usually located. If these nodes or hubs are disrupted, criminal activities are effectively dismantled.

The proposed algorithm uses an adaptive centrality choice parameter to guide the random walker in a layer to move to the next neighbours based on their hub centrality score. To effectively operate on a large network, the proposed algorithm allows multiple independent parallel walks to speed up the expected time required to visit every node (at least once) in a graph (Alon et al. 2008). Because the goal of this algorithm is to find the 'small' and "good' communities that reflect the characteristics of a terrorist network, a community detection model is also designed using the Jaccard correlation of walked sequences between each pair of nodes to maximise a resolution-limit-free optimisation function. This function will enable the proposed approach to identify the 'small' and 'good' communities, thus allowing a list of suspects to be extracted for law enforcement agencies to start their investigation in a more targeted manner (Magalingam et al. 2015).

Currently, most state-of-the-art research studies focus on partitioning networks by optimising a modularity-based optimisation function (Cherifi et al. 2019; Traag et al. 2015). However, modularity fails to identify community structures below a certain characteristic scale (i.e. a resolution limit (Xiang et al. 2019)), and therefore, the 'small'

communities (relative to the network) slip through the detection process. In short, modularity-based methods yield dense sub-networks that are difficult and time-consuming to analyse and miss the 'small' and 'good' communities of interest to law enforcement agencies (Fortunato and Barthelemy 2007). To overcome these limits, a statistical measure called AS is introduced. AS is a fitness function that can (i) outperform modularity-based methods (thus finding smaller communities) and also (ii) find lower-density communities (Traag et al. 2015).

5.3 Algorithm Development

This section begins with a brief description of multi-layer networks and the random walk algorithms before presenting the details of the proposed approach.

5.3.1 Multi-layer Network Model

Let graph G denote a multi-layer network, where $G = \bigcup_{i=1}^{L} G_i$, and $L \in R^+$ indicates different types of relationships in the network, and $G_i = (V, E_i, L_i)$ is a sub-graph of G. For each sub-graph G_i, E_i denotes a list of relations of type L_i between each pair of vertices from a vertex set V, which is common among all layers (Interdonato et al. 2017; Pourhabibi et al. 2019). For each G_i, the connectivity structure of a multi-layer network, including both intra-layer and inter-layer edges, can be encoded using an adjacency tensor A as follows (Jeub et al. 2017):

$$A_{i_\alpha}^{j_\beta} = \begin{cases} w, & (i_\alpha, j_\beta) \epsilon\ E \\ 0, & otherwise. \end{cases} \quad (5\text{-}1)$$

where $i_\alpha \in V$ denotes node $i \in V$ in layer $\alpha \in L$, and (i_α, j_β) denotes an edge from node i_α to node j_β with weight $w \in R^+$.

5.3.2 Preliminaries on Random Walks on Multi-layer Network

A random walker in a multi-layer network forms a Markov system by randomly selecting a sequence of vertices (Solé-Ribalta et al. 2016). Generally, a random walker

on a multi-layer network can exploit all the connections leaving the current node across all layers (Figure 5.2).

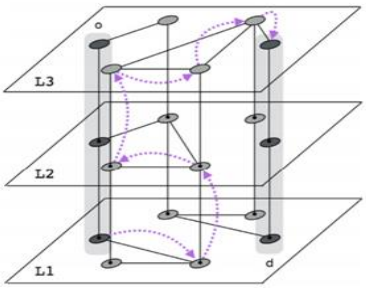

Figure 5.2. Schematic of a walk (dotted trajectories) in a multi-layer network (Source: (Solé-Ribalta et al. 2016, p. 75)).

Following Jeub et al. (2017), a discrete-time random walk on a multi-layer network can be written as:

$$p_{i\alpha}(t+1) = \sum_{j\beta \epsilon V} P_{i\alpha}^{j\beta} p_{j\beta}(t) \tag{5-2}$$

where $p_{j\beta}(t)$ denotes the probability for a random walker to be at node j in layer β at time t, and $P_{i\alpha}^{j\beta}$ denotes the probability for a random walker at node j in layer β to transfer to node i in layer α in one time step. The transition transfer P encodes both the intra-layer and inter-layer behaviours of a random walk. Classical random walk is the most direct way to generalise the concept of a random walk in a multi-layer network. This kind of random walk treats inter-layer and intra-layer edges as equivalent objects and is defined by the following transition probability, which denotes a biasing function:

$$P_{i\alpha}^{j\beta} = \frac{A_{i\alpha}^{j\beta}}{\sum_{j\beta \epsilon V} A_{i\alpha}^{j\beta}} \tag{5-3}$$

5.3.3 Proposed Approach

Figure 5.3 presents the overall structure of the proposed algorithm, called the DarkNetExplorer (DNE), which comprises four stages. In Stage 1, multiple walkers begin random choice-based walks at each node of length l. For each node, sequences

of walks are integrated in Stage 2, and nodes that do not appear sufficiently often (e.g. less than a predefined threshold) in the integrated walk sequence are removed to prevent accidental moves to other communities. Then, in Stage 3, the Jaccard correlations (Satuluri et al. 2011) between each pair of nodes are calculated using *minwise* hashing. Finally, in Stage 4, agglomerative clustering is applied based on Jaccard similarities. An optimisation function is employed to maximise the AS (Nicolini et al. 2017) of the detected clusters to obtain the best partitions. This function helps prevent very dense and large clusters and overcome the resolution limit of the modularity-based approaches.

The implementation of DNE is presented in Algorithm 5.1 and is discussed in the following subsections.

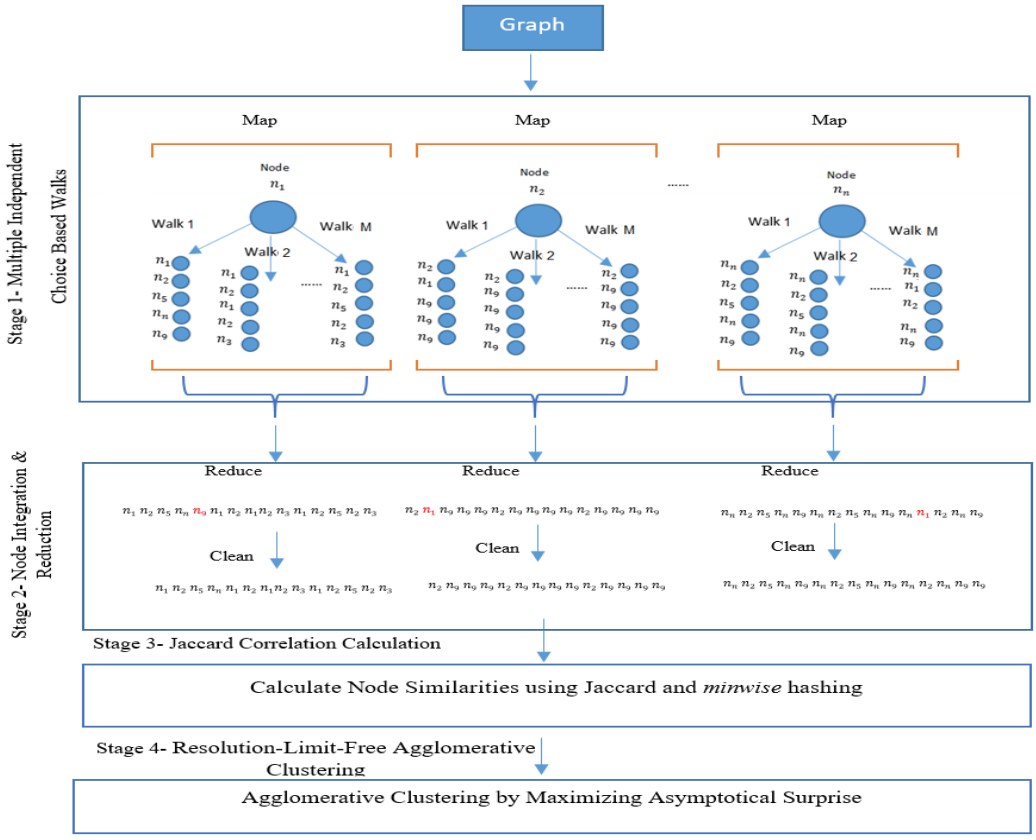

Figure 5.3. Structure of DarkNetExplorer (DNE).

Algorithm 5.1. $DarkNetExplorer\ (DNE)$

Input: $A_{i_\alpha}^{j_\beta}$: multi-layer graph, W: no. of walks, l: walk length, $Walkers$: no. of walkers
Output: $Clusters$

$nodes \leftarrow Size(A)$
Class Mapper
  method MAP ($start\_node$ n, $Walker\ walker$)
    $w \leftarrow 1$
      While $w < W$ *do*
      $seq \leftarrow \emptyset$
      $Curr \leftarrow n$
      While $len(seq) < l$ do
        calculate the probability $P_{i\alpha}^{j\beta}$ using Eq. 5-4 for $Curr$ node
        $v \leftarrow$ move $walker$ to the next node with maximum $P_{i\alpha}^{j\beta}$
          $seq[w] \leftarrow seq[w] \cup v$
        $Curr \leftarrow v$
      $w \leftarrow w+1$
  Return seq
Class Reducer
  method Reduce ($node\ n, sequence\ seq$)
    $final_{seq}[n] \leftarrow \emptyset$
    For s in seq do
      $final_{seq}[n] \leftarrow final_{seq}[n] \cup s$
      $\partial \leftarrow int(0.1 * len(final_{seq}[n]))$
    $final_{seq}[n] \leftarrow$ remove nodes from $final_{seq}[n]$ with a count of less than ∂
  Return $final_{seq}$

Class Main()
  $nodes = shuffle(nodes)$
  While $ExistsNodeToWalkOn()$ do
    For $walker$ in $Walkers$ do
      MAP $(n, walker)$
      Reduce (n, seq)

  $Sim \leftarrow$Calculate $Jaccard$ similarities for all pairs of nodes referring to (Satuluri et al. 2011)
  Sim=$Sort(Sim, desc)$
  $S_a = -Inf$
  $Clusters = [n\ for\ n\ in\ nodes]$
  While Sim do
    $Clusters_{new}$=Combine $Clusters$ using agglomerative clustering and Sim matrix
    S_{a_new}= Calculate AS of $Clusters_{new}$ using Eq. 5-6
    IF $S_{a\_new} >= S_a$
      Remove from Sim the combined nodes value
      $Clusters = Clusters_{new}$
      $S_a = S_{a\_new}$
      Go to **34**
    ELSE:
      Remove from Sim the last uncombined nodes
      Go to **34**
  Return $Clusters$

5.3.3.1 Choice-Based Walks

To ensure that a random walker visits each node of a network (or the vertex of a graph) at least once, a stream of short random walks is introduced to extract information from the network. This approach has two advantages (Perozzi et al. 2014). First, several random walkers can simultaneously explore different parts of a network, allowing for a MapReduce parallel setup, as presented in Figure 5.3. This feature is essential on large networks, since k parallel random walks reduce the cover time of a graph by $\Omega(k)$ times compared with a single walk (Alon et al. 2008). The second advantage is that small changes in the structure of a graph can be quickly picked up with short random walks, leading to a shorter runtime performance (Alon et al. 2008). Thus, the proposed approach generates k walkers to start independent biased random walks of length l in parallel.

Covert networks contain a high level of secrecy in their functions and operations. Thus, connections among the members of interest are sparse, i.e. the average node degree is low, the average degree of separation is high, and very few actors play the 'brokerage' role (Memon 2012). Therefore, a random walker can choose (hence, choice-based walk) to move towards the key actors and form clusters around them. This feature helps destabilise the network by isolating or eliminating potential criminals.

According to Sageman (2004), the discovery of hubs (nodes pointing to many critical nodes or nodes with a brokerage role) is useful for intelligence collection and law enforcement disruption efforts. By destroying the hubs, law enforcement agencies can break the dark network down into isolated nodes, thus incapacitating criminals from mounting sophisticated or large-scale operations (Everton 2008). By extension,

terrorist leaders are more likely hidden in hubs, which should be the focus to achieve the effect stated (Roberts and Everton 2016).

To reflect Sageman's (2004) heuristics, the transition probability of a random walker in a multi-layer network (Eq. 5-3) is transformed to Eq. 5-4 to guide the random walkers to move towards the nodes with higher hubs (h) (see Algorithm 5.1, lines 8–11), as shown below:

$$P_{i_\alpha}^{j_\beta} = \frac{A_{i_\alpha}^{j_\beta}}{\sum_{j_\beta \in V} A_{i_\alpha}^{j_\beta}} * h_j \qquad (5\text{-}4)$$

where h_j denotes the normalised hub score of node j (for calculating hub scores, refer to (Mirzal and Furukawa 2010)). Eq. 5-4 suggests that the higher the hub score of a neighbouring node (h_j), the more likely a random walker moves towards node j.

5.3.3.2 Node Integration and Reduction

When random walkers finish walking through the network, the histories of all walked sequences for a particular node i are combined into one unified sequence (Algorithm 5.1, line 19). Nodes with a minimum occurrence threshold in a walked sequence are then eliminated in the Reduce function (Algorithm 5.1, lines 20–21). This feature accounts for the probability of a walker starting in a specific community and ending up moving into another community by 'accident'. In this case, the number of visited nodes that may belong to other communities may be far less than the rest of the nodes in a unified sequence. These sets of nodes are considered as noise in the observed sequence and can thus be eliminated.

5.3.3.3 Jaccard Correlation Calculation

Similarities between nodes are estimated and sorted in a descending order based on the Jaccard correlation (Satuluri et al. 2011) between each pair of connected nodes

using their histories of walked sequences (Algorithm 5.1, line 30–31). The similarity is approximated by hashing *via minwise* hashing (Satuluri et al. 2011), which reduces the time complexity for the calculation of the similarity between all pairs of nodes in the graph from $O(n^2)$ to a linear time of $O(n)$, where n denotes the number of nodes in the graph (Satuluri et al. 2011).

5.3.3.4 Resolution-Limit-Free Agglomerative Clustering

Finally, an agglomerative cluster analysis (Sibson 1973) is employed to form the clusters based on similarities. As mentioned, the main focus of the proposed approach is to find 'good' and 'small' structural communities so that law enforcement agencies can easily identify a list of suspects to start an investigation (Magalingam et al. 2015). This objective sets the proposed approach apart from existing modularity-based optimisation techniques, which results in dense sub-networks that are difficult to analyse (Fortunato and Barthelemy 2007). To achieve the proposed objective, this chapter introduces the AS in the agglomerative clustering in place of the modularity measure.

5.3.3.4.1 Asymptotic Surprise

The discovery of an optimal cluster arrangement $\boldsymbol{C} = [c_1, c_2, \dots, c_N]$, where $c_i \cap c_j = \emptyset$ and $\bigcup_{i=1}^{N} c_i = V$, can be cast as an optimisation problem (Ser et al. 2016). As a quality measure rooted in probability theory, Surprise assumes a null model that links nodes in a graph uniformly drawn at random with n nodes. It evaluates the departure of the observed partition from the expected distribution of nodes and links into communities given the null model. For binary networks, Surprise can be computed using a cumulative hypergeometric distribution (Aldecoa and Marín 2014):

$$S(\boldsymbol{C}) = -log \sum_{j=m_\varepsilon}^{min(M,m)} \frac{\binom{M}{j}\binom{F-M}{m-j}}{\binom{F}{m}} \quad (5\text{-}5)$$

where F denotes the maximum possible number of links in the network; m, the actual number of links within the network; M, the maximum possible number of intra-community links; and m_ε, the actual number of links within communities.

Eq. 5-5 is difficult to compute, especially in the case of large networks (Traag et al. 2015). Hence, Surprise can be approximated by a binomial distribution, leading to Eq. 5-6 called AS. This expanded version of Surprise assumes that when the graph grows, the relative number of internal edges and the related number of expected internal edges remain fixed (Traag et al. 2015). In information theory, AS represents the Kullback–Leibler (KL) (Eq. 5-7) divergence between the observed (q) and expected fraction (<q>) of intra-cluster edges. KL is a quasi-distance on probability distributions as it is always non-negative, non-symmetric and zero only when $q =< q >$, like binary Surprise (Nicolini et al. 2017):

$$S_a(\mathbf{C}) = mD_{KL}(q||< q >) \quad (5\text{-}6)$$

$$D_{KL}(x||y) = xlog\left(\frac{x}{y}\right) + (1-x)log(\frac{1-x}{1-y}) \quad (5\text{-}7)$$

The formulation of AS is extended to a weighted directed version while keeping the same formulation in Eq. 5-6 and Eq. 5-7 (see Table 5.1) (Traag et al. 2015). A uniform distribution of weights across the graph in the random graph is assumed, and the expected weights are calculated as $< w >$. The total possible internal weight is then $< w > * M$, whereas the total possible weight is $< w > * F$. Hence, $< q >$ remains unchanged (Traag et al. 2015).

5.3.3.4.2 Hierarchical Clustering by Maximising AS

The proposed approach uses a single-linkage agglomerative clustering (Sibson 1973) to merge communities, which, in the worst case, has a time complexity of $O(n^2)$.

While merging communities, the AS optimisation function is adopted to choose the best partitions. Two nominated communities are merged if the resulting combined community increases the AS value. The algorithm starts by assigning each node to its community (Algorithm 5.1, line 33). Then, it iteratively merges nodes based on the calculated Jaccard similarities to determine the optimal clustering $\boldsymbol{C}^*$over the whole L-layer network (Algorithm 5.1, lines 34–45):

$$\boldsymbol{C}^* = \underset{c \in c^{\Delta}}{\operatorname{argmax}} \sum_{i=1}^{L} S_a(G_i, \boldsymbol{C}) \tag{5-8}$$

where c^{Δ} denotes the set of all possible partitions.

Table 5.1. Variable definition

Variable	Unweighted & undirected	Weighted & directed	Description
F	$\binom{n}{2}$	$\frac{\binom{n}{2}}{2}$	Maximum possible number of links in a graph
M	$\sum_{c \in \boldsymbol{C}} \binom{n_c}{2}$	$\sum_{c \in \boldsymbol{C}} \frac{\binom{n_c}{2}}{2}$	Total possible intra-community edges, where $\boldsymbol{C}$ denotes the list of identified clusters, and n_c denotes the number of nodes in a specific cluster $\boldsymbol{c}$
m	$\sum_{i,j} A_{ij}$	$\sum_{i,j} w_{ij}$	Total edges (if the graph is weighted, it indicates total internal weights)
m_{ε}	$\sum_{i,j \epsilon n_c} A_{ij}$	$\sum_{i,j \epsilon n_c} w_{ij}$	Total internal weights/edges of a cluster
q	$\frac{m_{\varepsilon}}{m}$	_____	Observed fraction of internal edges
$< q >$	$\frac{M}{F}$	_____	Expected fraction of internal edges

5.4 Knowledge Base

5.4.1 Dataset Description

This chapter uses three criminal networks–the Noordin Top Terrorist network, Boko Haram network and Caviar network–to evaluate the performance of the proposed approach. The structural characteristics of these networks are presented in Table 5.2.

Table 5.2. Network structural and interconnectedness features

Dataset	No. of Nodes	No. of Links	No. of Layers	Network Features	Network Density	Network Average Degree	No. of Louvain Clusters	No. of InfoMap Clusters
Noordin Top network	78	1014	4	Undirected, unweighted	0.337	26	5	6
Caviar network	107	651	11	Directed, weighted	0.057	6.08	8	9
Boko Haram network	44	82	3	Undirected, weighted	0.08	3.72	9	11

5.4.1.1 Noordin Top Terrorist Network

The Noordin Top Terrorist network is drawn from a terrorist network operating in Indonesia. Noordin Mohammad Top, from the Jemaah Islamiyah (JI) organisation, acted as a coordinator to reach out to young men from other jihadist organisations and some with no previous organisational affiliation. The actors in this terrorist network were responsible for various terrorist activities, including the Marriott Hotel bombing in Jakarta in August 2003, Australian embassy bombing in September 2004, Bali bombing I in October 2002 and Bali Bombing II in October 2005 (International Crisis Group 2006).

The ties or links between actors represent one or more common affiliations or relationships. The network includes 78 actors (criminals) attending 45 different events, which are categorised into four to form a four-layer network: trust, operational, communication and business ties. The ties in each category are undirected and considered as a separate layer of the network. The trust layer is generated by the superposition of classmate, friendship, kinship and soul mate ties, whereas the operational layer is produced from four sub-layers: logistics, meetings, operations and trainings (Roberts and Everton 2011).

5.4.1.2 Boko Haram Network

The Boko Haram Terrorist network contains the relationship information of 44 terrorists belonging to an Islamic sect that has been operating primarily in Northern Nigeria since 2002. The group believes that the current Nigerian government is corrupted by false Muslims (Walker 2012). This network is remarkably sparse owing to its relatively young cell-like structure and the lack of collective leadership. Cunningham (2016) created this network using a variety of open-source documents. The available undirected ties are re-organised into edges to build a three-layer network: trust, communication and knowledge sharing. The trust layer includes colleagues, kinship, superior and supporter. The communication layer is formed by the superimposition of financial ties, communication and membership, and the knowledge-sharing layer is built from shared events and collaboration (Gera et al. 2017).

5.4.1.3 Caviar Network

The Caviar dataset was created by Morselli (Morselli 2009) based on an investigation that targeted a hashish and cocaine network operating from Montreal between 1994 and 1996. The principal data source is the information submitted as evidence during the trials of 22 participants in the Caviar network in a series of hashish and cocaine distribution chains. It included 4,279 paragraphs of information (over 1,000 pages) revealing electronically intercepted telephone conversations between network participants. The transcripts were utilised to create the overall matrix of the drug-trafficking operation's communication system throughout the course of the investigation. The ties are a person-to-person relation of 110 participants related to 11 different phases of the project drawn from information provided by law enforcement agencies (Morselli 2009). To hide the identity of individuals monitored during the

different phases of the project, these individuals are designated as nodes (e.g. Node 1,…, Node 110) (Hmimida and Kanawati 2015). For the experiments in this chapter, the directed ties of each phase are considered as a separate layer in this dark network to form an 11-layer multiplex network.

5.4.2 Baseline Methods

To determine the effectiveness of the proposed algorithm, its performance is compared against two well-known community detection algorithms, which have been employed to detect covert communities. The first is the 'multi-slice modularity'-based Louvain[1] method (Liu et al. 2018), and the other is the multiplex InfoMap[2] (De Domenico et al. 2015), where both methods attempt to find communities using all the structural information across the layers of the multiplex network (Liu et al. 2018). It is noted that there are only two comparable techniques, as the other techniques operate on monoplex networks.

The Louvain method is a widely used modularity-based community detection algorithm (Bahulkar et al. 2018). It uses a bottom-up approach in the identification of communities by optimising the local modularity of communities. The drawback of the Louvain method is that the identified communities can be unstable, resulting from local modularity optimisation. This instability is further exacerbated by the limited connectivity between communities in a criminal network (Bahulkar et al. 2018). Like other modularity-based community detection approaches, the Louvain method suffers from a resolution limit that prevents it from detecting the small clusters (Fortunato and Barthelemy 2007) required in the use-case of terrorist network analysis.

[1] Multiplex Louvain (https://louvain-igraph.readthedocs.io/en/latest/multiplex.html)
[2] Multiplex InfoMap (http://www.mapequation.org/code.html).

From the benchmark by Lancichinetti et al. (Lancichinetti and Fortunato 2009), InfoMap is the best-performing community detection algorithm for large monoplex networks. The InfoMap clustering method identifies communities according to the flow of information in the network structure. Like the proposed approach, InfoMap uses a random walk-based approach to reveal the hierarchical structure of large networks as it agglomerates clusters into supernodes. As a result, InfoMap does not suffer from the resolution limit problem of modularity maximisation approaches like Louvain. This feature makes it a better candidate for finding small communities. With these two baseline methods explained, this chapter now turns to the discussion of the evaluation of the proposed algorithm against Louvain and InfoMap using three real-world multiplex dark network datasets.

5.4.3 Experimental Setup

To evaluate the baseline methods against these datasets, their default parameter settings are used. With the proposed algorithm, 40 random walkers are utilised to sample sequences of length $l = 5$ from the neighbouring nodes of each node $W = 10$ times.

5.5 Results and Discussion

5.5.1 Cluster Analysis on the Noordin Top Network

The Noordin Top dataset is drawn from a terrorist network operating in Indonesia. Noordin Mohammad Top from the JI organisation acted as a coordinator to reach out to young men from a variety of backgrounds. The actors were responsible for various terrorist activities, including the Marriott Hotel bombing in Jakarta in August 2003, the Australian embassy bombing in September 2004 and the Bali bombings in October 2002 and 2005 (International Crisis Group 2006).

The ties between actors represent one or more common affiliations or relationships. The network includes 78 actors (criminals) attending 45 different events, which are categorised into four to form a four-layer network: trust, operational, communication and business ties. The ties in each category/layer are undirected. The trust layer is generated by the superposition of relationships, such as classmates, friendship, kinship and soul mates. Meanwhile, the operational layer is produced from four sub-layers: logistics, meetings, operations and trainings (Roberts and Everton 2011).

Figure 5.4(a–c) presents the results of running Louvain, InfoMap and DNE on the Noordin network. Compared with Louvain (five communities, S_a=127.835), in Figure 5.4(a), and InfoMap (six communities, S_a = 203.922), in Figure 5.4(b), as shown in Figure 5.4(c), the proposed algorithm produced seven different non-singleton communities (i.e. communities with more than two participants). Here, it can be seen that the proposed algorithm yields better 'good' communities compared with InfoMap and Louvain, i.e. the clusters are lower in density as reflected by a higher AS (S_a=242.683). Beyond what the AS measure suggests, the quality of the communities discovered by the different algorithms is confirmed by looking into the dataset. According to the (International Crisis Group 2006), there are seven different groups to which the actors in the network can belong. Each group provides us with some ground truth that can be utilised to check how well each algorithm performs, which are described below.

Developing Darul Islam (DI). The result of cluster *C1* is identical in InfoMap and DNE, whereas Louvain was not able to detect this cluster. Both InfoMap and DNE picked up the relation among Node 1, Node 9 and Node 16. Having this relation in the output is important as it is noted from the ground truth that Node 16 was the younger

brother of Node 1. He was involved in training DI, the Islamic group that fought for the establishment of an Islamic state in Indonesia, whereas his older brother was involved in sending DI recruits to the Philippines.

Bali Bomb II. In this group, the small cluster *C2* detected by InfoMap and DNE revealed some interesting information. Nodes 18 and 64 in *C2* both trained together as suicide bombers in Bali Bomb II in 2005, whereas Node 69 was suspected of making a video of the suicide bombers' last testaments and went on to become Noordin's courier and coordinator (International Crisis Group 2006). With regard to the previous category, Louvain did not pick up this small cluster, and while InfoMap and DNE both did, the proposed algorithm performed better. In the case of InfoMap, it included Node 50 in this cluster, whereas the proposed algorithm, DNE, did not. Against the ground truth, Node 50 was killed in the first Bali bombing in October 2002; thus, it should not appear as an actor in this category (Bali Bomb II in October 2005).

JI Group and Marriott Bombing. Cluster *C3* includes two principal leaders and planners of the Noordin network, namely, Node 59 and Node 23. Most of the actors in *C3* are from the same organisation, namely, JI, a transnational Southeast Asian militant Islamist terrorist organisation linked to Al-Qaeda mainly responsible for either educating suicide bombers or engaging in the bombing in Marriott. Again, the outputs of InfoMap and DNE for *C3* are highly similar, except that DNE is better at excluding the less critical or singleton communities, leading to a lower-density *C3* that is better for interpretability. These exclusions make sense when they are matched with the ground truth information. For example, the DNE algorithm excluded Node 15, the leader of DI, from *C3*, which InfoMap did not. Given the DI affiliation, it is noted that this node should not be in *C3*. This result indicates that DNE is better than InfoMap at

categorising members based on their specific characteristics and communication patterns.

Hiding Noordin (Jan 2005). In cluster *C4*, the proposed algorithm produced a similar community structure as InfoMap with both accurately including all those involved in finding a hiding place for Noordin in January 2005. Conversely, Louvain miscategorised four members (Nodes 3, 5, 6 and 31) into this community (marked as *C1* in Louvain's output) when they should be in *C3*.

JI Group. Members of cluster *C5* are from the JI group. Except for non-critical members (Nodes 14, 49, 57 and 79) categorised as singletons in DNE, the proposed algorithm and InfoMap yielded identical results. With Louvain, members from other communities were found here, leading to a dense cluster (e.g. Nodes 1, 9 and 16 from *C1*; Nodes 35 and 42 from *C7*; and Node 28 from *C4*).

Disposal of Bali Bombings Leftovers. Nodes 62 and 32 in cluster *C6* (Figure 5.4(c)) were two influential members of the Ring Banten group. They were responsible for finding a safe house for the two leaders of the Noordin Top network (Nodes 59 and 23) and helped dispose of the leftover explosives from the Bali bombings. Both Louvain and InfoMap were not able to identify this cluster.

Embassy Bombing in 2004. Cluster *C7* in Figure 5.4(c) includes the actors involved in the Australian embassy bombing in September 2004. Node 45 was the field commander, and Node 66 was Node 45's uncle who was the military instructor for the suicide bombers. Other members of this cluster, including Nodes 68, 73, 77, 74, 24 and 43, were also trainers to the suicide bombers. Node 35 helped with the recruitment, Node 38 studied bombing with Node 23, and together, they helped assemble the bomb. The ground truth also confirmed that Node 41 was involved in

getting the detonating cord used in the bombing. Nodes 10, 12, 19, 25 and 37 were also found to be suicide bombers in this event. It can be noted that *C7* in DNE is identical to *C6* in InfoMap, as presented in Figure 5.4(b); however, the proposed algorithm was able to exclude Node 11, who was killed in Bali Bombing I, as well as the nodes of lesser influence (e.g. Node 70, who was the courier) (see Figure 5.4(c)). The corresponding Louvain community *C5*, which *C7* is compared with, has not included these actors and has also incorrectly included Nodes 11 and 78 in the cluster. These two actors were involved in the Marriot bombing rather than the embassy bombing in 2004.

The discussion of nodes in their correct place confirms the practical utility of the proposed algorithm. More importantly, the proposed algorithm detected *C6* and *C7* that are covert communities, which would not be apparent with InfoMap or Louvain– the two state-of-the-art techniques. In addition, with better precision of nodes and a lower density in each community, the proposed algorithm will enable a better utilisation of enforcement resources than ever before.

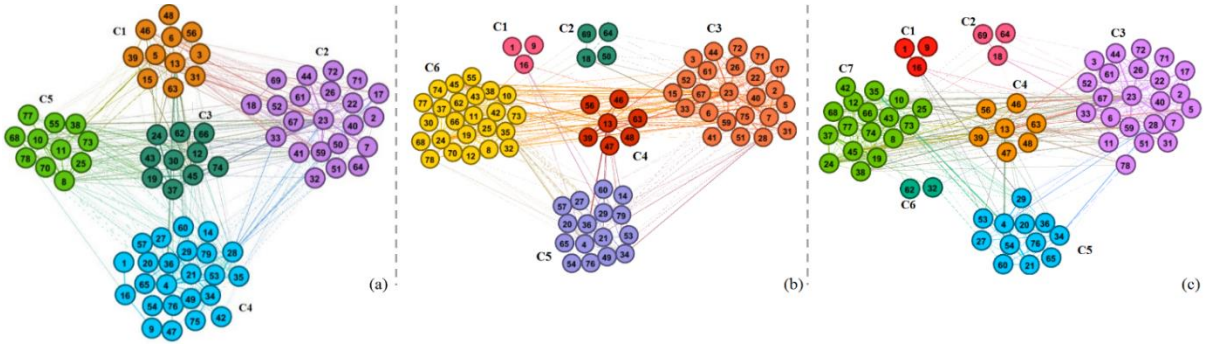

Figure 5.4. Simulation results of different clustering algorithms on Noordin Top network. (a) Multiplex Louvain with 5 communities, *C1* to *C5* ($\boldsymbol{S_a}$= 127.835). (b) Multiplex InfoMap with 6 communities, *C1* to *C6* ($\boldsymbol{S_a}$= 203.922). (c) DNE with 7 non-singleton communities, *C1* to *C7* (for better resolution, singleton clusters are not included, $\boldsymbol{S_a}$= 242.683).

5.5.2 Cluster Analysis on the Boko Haram Network

The second dataset that the proposed algorithm is tested against is the Boko Haram Terrorist network. This dataset, created by Cunningham (2016) from a variety of open-source documents, contains network information of 44 terrorists from an Islamic sect that has been operating primarily in Northern Nigeria since 2002. Unlike the Noordin Top dataset, this dataset is remarkably sparse owing to its young cell-like structure and the lack of collective leadership. From the undirected ties, a three-layer network is constructed: trust, communication and knowledge sharing. The trust layer captures relationships such as colleagues, kinship, superior and supporter. The communication layer is formed by the superimposition of financial ties, communication and membership. Lastly, the knowledge-sharing layer is built from shared events and collaboration (Gera et al. 2017) among the actors.

As presented in Figure 5.5(c), the proposed algorithm finds 12 non-singleton communities. For better resolution, the additional five resulting singleton communities are not included in this figure. Contrarily, Louvain in Figure 5.5(a) and InfoMap in Figure 5.5(b) with AS value of S_a= 46.565 and 52.242 only discovered 9 and 11 non-singleton communities, respectively. When the clusters among the three algorithms are compared, their performances are almost identical in terms of the detection of small clusters. The DNE algorithm performs better in breaking down the larger clusters detected by InfoMap and Louvain into smaller clusters, improving the interpretability of the results for law enforcement agencies. As with the Noordin Top dataset, the outputs of each cluster against the ground truth are discussed below.

Different Terrorist Activities. This was a single large cluster, marked as *C9* in Louvain. However, it was broken down into two smaller clusters, namely, *C10* and *C1*,

by InfoMap. With DNE, cluster *C9* in Louvain was discovered as three clusters, namely, *C1*, *C2* and *C3*, which made it easier to establish a hierarchical relationship. Similarly, cluster *C8* from Louvain which has 11 actors was split into two smaller clusters, namely, *C11* and *C12*, using the DNE algorithm. At the same time, the proposed algorithm also removed actors who were not involved in terrorist activities (Nodes 10, 44, 62, 75 and 79). In turn, this helped reveal the hidden hierarchical structure among actors, making it easier for law enforcement agencies to undertake their investigation.

Mauritania Bombing 2006. Cluster *C7* in Louvain and cluster *C8* in InfoMap are identical, but DNE has pruned this cluster by eliminating inactive actors while keeping the active and important ones. The ground truth about this event is limited. But according to (International Crisis Group 2006), Node 69 was the superior of Nodes 66 and 68, and Node 66 was the superior of Node 67 who was a courier and responsible for sending orders to Node 87, a Nigerian member of Boko Haram who killed 10 Mauritanian soldiers in 2006 (Cunningham et al. 2016). From the ground truth information, it is also noted that both Nodes 67 and 69 were involved in the Mauritanian attack. These five actors (Nodes 66–69 and 87) were in one cluster in Louvain and InfoMap, whereas in the DNE algorithm, the inactive actors are pruned with the active actors put into cluster *C10* (including Nodes 66, 67 and 69).

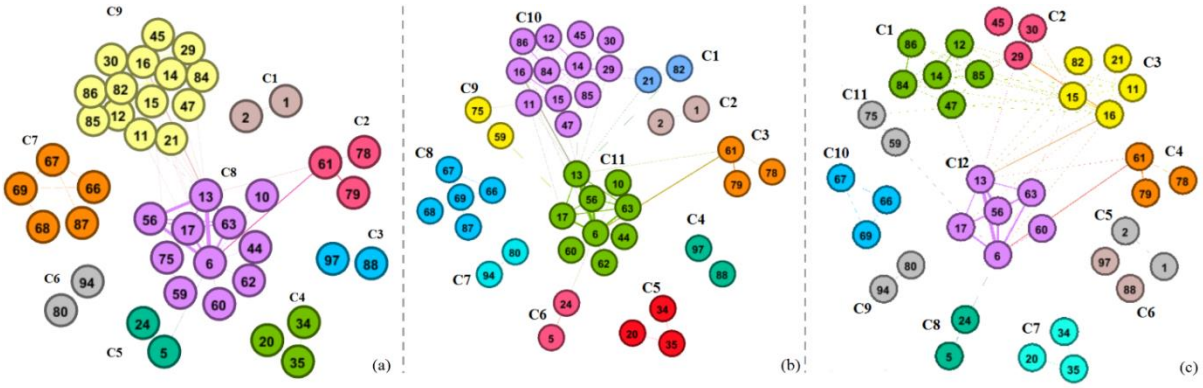

Figure 5.5. Simulation results of different clustering algorithms on Boko Haram network. (a) Multiplex Louvain with 9 communities, *C1* to *C9* ($\boldsymbol{S_a}$= 46.565). (b) Multiplex InfoMap with 11 communities, *C1* to *C11* ($\boldsymbol{S_a}$= 52.242). (c) DNE with 12 non-singleton communities, *C1* to *C12* (for better resolution, singleton clusters are excluded) ($\boldsymbol{S_a}$= 55.392).

5.5.3 Cluster Analysis on the Caviar Network

The Caviar dataset was created by Morselli (Morselli 2009) based on an investigation targeting a hashish and cocaine network operating in Montreal between 1994 and 1996. The principal data source is the information submitted as evidence during the trials of 22 participants in the Caviar network. It included over 1,000 pages of information revealing intercepted phone conversations among actors in the network. The transcripts were used to create the matrix of the drug-trafficking operation's communication system during the investigation. The ties are a person-to-person relation of 110 participants involved in 11 different phases of the investigation drawn from information provided by law enforcement agencies (Morselli 2009). To conceal the identity of individuals, they are designated as nodes (e.g. Node 1,…, Node 110) (Morselli 2009). For experiments, the directed ties of each phase are considered as a separate layer in this dark network, providing us with an 11-layer multiplex network.

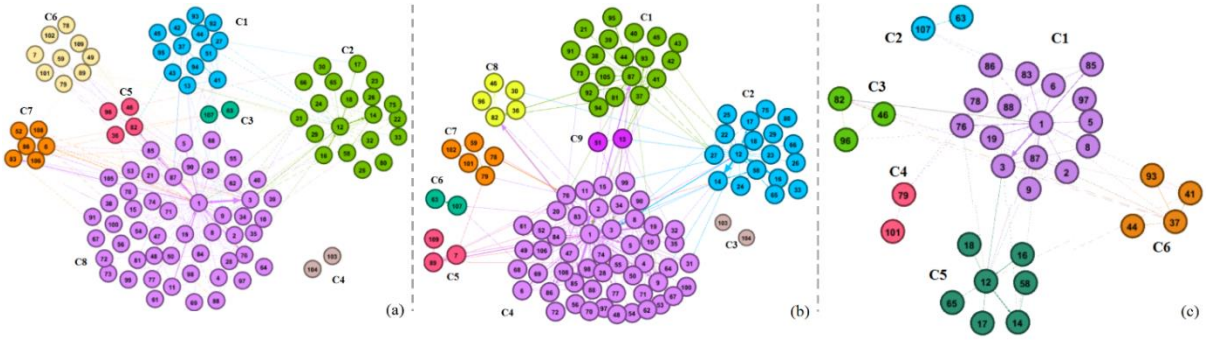

Figure 5.6. Simulation results of different clustering algorithms on Caviar network. (a) Multiplex Louvain with 8 communities, *C1* to *C8* ($\boldsymbol{S_a}$= 990.533). (b) Multiplex InfoMap with 9 non-singleton communities, *C1* to *C9* ($\boldsymbol{S_a}$= 1114.52). (c) DNE with 6 non-singleton communities, *C1* to *C6* (for conciseness, singleton clusters are excluded, $\boldsymbol{S_a}$= 3075.41).

Figure 5.6(a) presents the communities discovered by Louvain with a maximum AS value of S_a = 990.533. The non-singleton communities identified by InfoMap are presented in Figure 5.6(b), including nine different communities with a maximum AS value of S_a = 1114.52. For conciseness, two singleton communities are not presented. As expected, InfoMap better identifies smaller communities compared with Louvain, but the DNE algorithm again outperforms the two baselines with a higher AS value, S_a=3075.41, when comparing the non-singleton communities. As can be seen from Figure 5.6(b), the communities discovered by InfoMap are still very dense. Among the three methods, DNE is the better choice in terms of the identification of hubs and key actors in different communities. Using ground truth information from (Morselli and Giguere 2006), the results are briefly discussed within the five clusters in this network below.

Hashish Trafficking. Cluster *C1* of DNE includes Node 1, the central participant targeted by law enforcement agencies as the principal coordinator for hashish. It also comprises of a subset of other nodes with potential roles within the network. These nodes include: (i) two key traffickers (Nodes 3 and 76) who had pivotal roles in making links with various non-traffickers, (ii) actors with operational roles (Nodes 85, 87 and

89) and (iii) actors serving as legitimate guises for the operation who were also couriers (Nodes 83, 86 and 88). This cluster appeared as *C8* in Louvain and *C4* in InfoMap, which both were dense, rendering the investigation difficult. Contrarily, the DNE algorithm significantly pruned this cluster, as presented in Figure 5.6(c), retaining only the important actors.

Traffickers/Non-traffickers. Similarly, DNE has reduced the membership of cluster *C1* of Louvain into cluster *C6* with only a list of key traffickers and non-traffickers.

Cocaine Importations. Here, Node 12 of cluster *C5* in the DNE algorithm was the principal coordinator for cocaine importations. This cluster is identical to *C2* in Louvain, but again, DNE managed to correctly prune the non-traffickers, retaining only actors with more crucial roles.

Trafficking Operations. In this cluster, DNE has similar results to the baseline methods, except that Node 107 in cluster *C2* in DNE was singled out as the link in the trafficking operations (Morselli 2009).

Legitimate Importers. For this group, both clusters *C5* and *C6* in Louvain were denser than the outputs of DNE in clusters *C4* and *C3*, respectively. Nevertheless, the proposed algorithm proves to be capable of retaining the important nodes. Node 101 was retained in *C4* in DNE, and Node 96 was retained in *C3* in DNE, as these nodes acted as a legitimate importer but rendered traffickers services.

In summary, the comparative analysis of DNE with the two baseline methods using these three datasets emphasises how the use of the AS measure has helped us yield meaningful results for the application problem in this thesis. Specifically, the proposed DNE algorithm performs better in terms of *precision* (i.e. crucial actors, relations and

events are detected) despite a more *concise* (i.e. ‘small’ and low-density communities that are easy to analyse are identified) output compared with the baseline methods. This is further supported by the analysis in Table 5.3 on key actors, roles and clusters in each of these three datasets.

Table 5.3. Analysis of potential actors within detected clusters based on the centrality measures and their role for further disruption (Cluster IDs are according to DNE).

Dataset	Top 10 Actors				Detected Clusters	Disruption Analysis
Noordin Top Network	**Degree**	**Hub**	**Betweenness**	**Closeness**	Developing DI	In cluster C1, Node 16 has a high betweenness centrality reflecting his brokerage role within the network. To disrupt the network, such actors should be targeted because their removal could destabilise the network or even cause it to fall apart (Ferrara et al. 2014).
	Node 23 {C3} (0.610)	**Node 23 {C3}** (0.310)	**Node 23 {C3}** (0.168)	**Node 23 {C3}** (0.681)		
	Node 59 {C3} (0.428)	**Node 24 {C3}** (0.245)	**Node 59 {C3}** (0.115)	**Node 59 {C3}** (0.636)	Bali Bomb II	Cluster C2 is an important clique to be considered for more investigation, which was not detected by Louvain. Members of this cluster could easily avoid from being identified because of keeping a minimum communication with others (as it can be seen, they are not among the top 10 actors of the Noordin Top network).
	Node 24 {C7} (0.415)	**Node 59 {C3}** (0.235)	**Node 4 {C5}** (0.103)	**Node 24 {C7}** (0.592)		
	Node 5 {C3} (0.377)	**Node 5 {C3}** (0.198)	**Node 28 {C3}** (0.072)	**Node 28 {C3}** (0.579)	JI Group and Marriott Bombing	Actors involved in community C3 are of high importance: they play a brokerage role (high betweenness centrality), hold potentially advantageous positions within the network (high degree and hub centrality) (Bright et al. 2017) and are close to other members (high closeness centrality) through both direct and indirect paths (Strang 2014). The arrest of these individuals could destabilise or even dismantle the network.
	Node 4 {C5} (0.325)	**Node 38 {C7}** (0.194)	**Node 13 {C4}** (0.072)	**Node 5 {C3}** (0.570)		
	Node 28 {C3} (0.312)	**Node 8 {C7}** (0.185)	**Node 5 {C3}** (0.069)	**Node 13 {C4}** (0.566)	Hiding Noordin (Jan 2005)	Node 13 of cluster C4 has high betweenness centrality and high closeness centrality and was a conduit in the flow of information.
	Node 45 {C7} (0.312)	**Node 45 {C7}** (0.184)	**Node 24 {C7}** (0.054)	**Node 35 {C7}** (0.562)	JI Group	In cluster C5, Node 4 acts as a connection point (high betweenness centrality).
	Node 35 {C7} (0.299)	**Node 10 {C7}** (0.182)	**Node 16 {C1}** (0.052)	**Node 4 {C5}** (0.558)	Dispose of Bali bombings leftovers	Members of C6 are not among those with high centrality values. Their arrest would have a minimum impact on the disintegration of the network.
	Node 8 {C7} (0.299)	**Node 35 {C7}** (0.182)	**Node 35 {C7}** (0.041)	**Node 73 {C7}** (0.558)	Embassy bombing in 2004	Members of this cluster (marked as C7) play a brokerage role. By having high degree and hub centralities, they are among the highly positioned actors. Disrupting this cluster could potentially destabilise the network.
Boko Haram Network	**Degree**	**Hub**	**Betweenness**	**Closeness**	Different terrorist activities	DNE divides a large cluster C9 of Louvain into smaller clusters C1, C2 and C3, which are easier to analyse. Such a breakdown uncovers the hidden relations that these small clusters have with other members within the network. Clusters C1, C2 and C3 of DNE include members with potentially important roles as they have high degree and hub centrality values. C2 and C3 include members that play brokerage roles (high betweenness); their arrest leads to the disintegration of the network. With the same analysis, cluster C12 includes important members whose arrest is vital in the investigation.
	Node 6 {C12} (0.0.302)	**Node 16 {C3}** (0.432)	**Node 6 {C 12}** (0.323)	**Node 35 {C7}** (1.0)		
	Node 16 {C3} (0.280)	**Node 13 {C 12** (0.341)	**Node 16 {C 3}** (0.178)	**Node 97 {C6}** (1.0)		
	Node 13 {C12} (0.255)	**Node 6 {C 12}** (0.282)	**Node 13 {C 12}** (0.128)	**Node 88 {C6** (1.0)		
	Node 12 {C1} (0.162)	**Node 12 {C1}** (0.279)	**Node 15 {C3}** (0.090)	**Node 2 {C5}** (1.0)		

	Node 85 {C1},84 {C1},15 {C3},11 {C3} (0.140)	**Node 85,84 {C1}** (0.251)	**Node 61 {C4}** (0.086)	**Node 1 {C5}** (1.0)	Mauritania Bombing 2006	DNE has pruned cluster C7 (Louvain) or C8 (InfoMap) to a less-dense cluster, C10. Members of cluster C10 are close to other members within the network (high closeness centrality) and are also actors with key role within this network who have high degree centrality.
	Node 47 {C1},29 {C2}, 86 {C1},17 {C12} (0.116)	**Node 11 {C3}** (0.247)	**Node 30 {C2}** (0.045)	**Node 94 {C9}** (1.0)		
	Node 61 {C4}, 56 {C12}, 63 {C12}, 14 {C1} (0.093)	**Node 47,86 {C1}** (0.223)	**Node 5 {C8}** (0.043)	**Node 80 {C9}** (1.0)		
	Node 30 {C2},82 {C3},67{C10},21 {C3},69 {C10} (0.069)	**Node 29 {C2}** (0.208)	**Node 29 {C2}** (0.038)	**Node 67 {C10}** (0.800)		
	Node 35 {C7}, 66 {C10}, 5 {C8},75 {C11}, 59 {C11} (0.046)	**Node 15 {C3}** (0.190)	**Node 11 {C3}** (0.014)	**Node 69 {C10}** (0.800)		
Caviar Network	**In-degree**	**Out-degree**	**Hub**	**Betweenness**	**Closeness**	
	Node 1 {C1} (0.355)	**Node 1 {C1}** (0.486)	**Node 1 {C1}** (0.649)	**Node 1 {C1}** (0.397)	**Node 107 {C2}** (1)	Hashish Trafficking — Cluster C1 of DNE includes very important members; they have high degree and hub centralities, act as coordinators between different clusters (high betweenness) and are very close to other members within the network.
	Node 3 {C1} (0.187)	**Node 3 {C1}** (0.224)	**Node 3 {C1}** (0.395)	**Node 12 {C5}** (0.186)	**Node 1 {C1}** (0.676)	Traffickers/Non-traffickers — DNE shows a list of key actors within the network: Nodes 37 and 46 of cluster C6 are highly positioned members, and Node 37 also acts as a broker.
	Node 12 {C5} (0.177)	**Node 12 {C5}** (0.187)	**Node 87 {C1}** (0.213)	**Node 76 {C1}** (0.097)	**Node 3 {C1}** (0.553)	Cocaine Importations — DNE keeps a list of key actors within the network: Node 12 of cluster C5 was the principal coordinator of cocaine trafficking and also has a high betweenness and high degree centrality values.
	Node 76 {C1} (0.084)	**Node 87 {C1}** (0.149)	**Node 12 {C5}** (0.207)	**Node 3 {C1}** (0.092)	**Node 12 {C5}** (0.5)	
	Node 9 {C1} (0.084)	**Node 76 {C1}** (0.121)	**Node 76 {C1}** (0.180)	**Node 87 {C1}** (0.063)	**Node 87 {C1}** (0.489)	Trafficking Operations — Node 107 of this cluster has a close relation (high closeness value) with others and had a linkage role within the network.
	Node 83 {C1} (0.075)	**Node 83 {C1}** (0.093)	**Node 83 {C1}** (0.162)	**Node 37 {C6}** (0.052)	**Node 76 {C1}** (0.47)	
	Node 87 {C1} (0.065)	**Node 37 {C6}** (0.084)	**Node 85 {C1}** (0.149)	**Node 79 {C4}** (0.038)	**Node 37 {C6}** (0.452)	Legitimate Importers — DNE reduces the clusters to keep only the most potential actors within the network. Node 79 of cluster C4 was a link between this cluster and others. Node 96 of cluster C3 has a high degree centrality and acts as a potential key member within this cluster, as verified by its role in several important operations.
	Node 37 {C6} (0.065)	**Node 41 {C6}** (0.065)	**Node 8 {C1}** (0.132)	**Node 78 {C1}** (0.032)	**Node 14 {C5}** (0.444)	
	Node 85 {C1} (0.065)	**Node 96 {C3}** (0.065)	**Node 88 {C1}** (0.125)	**Node 41 {C6}** (0.029)		

5.5.4 Comparison of Evaluation Metrics

As the objective of this chapter is to increase AS rather than modularity, measures that are independent of modularity-based metrics are required to evaluate the statistical quality of the detected communities to further support the value of the proposed empirical observations. On this account, additional metrics are presented in this section for further comparison: multiplex-modularity, Surprise value, number of non-singleton clusters, Significance, Performance, internal density, conductance and scalability.

Multiplex-Modularity. Didier et al. (2018) define the multiplex-modularity of multiplex networks as the average of modularities over various network layers. As expected, Table 5.4 demonstrates that Louvain has the highest modularity among all datasets as it results in larger-sized communities. The maximisation of modularity leads to fewer and denser clusters, such as the case in Louvain. As discussed, this slows down the investigation. Contrarily, the maximisation of AS may reduce modularity, but in practice, the produced communities better match what security analysts need for a faster and more accurate detection.

Surprise Value and Number of Non-singleton Clusters. In practice, law enforcement agencies would want to arrest the least number of actors for disrupting a network. As such, the maximisation of AS to overcome the resolution limit helps move insignificant actors into singleton clusters, leading to lower-density non-singleton communities that are easier to interpret by analysts. While this means that there are more clusters driven in part by the singleton clusters, the non-singleton clusters benefit from lower memberships to the key actors that support faster and more accurate

analysis in practice. As presented in Figure 5.7, the DNE algorithm managed to achieve the highest AS on the test data.

Significance (Traag et al. 2013) is a recently introduced objective function to evaluate the quality of the community structure similar to Surprise (Traag et al. 2015). It demonstrates how 'real' a detected community structure is and that the results are not because of chance (Traag et al. 2013). Surprise describes how likely it is to observe internal links in communities. Conversely, Significance looks at how likely such dense communities appear in a random graph. When the number of communities is large or the network is dense, Significance will be more discriminative than AS (Traag et al. 2013). In the accomplished experiments, the proposed algorithm has the highest Significance score, indicating that criminals are not clustered by chance but by their close communication within the network.

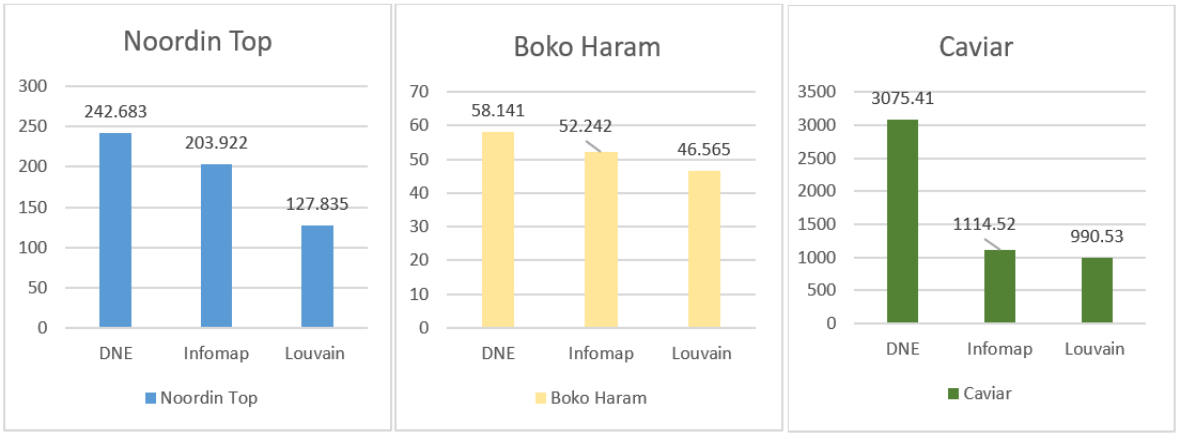

Figure 5.7. Comparison of AS in different community detection methods over different datasets.

Table 5.4. Community metrics over different datasets using three community detection methods

Dataset	Community Detection Approach	No. of non-singleton clusters	Modularity	Graph conductance	Total internal density	Significance	Performance
Noordin Top	DNE	7	0.29	**0.50**	11.41	**379.99**	**0.84**
	InfoMap	6	0.37	0.41	8.71	304.00	0.77
	Louvain	5	**0.40**	0.45	5.80	210.65	0.78
Booko Haram	DNE	12	0.30	0.52	11.9	**66.21**	**0.94**
	InfoMap	11	0.38	0.80	9.57	53.30	0.87
	Louvain	9	**0.40**	**0.89**	7.18	40.45	0.83
Caviar	DNE	6	0.17	**0.59**	65.74	**4398.25**	**0.98**
	InfoMap	9	0.23	0.22	32.23	2459.50	0.86
	Louvain	8	**0.25**	0.23	32.21	2327.16	0.86

Performance. The performance of a cluster is defined as the number of 'correctly interpreted pairs of nodes' in a graph (Brandes et al. 2003; Gaertler 2005). It indicates how well connected the actors are within a cluster (Brandes et al. 2003; Gaertler 2005) and can be used to determine the density of a cluster. If a cluster is dense, each pair of actors in a cluster is highly connected; however, they may have few connections with actors in other clusters (Brandes et al. 2003; Gaertler 2005). Therefore, a higher Performance value indicates that criminals within a cluster may not survive the disruption within a cluster from law enforcement agents as they will not be able to transfer their covert activities to another community in the network (Galvan and Agarwal 2018). As presented in Table 5.4, DNE has the best performance among the three datasets tested in this chapter.

Internal Density. This measure provides a reflection of the internal structure within a community (Liu et al. 2009; Song and Bressan 2013), so that the parts of highly interconnected dark networks can be identified. An increase in the internal connectivity

of a community reduces the possibility of using neighbouring external nodes to bridge any internal disruption. With the DNE algorithm, the detected clusters will yield a higher total weighted internal density (Liu et al. 2009), as presented in Table 5.4. Because the DNE algorithm prunes less-important actors from the clusters, disrupting every community can potentially ensure the failure of the entire network.

Conductance. The conductance of a set of vertices *S* is defined as $\frac{c_s}{2m_s+c_s}$ (Almeida et al. 2011), where $c_s = |(u,v) \in E: u \in S, v/\in S|$ denotes the number of edges with one end in the set and the other end outside, and $m_s = |(u,v) \in E: u \in S, v \in S|$ denotes the number of edges in *S*. A higher conductance in a cluster indicates that it is more isolated from other clusters in the network. Hence, conductance measures the connectedness of a set of nodes to the rest of the graph. The sets of nodes that have fewer connections to the rest of the graph make good communities. This is because such communities reduce the possibility of using neighbouring nodes within other clusters to bridge an internal disruption attempt by law enforcement agencies (Galvan and Agarwal 2018). In the Noordin Top and Caviar datasets, the proposed approach has the highest conductance score, whereas in the Boko Haram data, Louvain achieves the highest conductance score (Table 5.4). In the Boko Haram network, the DNE algorithm's low conductance rate can be attributed to the fact that DNE breaks down larger clusters into smaller ones that may be internally related. This trade-off may be acceptable as several smaller clusters are less challenging to analyse compared with a few large dense clusters.

Figure 5.8. Scalability: different numbers of walkers and various walk lengths.

Scalability. Figure 5.8 presents the elapsed time for a set of different numbers of random walkers to traverse over the network from each and every node. The more walkers used, the faster the entire network is traversed until the number of walkers used reaches about 20, where any further increase does not seem to lead to further speedup. This is attributed to the settings of the server utilised in the experiments that has a configuration of 8 GB RAM and a 2.40 GHs CPU with 32 cores. The programming environment prohibits the commencement of a new walker thread until an existing walker thread completes its task once every CPU core has a walker thread running.

5.6 Chapter Summary

In this chapter, a community detection algorithm, called DNE, is developed to find ‘small’ and ‘good’ communities in dark multi-layer networks. On account of the premise that criminals hide in network hubs, the proposed approach involves the use of random walkers to move towards nodes with higher hub centrality scores. The approach also employs *minwise* hashing to speed up the *Jaccard* correlation calculations in order to hasten the hierarchical agglomerative clustering procedure. The proposed clustering procedure is also unique as it creates clusters to maximise AS instead of modularity.

This helps in the identification of small and lower-density clusters, making the results easier to interpret by law enforcement agencies. Analysis using three real-world dark multi-layer networks demonstrates that the proposed approach outperforms two state-of-the-art techniques. Specifically, this performance is achieved by finding clusters that easily yield the key actors and relations while pruning other actors of lower importance to keep each cluster small and low in density.

One major problem in machine learning on networks is finding a way to incorporate the rich topological information of a network into a machine learning model. For example, in this chapter, such information is extracted using the *Jaccard* correlation values of walked sequences between nodes, and they are fed into the hierarchical clustering algorithm to further detect the clusters. However, the *Jaccard* correlations are calculated once and may not be optimised during the learning process, thus leading to the inaccurate identification of clusters. Recently, there has been a surge towards a new paradigm of graph-based techniques called network embedding (Bengio et al. 2013; Hamilton et al. 2017; Pourhabibi et al. 2020; Zhong et al. 2016). The idea behind these techniques is to map the rich topological structure of networks (e.g. nodes, entire graph or sub-graph) into a low-dimensional space which is also called feature space. The next chapter of this thesis investigates the application of these approaches in the detection of covert communities within a criminal network to probe further into the second sub-research question: **How can users' anomalous activities be detected in a network without any manual feature engineering? (SRQ 2)**.

6 Chapter 6—Discovering Covert Communities in Dark Multi-layer Networks: An Embedding Approach [a]

The detection of community structures in social networks plays a significant role in understanding the functions of complex networks. A common technique to detect communities is graph clustering, where the nodes in a graph (or network) are partitioned into disjoint groups. Numerous clustering techniques are used in graph clustering, such as hierarchical clustering, cut-based partitioning and Girvan–Newman algorithm (Fortunato 2010). The proposed approach in Chapter 5 also falls in this category of community detection approaches. The major challenge in the use of the graph clustering techniques is how the structural information of networks can be translated into a suitable set of features for machine learning (Hamilton et al. 2017). To overcome this drawback, recent studies have turned to 'network embedding' (also known as representation learning) techniques to extract features that demonstrate improvements in classification/prediction results (Bengio et al. 2013; Hamilton et al. 2017; Pourhabibi et al. 2020; Zhong et al. 2016). Network embedding enables us to transform the rich structural information of networks into a low-dimensional vector space that can be subsequently utilised for different machine learning tasks, such as node classification, node clustering, regression and link prediction (Goyal and Ferrara 2018; Li et al. 2018; Salim et al. 2020).

This chapter investigates how network embedding can be applied in the detection of covert communities in multi-layer criminal networks. Using network embedding,

[a] A journal paper developed based on the information presented in this chapter was published: Pourhabibi, T., Ong, K.-L., Boo, Y.L., Kam, B.H., (2021), 'Detecting covert communities in multi-layer networks: A network embedding approach', *Future Generation Computer Systems*, vol. 124, pp. 467–479'.

while the structural characteristics of criminals' network are extracted and learned, the covert communities are also extracted. This chapter attempts to cover the second sub-research question using embedding methods:

- **RQ 2. How can users' anomalous activities be detected in a network without any manual feature engineering?**

The proposed approach is again motivated by social disorganisation theory; the applicability of this theory in the detection of covert networks has been discussed in Chapter 5 (see Section 5.1). The following sections directly explore the proposed approach using Hevner et al.'s (2004) IS framework (see Figure 1.1 in Section1.4).

6.1 Problem Formulation

In most of the studies, the network embedding technique focused on the existence of edges between nodes and ignored the different edge types in the network (Pourhabibi et al. 2020). This feature is akin to recognising the existence of a transportation route (edge) between two towns (nodes) but ignoring the distance or route type (i.e. road or railway). In detecting communities in social networks, this focus could lead to information loss and may prevent the discovery of important information (De Domenico et al. 2015; Rosvall et al. 2014). In reality, social interactions among communities comprise multiple types of relationships, a feature that recent works have increasingly recognised by steering towards analysing multi-layer networks with nodes connected by different edge types (i.e. relationships) (De Domenico et al. 2015; Rosvall et al. 2014). Multi-layer networks are known by different names, depending on the context. With reference to Kivelä et al. (2014), 'multi-layer network', 'multi-graph network', 'multiplex network', 'multi-relational network', 'multi-slice network' and 'multi-level network' are 'multi-layer networks' on the basis of their similar network structure.

Current works that employ network embedding to detect communities typically involve a two-step approach (Chun et al. 2019; Rozemberczki et al. 2019). The first step is network representation learning, and the second is the application of a clustering algorithm (e.g. a classical k-means) to identify communities from the learned features. The drawback of this approach is that these representations may not be the best fit for the preservation of social communities (Chun et al. 2019). Therefore, a goal-directed training framework is required to manipulate the learned representations according to the clustering result to identify more accurate communities.

Research on multi-layer network analysis has led to many new solutions in various application domains. However, as researchers may not have access to the data of networks in some domains, not every domain has received the same level of attention. One of these domains is the *dark network* or *covert social network* problems, where very little data are available (Pourhabibi et al. 2020).

The analysis of dark or covert networks involving illicit activities, such as drug or arm trafficking and terrorist activities (Erickson 1981), is especially problematic. Members of these networks tend to actively hide their actual network information by engaging in a range of ‘diversion’ or ‘cover-up’ activities to reduce the chances of being caught by the authorities (Erickson 1981; Warnke 2016). They would attempt to remain anonymous by exhibiting different ties (e.g. friendship and kinship) and engaging in activities that distract or divert attention from their real intent, e.g. distributing illegal drugs (Erickson 1981).

The current state-of-the-art studies of community detection in multi-layer networks, such as those by (Berlingerio et al. 2011; Berlingerio et al. 2013; Dickison et al. 2016; Rocklin and Pinar 2011), have not been successful in discovering the actual

organisation (De Domenico et al. 2015) when applied to dark networks. In some cases, it was observed that the proposed approaches yielded distorted insights into the network topology and its embedded dynamics (Rosvall et al. 2014). According to Robins (2009), finding covert communities within a dark multi-layer network requires law enforcement agencies to understand individuals' behaviours and qualities, psychological predispositions and network effects. To effectively do this, the algorithm must accurately capture the position of actors within the covert network as this is the salient feature from which the above information can be derived. Without accurate insights into covert network activities, it would remain challenging for law enforcement agencies to disrupt dark network operations. The better law enforcement agencies can understand the interactions and relationships within covert communities, the more efficient and effective they would be in disrupting criminal activities and inhibiting the cascade of influence from one community to another in the network (Moscato et al. 2019; Saxena et al. 2018).

Through a systematic literature review, Pourhabibi et al. (2020) found that network embedding has not been employed to discover covert communities in multi-layer networks, specifically crime and terror-related activities. Network embedding has the potential to find covert communities within a dark multi-layer network, including the position of actors within a covert network to reveal not only their standing but also how they communicate with other members within the network, as demonstrated by Robbins (2009). To capture such structural characteristics, this chapter uses a log-bilinear (LBL) model, which is a type of network embedding that can be applied to the sequences of nodes randomly sampled from the neighbourhood of each node in the network. LBL is able to preserve the structural information related to the different types

of relations in multi-layer networks using relation-specific matrices (Liu et al. 2017a). The context-specific matrices also enable the LBL model to preserve the structural position of the actors within the network (Liu et al. 2017a).

This chapter investigates how network embedding can be employed to detect covert multi-layer networks to overcome some of the abovementioned challenges. Specifically, it aims to find all covert communities within a dark multi-layer network.

6.2 Algorithm Development

The proposed solution, as outlined in Algorithm 6.1, discovers covert communities while learning node representations. It consists of two major mutually beneficial components, namely, (a) network embedding and (b) self-clustering. These components are described below.

6.2.1 Network Embedding

This chapter uses an LBL model (Mnih and Hinton 2007) to learn the representation of the nodes. The LBL model is used as a sequence-based network embedding algorithm to preserve the nodes' positional information about their neighbouring nodes. This objective is achieved by using a random walk to eliminate the need to store the entire neighbourhoods that can be expensive in a large graph (Rozemberczki and Sarkar 2018). This sequence-based approach helps discover covertness among the nodes of interest, as each random walk reveals a specific sequence starting from the node of interest (Rallapalli et al. 2019). In this implementation, the structural information is preserved *via* a position-specific transition matrix. In parallel, a similar matrix is used to capture the properties of multiple relationship types using a relation-specific matrix. This setup is suitable for learning representations from multi-layer networks, as noted by (Liu et al. 2017a). As can be seen in Algorithm 6.1, the

neighbourhood of a node is randomly explored to sample sets of nodes and their relationships with the neighbouring nodes. The LBL model is then applied to the sampled anchor-sets to extract the structural features in order to capture the rich structural information related to the relationship types by incorporating relation-specific matrices. While learning the representations of the nodes, the cluster centroids are also jointly learned to find the best cluster fit for the learned representations.

Algorithm 6.1. $LBLSelfJointOptimizClust$

Input: G: Multi-layer graph,
d: Embedding dimension,
C: No of clusters,
$Iter$: No of iterations,
l: Walk length,
$walk$: No of walks,
B: Batch size,
w: Window size
Output: Node Embeddings,
Cluster Centroids

1 $n = G.nodes().Count()$
/* Initialise θ: Softmax parameter and μ: cluster centroids*/
2 Initialise θ
3 Initialise cluster centroid matrix $\mu \subseteq R^{C \times 2d}$
/* As nodes are sampled, the layer from which they are sampled is also recorded */
4 $Walks, Layers = GenerateMultiLayerWalksTowardsHubs(G, l, walk)$
5 While $IterCount<Iter$ do
6 While True do
7 Update β, γ using Eq. 6-11
/* B anchor-sets of size w are taken and the respective layers for each anchor-set are recorded */
8 $S, L = TakeNextAnchorSet(Walks, Layers, w, B)$
9 For $s, l \in S, L$ do
10 Calculate $\widehat{V_s}$ using Eq. 6-2
11 Calculate L_{loss} using Eq. 6-9
12 Update θ, μ to reduce L_{loss}

13 $V = TakeSourceEmbeddingsFrom(\theta)$
14 $V' = TakeTargetEmbeddingsFrom(\theta)$
15 Return $[V:V']$, μ

6.2.1.1 Anchor-Set Selection

To extract the sequences of nodes in the network, a random walk on the multi-layer network is conducted to extract anchor-sets $\{S_i\}$, a sampling approach representing

the multi-layer network proposed by Grover and Leskovec (2016), as demonstrated in Algorithm 6.1, line 4. The anchor-set $\{S_i\}$ includes all the sequences sampled from the neighbourhood of node i.This sampling approach has two benefits.

First, random walks in a multi-layer network can capture the mutual influence between layers and their topological properties as the random characteristics ensure that a walk is not stuck within a 'local minimum' (Jeub et al. 2017). Consequently, random walkers are more likely to traverse between layers of a multi-layer network, thus capturing more nodes and their respective relationship types (Liu et al. 2017c). Second, the proposed random walk is designed with a heuristic derived from (Sageman 2004) who states that criminals mostly lay in network hubs. As a result, the random walkers in this algorithm are designed to sample the anchor-sets while moving towards network hubs (Grover and Leskovec 2016), making the approach appropriate for finding covert communities.

Following Liu et al. (2017c), given the fact that a random walker is on node j in layer β, the probability to transfer to node i in layer α is given by:

$$\mathrm{P}\left(c_{t+1} = v_i^{\alpha} \middle| c_t = v_j^{\beta}\right) \propto \frac{w_{j\beta}^{i\alpha}}{\sum_{i\alpha \epsilon V} w_{j\beta}^{i\alpha}} \qquad (6\text{-}1)$$

where $w_{j\beta}^{i\alpha}$ denotes the weight of the link between node j in layer β and node i in layer α. If the network is unweighted, $w_{j\beta}^{i\alpha} = 1$. If the network is directed, $w_{j\beta}^{i\alpha} \neq w_{i\alpha}^{j\beta}$, the random walkers walk directly; otherwise, they walk indirectly. When random walkers jump to the next neighbour with the probability $\mathrm{P}\left(c_{t+1} = v_i^{\alpha} \middle| c_t = v_j^{\beta}\right)$, they sample from the nodes and layers they traverse. This sampling process generates long sequences of length l, starting from each node, and records the layers from which the node is sampled (Algorithm 1, line 4) (Rozemberczki and Sarkar 2018). In next step, a group

of B anchor-sets are generated using the sliding window size w (Algorithm 1, line 8) and then fed into LBL for representation learning (Rozemberczki and Sarkar 2018).

6.2.1.2 LBL Embedding: Multiple Relationship Types

In deep learning applications, LBL is viewed as a single-layer feed-forward neural network (Liu et al. 2017a) and is usually used for sequential prediction problem. To use LBL, the final predicted representation ($\hat{V}_s$) of a given sequence $s = u_1, \dots, u_n$ is calculated using a linear combination of the input items u_i and the transition matrices at each position:

$$\hat{V}_s = \sum_{i=0}^{n-1} P_i \, V_{u_i} \tag{6-2}$$

where $P_i \in R^{d \times d}$ denotes the transition matrix for the corresponding position in a sequence; n, the number of elements in a sequence and V_{u_i}, the representation of item u_i in the sequence.

As Eq. 6-2 demonstrates, LBL represents the position of each item in a sequence with a specific matrix. Therefore, it can model the complex situations of a local context (i.e. neighbouring items in the sequences). To model multiple relations between nodes and capture the impact of the different types of relationships, a relation-specific matrix M is defined, where $M \in R^{r \times d}$ models the corresponding relationship of the i-th item in a sequence ($u_{i-1} \xrightarrow{r_i} u_i$) to determine the properties of multiple types of relationships. This feature can then be modelled by Eq. 6-3 as (Algorithm 6.1, line 10):

$$\hat{V}_s = \sum_{i=0}^{n-1} P_i M_i \, V_{u_i} \tag{6-3}$$

To learn the node representation, the conditional likelihood of target node v generated by an anchor-set s $\{s = [u_1, \dots, u_n, v] \in S\}$ is defined based on the following Softmax function (Takase et al. 2016; Yuan et al. 2017):

$$p(v|s,\theta) = \frac{\exp(f(v,s))}{\sum_{v' \in N_v^S} \exp(f(v',s))} \quad (6\text{-}4)$$

$$f(v,s) = \hat{V}_s^T V'_v + b_v \quad (6\text{-}5)$$

where $\theta = [V_{u_i}, V'_v, M, P, b_v]$ denotes the Softmax parameter; f, the similarity function between the predicted representation $\hat{V}_s$ and the actual representation V'_v of the target node v (Song et al. 2019); N_v^S, the list of neighbouring nodes of the target node v in anchor-set $s \in S$ and b_v, a bias term. The representation of each node v_i is defined as $[\hat{V}_{v_i} : \hat{V}_{v_i}'] \in R^{2*d}$, where source $\hat{V}_{v_i} \in R^d$ denotes the source representation; $\hat{V}_{v_i}' \in R^d$, the representation of its target and (:), the concatenation function (Yuan et al. 2017). Lastly, to learn the structural representation, the proposed algorithm minimises the negative log-likelihood of Eq. 6-6. The idea is that the likelihood of observing a node is independent of observing other nodes in a given sequence starting from the source node (Yuan et al. 2017). Minimising Eq. 6-6 maximises the likelihood of observing the target node v in sequence s starting from the source node:

$$L_{embd} = \sum_{v \in V} -\log p(v|s,\theta) \quad (6\text{-}6)$$

The proposed algorithm also minimises the reconstruction error by calculating the loss between the original network's adjacency matrix (A) and the reconstructed structure (Chun et al. 2019):

$$\hat{A} = \begin{cases} sigmoid\left(\hat{V}^T \hat{V}\right) undireceted; \\ sigmoid\left(\hat{V}_s^T \hat{V}_t\right) \ directed. \end{cases} \quad (6\text{-}7)$$

$$L_{reconstrct} = loss\left(A, \hat{A}\right) \quad (6\text{-}8)$$

where $\hat{V}$ denotes the resulting matrix of all node representations; $\hat{V}_s$, the representations of source nodes; $\hat{V}_t$, the representations of targets and $\hat{A}$, the adjacency matrix of the reconstructed network. In directed networks, as the adjacency matrix $\hat{A}$ is not symmetric, the use of the asymmetric reconstruction is required (Salha

et al. 2019). The aim is to make the reconstructed network similar to the original one. Because multi-layer networks are used in this chapter, to evaluate the reconstruction loss, the adjacency matrix A of the original multi-layer network is extracted by creating an aggregated weighted network using an aggregation of all L layers ($\sum_{\alpha=1}^{L} w_{ij}^{\alpha}$).

6.2.2 Self-Clustering

The major challenge in community detection is that the nodes' representations are usually learned, and a classic clustering (e.g. k-means) is then applied to the learned representations (Chun et al. 2019). The nodes are then assigned to specific clusters according to the distance of their representations to the cluster centres (Chun et al. 2019). As mentioned above, this two-step process produced less-accurate communities as the nodes' representations are not optimised according to their cluster centres (Rozemberczki et al. 2019). To overcome this issue, a cluster-optimiser module is developed to optimise cluster centres according to the nodes' representations using an unsupervised regularisation term. This module minimises a cost function using a similar approach to k-means. Here, the similarity between the extracted representation of node i and the cluster center μ_c, is measured using the following objective function (Rozemberczki et al. 2019):

$$L_{clust} = \sum_{v \in V} \min_{c \in C} ||\hat{V}_v - \hat{\mu}_c||_2 \quad (6\text{-}9)$$

In Eq. 6-8, there are C disjoint cluster centres where $\hat{\mu}_c \in R^{2*d}$ denotes the mean value of the c^{th} cluster in the embedding space, and $\hat{V}_v$ denotes the resulting representation of node $v \in V$. The objective is to minimise the distance from each node to its nearest cluster center and update the nodes' representations accordingly (Algorithm 6.1, line 11).

6.2.3 Joint Optimisation

A key feature of the proposed solution is that the proposed approach jointly optimises the nodes' representations and cluster centroids to identify more accurate communities. To do this, the total loss values defined in the previous sections are minimised as the overall objective function (see Algorithm 6.1, lines 11 and 12) as follows:

$$L_{loss} = L_{embd} + \gamma L_{clust} + \beta L_{reconstrct} \tag{6-10}$$

where $\gamma, \beta \geq 0$ are coefficients to control the balance between loss values. Variables γ and β are set according to an exponential annealing rule proposed by Rozemberczki et al. (2019) (Algorithm 1, line 7):

$$\varphi_{t+1} = \varphi_t . \left(10^{\frac{-t.log_{10}\varphi_0}{w.l.n.walk}}\right)\left(\varphi_{final} - \varphi_0\right) + \varphi_0, \varphi_0, \varphi_{final} \in [0,1] \tag{6-11}$$

where w denotes the context window size; l, the walk length; n, the number of nodes in the network and $walk$, the number of sampled sequences per node.

The algorithm continues to minimise the overall loss value until a specific criterion, e.g. some predefined number of iterations, is satisfied (Algorithm 6.1, line 5). In sum, minimising the costs related to the nodes' structural representations ($L_{reconstrct}, L_{embd}$) in line with clustering cost (L_{clust}) helps LBL manipulate the embedding space and scatter embedding points to obtain higher clustering performance and, therefore, more distinct communities.

6.3 Knowledge Base

6.3.1 Dataset Description

This chapter uses four real-world multi-layer dark networks and also one synthetic network to evaluate the effectiveness of the proposed algorithm compared with the

baseline models. The following sections describe the details of the datasets (see Table 6.1).

6.3.1.1 Noordin Top Terrorist Network

The Noordin Top Terrorist network is a dataset reflecting the terrorist network operating in Indonesia. The actors in this network were responsible for various terrorist activities (International Crisis Group 2006). The network includes 78 actors (criminals) attending 45 different events, which are categorised into four to form a four-layer network: trust, operational, communication and business ties. The ties in each category are undirected and considered as a separate layer of the network. The trust layer is generated by the superposition of classmate, friendship, kinship and soul mate ties, whereas the operational layer is produced from four sub-layers: logistics, meetings, operations and trainings (Roberts and Everton 2011).

6.3.1.2 Boko Haram Network

The Boko Haram Terrorist network contains the relationship information of 44 terrorists belonging to an Islamic sect that has been operating primarily in Northern Nigeria since 2002. The group believes that the current Nigerian government is corrupted by false Muslims (Cunningham et al. 2016). This network is created by Cunningham (2016) using a variety of open-source documents. The undirected ties are re-organised into edges to create a three-layer network: trust, communication and knowledge sharing. The trust layer includes colleagues, kinship, superior and supporter. The communication layer is formed by the superimposition of financial ties, communication and membership, whereas the knowledge-sharing layer is formed from shared events and collaboration (Gera et al. 2017).

6.3.1.3 FARC Terrorist Network

The FARC Terrorist network includes the relationship information of the terrorist group known as the Revolutionary Armed Forces of Colombia that has been operating primarily in Columbia and Venezuela since 1964 (Saxena et al. 2018). According to Weimann (2006), the organisation believes in the Marxist ideology and seeks to overthrow the Colombian government. The network is sparse for most layers, but being a social media network, it has a well-documented hierarchical structural layer (Weimann 2006). This network dataset was created by Cunningham et al. (2013) using a variety of open-source documents. Similarly, the undirected relationship data is re-organised into a three-layer network (Gera et al. 2017): trust, communication and knowledge sharing. The trust layer can be categorised into six sub-layers: friendship, kinship, superior, colleagues, co-workers and radicalisers. A combination of communications, meetings and shared organisations forms the communication layer. The knowledge-sharing layer includes collaboration ties in this network. Since the superior relationships were directed, the whole network was created as a directed network by adding parallel links to any pair of connected individuals.

6.3.1.4 LFR Network

The LFR network is a synthetic network generated using the mLFR benchmark (Bródka and Grecki 2016; Lancichinetti et al. 2008). Since most of the publicly available covert networks are small in scale, this synthetic network is utilised to provide the scalability evidence for the proposed approach on a larger scale. To generate the network, the mLFR parameters are set to mimic the behaviour of criminals in covert networks: low degrees (average degree = 10, maximum degree = 15) and intention to create small communities (minimum community = 50, maximum community = 500).

The number of layers is set to two. The other main parameter within this benchmark is mixing parameter ([0 1]), which controls the amount of noise by adding additional edges between the planted communities and the rest of the network to hide the community structure to make it difficult for the community detection algorithms to discover the communities. When this parameter is set to zero, the community structure is very evident and when it gets larger than 0.5, the structure starts to disappear (Bródka and Grecki 2016). Setting this parameter to 0.5 resulted in the creation of a two-layer network with 1500 nodes and 22725 undirected links with an overall modularity of 0.422 and 20 distinct clusters.

Table 6.1. Dataset characteristics

Dataset	No. of Nodes	No. of Links	No. of Layers	Features	No. of Clusters
Noordin Top	78	1014	4	Undirected, unweighted	5
Boko Haram	44	198	3	Undirected, weighted	9
FARC	294	1013	3	Directed, unweighted	26
LFR	1500	22725	2	Undirected, unweighted	20

6.3.2 Baseline Methods

As with any empirical evaluations, the first step is to establish the baseline. Because the proposed solution in this chapter is sequence-based embedding, six state-of-the-art sequence-based embedding methods were identified as the baseline for comparative analysis. Perozzi et al. (2014) developed DeepWalk, which is a random walk-based approach transplanted by Skip-gram and hierarchical Softmax to represent social relationships. Node2vec, which was developed by Grover and Leskovec (2016), is similar to DeepWalk; it introduces biased depth-first and breadth-first random walk strategies based on DeepWalk. Struc2vec, which was developed by Ribeiro et al. (2017), is another type of node embedding strategy that also uses

random walk to find similar representations on nodes that are structurally similar. Conversely, LINE, developed by Tang et al. (2015), learns node presentations on large-scale networks by preserving first-order and second-order proximities (Hamilton et al. 2017). ComE, which was developed by Cavallari et al. (2017) assumes that communities fit a Gaussian structure in the embedding space. It also employs a Gaussian mixture model to random walks on monoplex networks to learn node embedding and clusters jointly. These methods, although proven to be useful in monoplex network analysis (i.e. networks with one type of relationship), have ignored relationship multiplicity.

Motivated by the importance of multiplicity and multi-layer networks, recent works have steered towards learning representations of nodes in a multi-layer network. Principled Multilayer Network Embedding (PMNE) (Hongming Zhang et al. 2018) extended the idea of Node2vec to multi-layer networks and introduced three different network embeddings for nodes in a multi-layer network. The first is a similar approach to Node2vec, where the representations are extracted from the aggregated network (PMNE-n). The second one is a linear aggregation of the result of the representations in each layer of the network (PMNE-r). The third one is a network co-analysis method (PMNE-c). In this approach, the random walker can not only traverse on nodes of a layer but also be transported to the same node in another layer of the network using a jumping factor. In the end, the algorithms would have numerous sequences of visited nodes generated from all layers that can serve as an input to the Softmax classifier used in Node2vec.

Another work that studied node embedding in a multi-layer network is Scalable Multiplex Network Embedding (SMNE) (Liu et al. 2017c). This work proposed a high-

dimensional common representation for nodes and a low-dimensional additional representation for each type of relation by learning the representations of each layer. Once the representations of one layer are learned, they are used as the inputs of Softmax to learn the representations of other layers (Hajiseyedjavadi et al. 2019).

Multigraph2Vec, a recent algorithm developed by Roy et al. (2020) for finding communities in multi-graphs, also introduces a novel random walk-based strategy using Lévy flight, followed by the Skip-gram, to generate the node embeddings. Using the Lévy flight random walk strategy, the random walkers can traverse across multiple layers and reach far-off nodes in a single step. In Multigraph2Vec, the transition probabilities are learned in a supervised procedure using node attributes (e.g. node metadata or their network structure).

These aforementioned approaches have two significant drawbacks. First, the learned representations may not be the best fit for the subsequent graph clustering task. Second, some of these methods (e.g. DeepWalk, Node2Vec, Struct2Vec, LINE, PMNE-n and ComE) can only be applied in monoplex networks, which means that they only consider the existence of connections between nodes and ignore the types of relationships.

6.3.3 Experimental Setup

To evaluate the performance of the baseline methods, the parameter settings used in the published papers are followed. The parameters (γ, β) of the proposed algorithm are initially set to 0.1, and their value is increased through an annealing process while training the model up to a maximum value of 0.5 as proposed by (Rozemberczki et al. 2019). Because there is no ground truth provided for the membership of each node in the datasets used in this study, this chapter adopted the suggestion of (Alzahrani and

Horadam 2014; Canu et al. 2015) and used the number of clusters obtained using the 'multi-slice modularity'-based Louvain[1] method (Liu et al. 2018) as metadata ground truth, which are reported in Table 6.1. For the generated synthetic network, the number of clusters is derived from the mLFR benchmark (Bródka and Grecki 2016).

To generate the anchor-sets, following Rozemberczki and Sarkar (2018), five sequences ($walk = 5$) of random walks are sampled from each node with a length of 40 ($l = 40$). The anchor-sets are then created by sliding over the generated walks using a window size $w = 5$. The generated anchor-sets are then grouped into batches $B = 10$ to learn representations with an embedding dimension $d = 15$.

6.4 Results and Discussion

6.4.1 Time Complexity Analysis

Given the number of random walks (n_{walk}), walk length (l), context window size (w), representation size (d), number of layers (M) and number of clusters (n_c), the time complexity of the algorithm is dominated by training time of the Softmax model, which is linear with the number of nodes $O(Mn_{walk}|V|lw(d + n_c))$. As shown in Table 6.2, our linear complexity puts our approach in a competitive position compared to other methods when applied to multi-layer networks. Our method yields better results in terms of accurate community detection than methods that are very similar to our algorithmic approach, e.g., SMNE. As we will show in the next section, on similar level of time complexity, our method delivers more accurate representation of covert communities and is more capable of finding ones that others missed.

[1] Multiplex Louvain (https://louvain-igraph.readthedocs.io/en/latest/multiplex.html)

Table 6.2. Comparison of complexity with related work*.

Approach	Type of Network	Complexity
DeepWalk	Monoplex	O($n_{walk}lw$|V|(d+$d$log|V|))
Node2Vec	Monoplex	O($n_{walk}lw$|V|a^2)
PMNE (n)	Multi-layer	O($n_{walk}l$|V|a^2 +M|V|)
PMNE (r)	Multi-layer	O(M(($n_{walk}lw$|V|a^2))
PMNE (c)	Multi-layer	O($n_{walk}ldw$|V|a^2))
SMNE	Multi-layer	O($Mn_{walk}lw|V|$)
ComE	Monoplex	O(|V|+|E|)
Mutigraph2Vec	Multi-layer	O(|S||V|^3)
Our approach	Multi-layer	O($Mn_{walk}|V|lw(d+n_c)$)

* Note:
a is the average degree of the network
E is the set of all edges in the network
S is the set of all source nodes in the network

6.4.2 Experimental Results on Clustering

The results of the five experiments on the four datasets are presented in Tables 6.3–6.6. In both tables, the value for the best-performing approach on each metric is presented in bold. Given the absence of a gold-standard ground truth, the following measures are proposed to evaluate the quality of the detected communities.

Multiplex-Modularity (Didier et al. 2018). First, a competent algorithm for the proposed problem must be able to find distinct communities within a network, particularly the small and less-obvious ones, as they are likely to be the terrorist groups in the network (Sageman 2004). Technically, a good community is the one with a higher similarity of nodes within it, i.e. the nodes inside the community have a minimum similarity to the ones outside it (Luan et al. 2019). The proposed modularity measure evaluates this quality with a high value indicating the detection of a more distinct community.

By analysing each distinct community, law enforcement agencies can determine the viral effect of covert activities within the community (Pinheiro 2012). They will know what happens with other communities or other members of a specific community after

a particular member commits covert activities at a point in time (Pinheiro 2012). This viral influence of covert activities can be inhibited by disrupting a community within the covert organisation, leading to a cascading disruption of other communities (Saxena et al. 2018).

As presented in Tables 6.3–6.6, the proposed approach achieves a higher modularity than all the other baseline algorithms. Because modularity is a measure of the effectiveness of the community detection process, the results indicate that the proposed algorithm outperforms the other baseline methods in terms of finding distinct communities within covert networks.

Surprise (Traag et al. 2015). While multiplex-modularity helps identify the communities within the network, from Sageman (2004) it can be inferred that terrorist networks tend to be small; thus, a measure to help find such small but well-formed communities (high modularity) is required. This characteristic can be measured by Surprise. A high Surprise value indicates that an algorithm can identify smaller cliques and clusters that would be more valuable in the proposed application problem and yet are not easily identifiable given the elusiveness of such communities. As such, the extraction of small communities from a network that embodies the relationships of a list of suspects is an important starting point in an investigation (Magalingam et al. 2015). The Surprise values presented in Tables 6.3–6.6 indicate that the proposed algorithm is more capable than the other baseline methods in detecting small communities that reveal the hidden hierarchical structures among the criminals.

Internal Density and Cut-Ratio. Internal density (Liu et al. 2009; Song and Bressan 2013) estimates the density of a cluster: the higher the internal density, the

more connected are the nodes within a cluster. Hence, it indicates how well connected a given community is.

Contrarily, the cut-ratio (Song and Bressan 2013) is a cluster quality measure that estimates the number of edges between two communities. A good community is one with a low cut value but a high internal density.

A high internal density and a minimum cut-ratio in a community structure reduce the possibility of using neighbouring nodes in other clusters to bridge any internal disruption by law enforcement agencies (Galvan and Agarwal 2018). The introduced algorithm achieves a lower internal density on the Noordin Top and Boko Haram networks compared with the baseline methods (see Tables 6.3–6.6). Moreover, it does not hit the lowest cut-ratio on the Noordin Top, Boko Haram and FARC networks. This feature is attributable to the ability of the proposed approach to break down the network into smaller and more intelligible clusters, which resulted in a higher Surprise value, to reveal the hierarchical structure hidden among the criminals. This characteristic reduces the density but increases the cut-ratio as the clusters get smaller, which may be internally related to each other. However, smaller clusters are less challenging to analyse compared with large high-density clusters.

Significance (Traag et al. 2013). A recently introduced objective function for evaluating the community structure quality, Significance presents an approach similar to Surprise (Traag et al. 2015). It is a measure for evaluating how real a detected

Table 6.3. Experimental results on the Noordin Top dataset

	Modularity	*Cut-Ratio*	*Internal Density*	*Surprise*	*Significance*
Deep Walk + K-means	0.219 ±(0.038)	0.176 ±(0.024)	4.711 ±(0.531)	117.854 ±(14.340)	192.912 ± (30.617)
Node2Vec + K-means	0.312 ±(0.052)	0.170 ± 0.005)	5.334 ± (1.295)	142.992 ±(21.422)	211.759 ±(17.297)
PMNE (n) + K-means	0.263 ±(0.006)	**0.170** ±(0.152)	4.556 ±(0.0685)	133.892 ±(5.306)	208.909 ±(26.335)
PMNE (r) + K-means	0.311 ±(0.014)	0.224 ±(0.026)	4.810 ±(0.336)	80.044 ±(14.191)	154.025 ±(11.698)
PMNE (c) + K-means	0.345 ±(0.032)	0.186 ±(0.034)	5.513 ±(1.293)	131.308 ±(33.480)	195.835 ±(63.488)
SMNE+ K-means	0.235 ±(0.010)	0.189 ±(0.006)	**9.603** ±(0.031)	111.965 ±(5.326)	146.824 ±(3.902)
ComE	0.285 ±(0.003)	0.179 ±(0.001)	4.417 ±(0.025)	131.519 ±(4.022)	213.702 ±(0.008)
Multigraph2Vec + K-means	0.204 ±(0.003)	0.202 ±(0.008)	4.701 ±(1.208)	105.698 ±(2.598)	160.306 ±(53.148)
Proposed approach	**0.3894** ±(0.007)	0.2111 ±(0.063)	4.53 ±(0.877)	**149.078** ± (8.948)	**277.164** ±(11.657)

Table 6.4. Experimental results on the Boko Haram dataset

	Modularity	*Cut-Ratio*	*Internal Density*	*Surprise*	*Significance*
Deep Walk + K-means	0.2483 ±(0.008)	0.2125 ±(0.0312)	6.284 ±(0.774)	28.346 ± (3.949)	38.539 ±(5.959)
Node2Vec + K-means	0.267 ±(0.026)	**0.0984** ±(0.0111)	6.201 ±(0.298)	26.543 ± (2.506)	26.288 ±(3.940)
PMNE (n) + K-means	0.287 ±(0.022)	0.101 ±(0.027)	6.570 ±(0.257)	31.613 ± (2.839)	37.042 ±(8.365)
PMNE (r) + K-means	0.077 ±(0.010)	0.325 ±(0.183)	5.307 ±(1.074)	15.068 ± (1.882)	28.494 ±(3.014)
PMNE (c) + K-means	0.2744 ±(0.0075)	0.2998 ±(0.542)	**7.905** ±(0.373)	30.398 ±(1.765)	55.222 ±(9.060)
SMNE+ K-means	0.080 ±(0.044)	0.120 ±(0.010)	6.0937 ±(0.327)	22.833 ± (2.706)	23.783 ± (2.555)
ComE	0.292 ±(0.017)	0.134 ±(0.012)	5.903 ±(0.013)	39.052 ±(4.022)	**61.689** ±(2.458)
Multigraph2Vec + K-means	0.174 ±(0.014)	0.131 ±(0.008)	6.330 ±(0.142)	30.630 ±(9.085)	42.366 ±(10.289)
Proposed approach	**0.353** ±(0.0200)	0.137 ±(0.017)	5.746 ±(0.070)	**39.887** ±(4.069)	38.539 ±(7.306)

Table 6.5. Experimental results on the FARC dataset

	Modularity	*Cut-Ratio*	*Internal Density*	*Surprise*	*Significance*
Deep Walk + K-means	0.650 ±(0.024)	**0.054 ±(0.006)**	9.705 ±(0.822)	671.080 ±(37.739)	716.430 ±(37.276)
Node2Vec + K-means	0.645 ±(0.019)	0.055 ±(0.004)	9.623 ±(0.642)	648.480 ±(43.743)	700.071 ±(27.038)
PMNE (n) + K-means	0.663 ±(0.010)	0.603 ±(0.013)	9.728 ±(0.163)	697.865 ±(25.578)	726.782 ±(15.401)
PMNE (r) + K-means	0.392 ±(0.029)	0.188 ±(0.015)	10.733 ±(1.421)	218.093 ±(56.880)	413.714 ±(75.018)
PMNE (c) + K-means	0.566 ±(0.006)	0.833 ±(0.006)	9.521 ±(1.283)	421.511 ±(8.121)	513.526 ±(22.119)
SMNE+ K-means	0.686 ±(0.018)	0.501 ±(0.007)	10.383 ±(0.252)	783.706 ±(35.803)	733.355 ±(30.385)
ComE	0.617 ±(0.015)	0.585 ±(0.004)	10.850 ±(0.211)	561.733 ±(62.974)	698.005 ±(7.944)
Multigraph2Vec + K-means	0.524 ±(0.031)	0.099 ±(0.002)	10.846 ±(0.383)	436.47 ±(42.522)	520.973 ±(21.658)
Proposed approach	**0.694 ±(0.018)**	0.545 ±(0.003)	**10.983 ±(0.142)**	**791.312 ±(31.453)**	**763.341 ±(29.187)**

Table 6.6. Experimental results on the mLFR dataset

	Modularity	*Cut-Ratio*	*Internal Density*	*Surprise*	*Significance*
Deep Walk + K-means	0.377 ±(0.014)	0.141 ±(0.003)	4.756 ±(0.104)	5760.823 ±(55.213)	5721.295 ±(130.319)
Node2Vec + K-means	0.381 ±(0.021)	0.141 ±(0.009)	4.677 ±(0.109)	5842.342 ±(63.824)	5759.637 ±(217.423)
PMNE (n) + K-means	0.380 ±(0.011)	0.141 ±(0.010)	4.538 ±(0.221)	5800.783 ±(13.923)	5813.743 ±(69.245)
PMNE (r) + K-means	0.378 ±(0.030)	0.143 ±(0.012)	5.037 ±(0.340)	5766.494 ±(9.250)	5756.706 ±(83.487)
PMNE (c) + K-means	0.379 ±(0.013)	0.141 ±(0.001)	5.159 ±(0.105)	5710.359 ±(10.210)	5737.253 ±(73.907)
SMNE+ K-means	0.231 ±(0.016)	0.150 ±(0.003)	2.492 ±(0.085)	2892.497 ±(77.719)	2800.402 ±(113.076)
ComE	0.389 ±(0.012)	0.1445 ±(0.023)	5.438 ±(0.485)	5533.329 ±(36.927)	5778.825 ±(87.376)
Multigraph2Vec + K-means	0.294 ±(0.015)	0.1459 ±(0.003)	3.549 ±(0.013)	4094.916 ±(48.210)	4077.6811 ±(135.295)
Proposed approach	**0.406 ±(0.0110)**	**0.1399 ±(0.014)**	**6.597 ±(0.215)**	**6121.962 ±(21.439)**	**6200.239 ±(61.395)**

community structure is and whether the results are due to chance alone (Traag et al. 2013). In sparse networks, such as criminal networks, without an explicit community structure, the ‘significance’ of a cluster is a more discriminative measure compared with Surprise for evaluating the quality of the detected clusters (Traag et al. 2013). A high Significance value indicates that criminals are not categorised into their respective clusters by chance but are put in the clusters according to their close connections within the network. Compared with the other baseline methods, the proposed approach attains a high Significance value in the Noordin Top Terrorist network, FARC and LFR. However, in the Boko Haram network, which is sparse, the proposed approach has the second-highest Significance value following PMNE (c).

Normalised Mutual Information (NMI) (Emmons et al. 2016). For the LFR synthetic network, the clusters derived from the mLFR benchmark are used as a ground truth. Since there is no ground truth provided for the membership of each node in the selected real-world datasets, the clustering result of the ‘multi-slice modularity’-based Louvain method (Liu et al. 2018) is used as metadata ground truth (Alzahrani and Horadam 2014; Canu et al. 2015). Figure 6.1 presents the average NMI, a measure of mutual dependence between two clusters. In all datasets, the proposed approach tops the NMI value.

Impact of the Number of Dimensions. Finally, the impact of the number of embedding dimensions in the accuracy of the proposed approach is analysed. Figure 6.2 presents the average modularity values of the experiments using different dimensions on the four datasets. The best average result on the Noordin Top, Boko Haram and FARC networks is achieved when the embedding dimension is set to $d = 15$. As the dimension of node embedding exceeds 30, the modularity value decreases.

On the LFR, the behaviour is slightly different, as the modularity does not change much when the embedding dimension is set to *d = 60.* However, there is no clear explanation for this behaviour, which may be because the loss value is influenced by the number of embedding dimensions (Yin and Shen 2018), thus impacting the final embeddings, cluster centroids and, therefore, modularity. As observed by Arora (2016), there is always a sweet spot for the optimal dimensionality: neither too small nor too large.

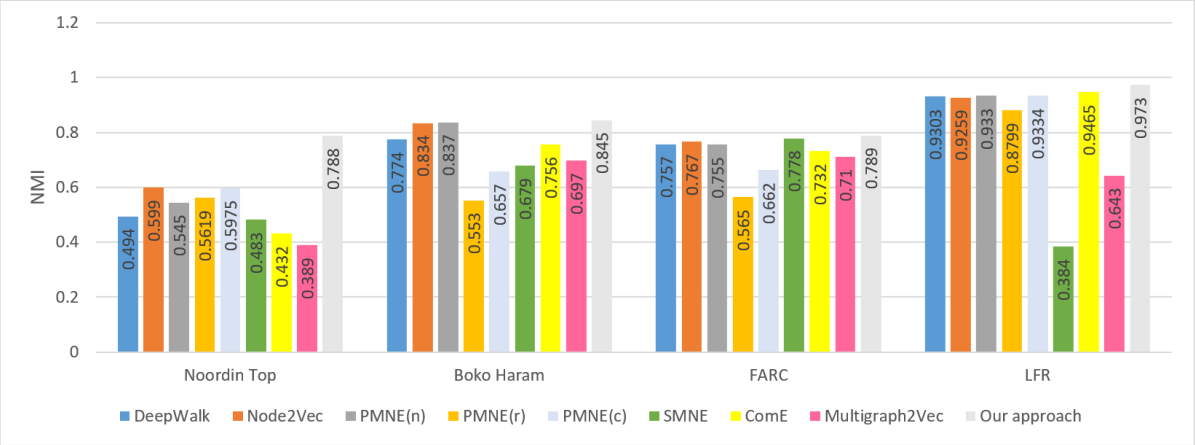

Figure 6.1. NMI values of clustering result over the four datasets in this chapter.

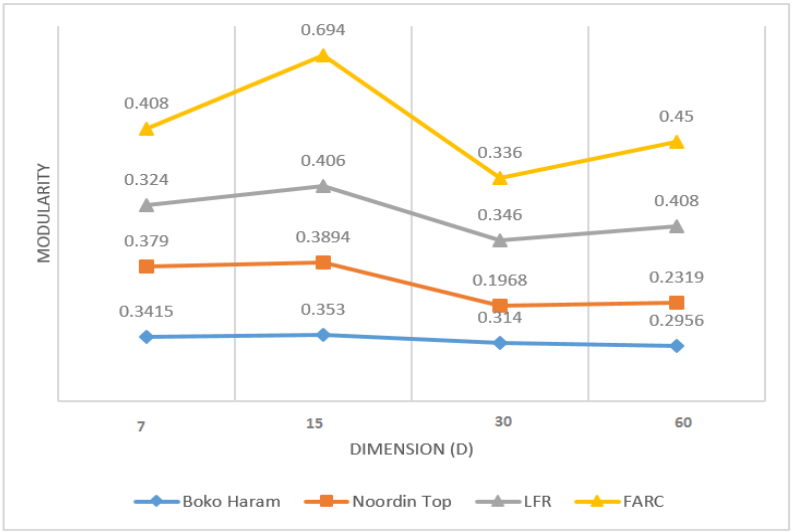

Figure 6.2. Modularity values of the proposed approach over the four datasets using different embedding dimensions.

6.4.3 Experimental Results on Link Prediction

Missing information is one of the main challenges in the criminal network analysis, given how the actors and their activities are predominantly covert. The growing attention paid by law enforcement agencies to the intelligent analysis of data in organised crimes since the mid-1907s has created great strides on recovering missing connections among the actors of criminal networks (Berlusconi et al. 2016). These connections are likely to exist but have not been reported due to the criminals' anti-detection strategies (Berlusconi et al. 2016; Calderoni 2014; Lim et al. 2020; Lim et al. 2019; Moradabadi and Meybodi 2018). In this context, link analysis and link prediction have been employed to 'establish the relationships that exist among individuals and organisations from bits and pieces of available evidence' (Harper and Harris 1975).

Figure 6.3 presents the comparison of the AUC result of the link prediction generated by different methods over the two networks using the k-fold ($k = 5$) cross-validation and Hadamard link prediction metric (Grover and Leskovec 2016):

$$e_{uv} = e_u * e_v \tag{6-12}$$

The overall AUC is the average result of AUC for each relation type; a higher value indicates that an algorithm was able to find more hidden links. For DeepWalk, Node2Vec and ComE, which are applicable to just monoplex networks, a separate embedding is learned for each relation type, and the trained model is utilised to predict links of the corresponding network layer.

For the baseline methods that consider the importance of relationship types among actors in the network, the experiments demonstrate that they all return a higher AUC value. This result is expected as techniques considering different relationship types in multi-layer networks are more likely to capture the hidden structural information of the

network with higher accuracy (De Domenico et al. 2015; Rosvall et al. 2014). The exception here is Multigraph2Vec, which did not perform well in either of the datasets. The other exceptions are ComE with a low AUC value (AUC <= 0.50) in all datasets, Node2Vec and DeepWalk, which could not accurately predict the unreported links (AUC < 0.60) in the sparse Boko Haram and FARC dark networks. These two algorithms, however, performed better in the Noordin Top and LFR networks as they have a denser structural topology. In the case of PMNE(r), the algorithm did not perform well in the Boko Haram and Noordin Top networks, suggesting that the structural topology could not be accurately trained using this algorithm. However, PMNE(r) performs better on the FARC and LFR networks. Contrarily, the proposed approach performs well in recovering missing information and predicting unreported links, with an accuracy of over 0.80 (AUC > 0.80) on all networks.

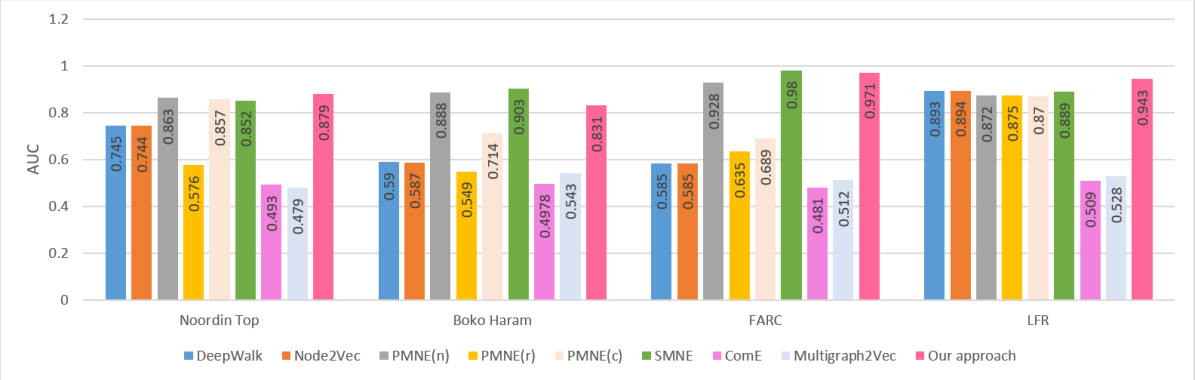

Figure 6.3. AUC result of link prediction over the two datasets obtained from the different methods in this study.

6.4.4 Experimental Results on Network Disruption

The purpose of finding covert communities in a network is to facilitate an intervention by law enforcement agencies to prevent terror-related communications, activities and ideologies from spreading within that network. Any effective attempt to disrupt a network is known as ‘network disruption’, which lies in the ability of an

algorithm to find these communities. According to Morone and Makse (2015), the most influential nodes are those forming the minimal set that guarantees a global connection of the network. If the nodes are randomly removed, the network undergoes a structural collapse, leading to the reduction of the collective influence (CI) of the network (Morone and Makse 2015; Teng et al. 2016). CI measures the influence of nodes in a criminal network, considering the degree of the nodes' neighbours at a given distance. The total CI of a given network with N nodes is defined as (Morone and Makse 2015):

$$CI_l = \sum_{i=1}^{N} CI_l(i) \tag{6-13}$$

$$CI_l(i) = (k_i - min_{(i,j)\epsilon E}\, w_{ij}) \sum_{j \in \sigma B(i,l)} (k_j - min_{(j,s)\epsilon E}\, w_{js}) \tag{6-14}$$

where k_i denotes the degree of node i; $B(i,l)$, the ball of radius l $(l = 2)$ centred on node i and $\sigma B(i,l)$, the frontier of the ball, which is the set of nodes at distance l from i. For a weighted network, the degree k of a node should be substituted by its weighted degree ($\sum_{(i,j)\epsilon E} w_{ij}$, E is the list of edges).

Instead of randomly removing nodes from the network, the block removal method is simulated to mimic a police raid scenario (Cavallaro et al. 2020) using the detected clusters in different methods in this study. In the block removal scenario, each community is considered as a sub-network (or supernode) (Figure 6.4), and the total collective influence (CI_l) of the community structure (CI_l^c) is evaluated using Eq. 6-13 (Kobayashi and Masuda 2016). The resulting values are then sorted, and in each iteration of block removal, the cluster with the highest CI_l^c is eliminated. Figure 6.5 demonstrates how the removal of communities, including the most influential nodes, affects the dismantling of the network in terms of the total network CI, which is the overall influence of all criminals within the network to retain the network as a giant

connected component.

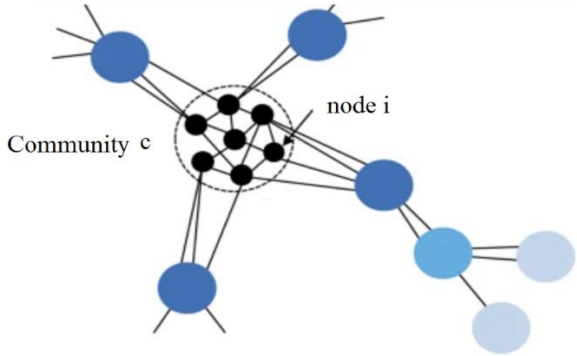

Figure 6.4. Community structure: each community is considered as a sub-network.

As can be seen from Figure 6.5, the community structure detected by the proposed approach leads to a lower (CI_i^c), indicating that the detected community structure tends to form smaller connected components. This means that the use of the proposed algorithm in this chapter leads to the creation of a community structure that minimises the overall influence of important criminals in the entire network (Teng et al. 2016). This result indicates that by attacking one community, the criminals within that community would not be able to transfer their covert activities to another community in the network (Galvan and Agarwal 2018). Furthermore, as illustrated in Figure 6.5, the community structures detected by the proposed approach are less resistant to network disruption: more reduction in CI_i^c as the communities are removed.

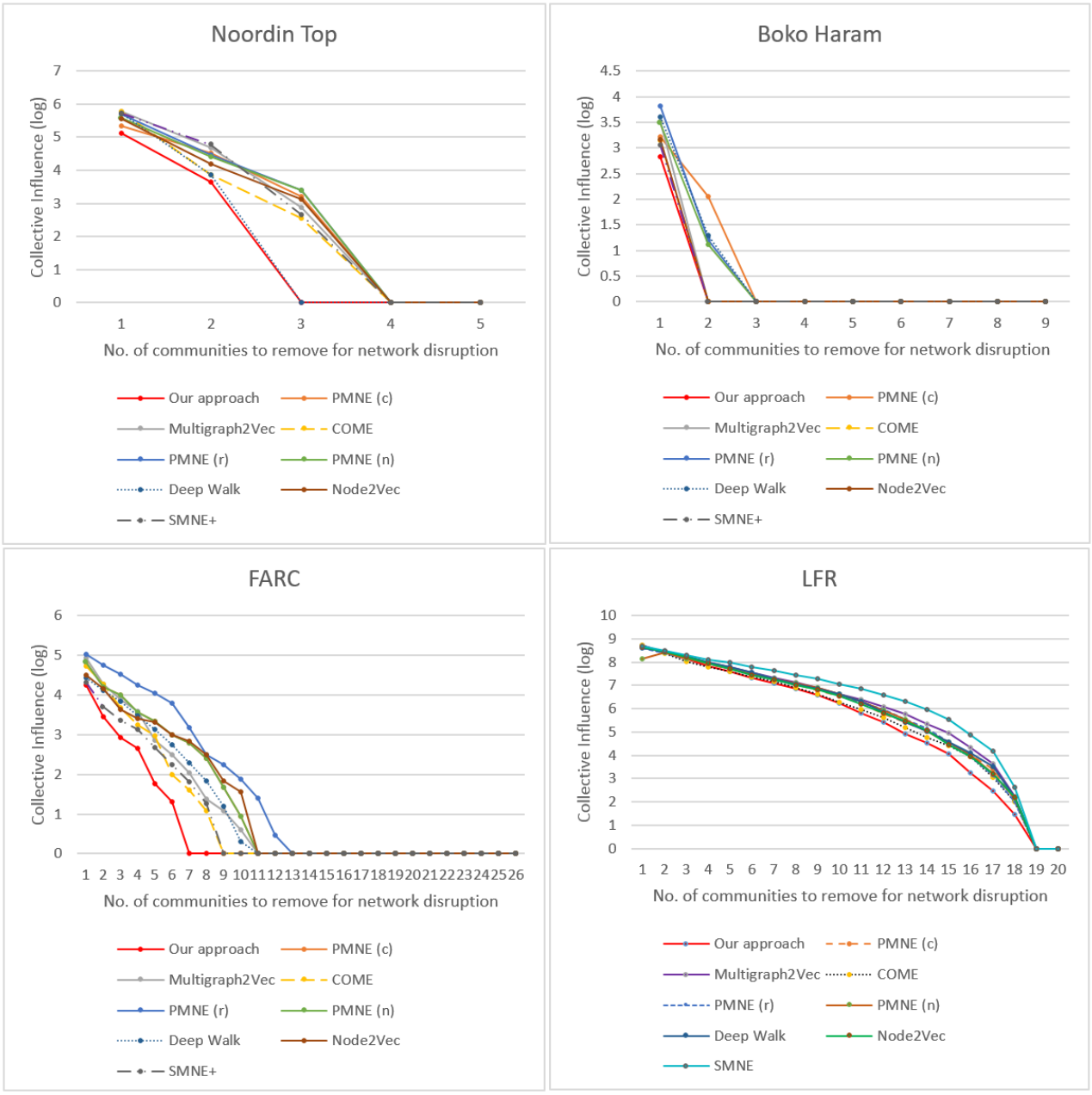

Figure 6.5. Block removal attack: the impact of eliminating each community in the reduction of the log values of $\boldsymbol{CI}_i^c$, leading to network disruption.

6.5 Chapter Summary

The detection of communities within criminal networks is an important step for law enforcement agencies to disrupt criminal organisations. Law enforcement agencies can benefit from understanding the inter-relationships between communities and the operations of criminal organisations. Furthermore, the disruption of one community of

the organisation can lead to a cascading disruption of other communities. In this chapter, a network embedding algorithm using an LBL model is proposed to jointly perform graph clustering and learn graph embedding on multi-layer networks in a unified framework. Using an LBL model, the proposed solution incorporated: (i) the nodes' positional information about the other neighbouring nodes and (ii) the type of relations that connects the nodes. The result is a network embedding algorithm that is well suited to clustering tasks, rendering the proposed algorithm applicable in finding covert communities, which are less resistant to network disruption effort. Moreover, this algorithm predicts missing links in dark multi-layer networks with high accuracy. A comparison of the experimental results achieved using various state-of-the-art methods validates the superiority of the proposed approach to others in finding high-quality clusters and predicting missing links among the network actors, with an accuracy of over 80%.

7 Chapter 7—Thesis Restatement and Conclusion

This thesis introduces GBAD-based machine learning algorithms to detect deviant behaviours in social networks using two main approaches, namely, feature engineering and graph embedding. The proposed approaches provide the opportunity to reveal and study the topological structure and properties of social networks to identify suspected criminals attempting to evade detection using a range of cover-up activities, which lead to the formation of multi-layer networks and time-evolving networks. Moreover, to improve the validity of the proposed algorithms, the GBAD algorithms developed in this research are guided by the basic tenets of criminological theories.

7.1 Conclusion and Contributions

The work presented in this thesis highlights several methods and applications of the GBAD techniques in detecting deviant behaviours. It contributes to both the theory and practice of identifying suspicious behaviours in social networks in several ways.

Through a systematic literature review of current research studies of fraud detection using the GBAD techniques, *Chapter 2* facilitates the identification of the key issues and possible improvement opportunities in recent research studies. It develops a classification framework to facilitate the analysis and comprehension of current research studies on fraud detection using the GBAD techniques.

The proposed classification framework provides an analytical platform for synthesising existing work from various aspects. In addition to offering researchers an insightful understanding of the application of the GBAD techniques in fraud detection, this classification framework provides practitioners and researchers a roadmap to

perceive the correspondence between the nature of their network, different types of anomalies and appropriate graph-based methods that match their needs to their application areas.

Chapter 3 develops the theoretical foundation of the proposed GBAD algorithms in this research. Using five different criminological theories, this chapter attempts to provide insights into the causes and consequences of crime by answering the *why* (i.e. rational choice theory), *what* (i.e. routine activity theory), *where and when* (i.e. crime pattern theory) and *how* (i.e. differential association theory and social disorganisation theory) questions pertaining to criminal motivations and behaviours. It explicitly translates the principles of criminological theories into SNA methodologies for implementation using the GBAD techniques. It also sheds light on the methods and strategies used by criminologists and gives contextual knowledge when it comes to develop and design GBAD algorithms aimed to support criminologists. Further, applying the basic tenets of criminological theories to substantiate the logic for developing algorithms gives validity to the techniques, leading to the design of robust algorithms.

Chapter 4 focuses on the development of human-engineered features or feature engineering of deviant characteristics within a *time-evolving multi-layer* online social dating website. It addresses the need for developing algorithms capable of detecting suspicious behaviours when criminals evade detection by spreading their devious activities over different timestamps or getting involved in multiple types of activities to divert attention. Four different sets of features are introduced based on the principles of differential association theory: a set of profile-based features, a set of lightweight

behaviour-based features, a set of bursty features and a set of sequence-based features.

The four designed features are novel creations derived from other research areas (e.g. gene analysis, Twitter) and brought together to enable the detection of deviant cybercrimes within a *time-evolving multi-layer* network by analysing the frequency, intensity and durability of interactions. One of the strengths of the designed features in this chapter is its accuracy in differentiating criminals from normal users compared with the baseline method in terms of the AUPR curve, AUROC curve and Accuracy. In practice, the combination of the gradient-boosted decision trees classifier and the proposed features results in a single model that could be applied in an OSN to prevent any harmful consequence on the legitimate users. This model provides high-precision classification for spamming accounts within a social network. These accounts, which are relatively rare and are likely owned by potential criminals, are automatically blocked without affecting the majority of normal users. The other merit of the proposed algorithm is that the designed features are scalable to large networks as the extraction of features using the proposed processing framework (see Figure 4.3) leads to a lower extraction time compared with the baseline method.

Human-designed features are not always able to accurately identify suspicious activities. Extracting them from large-scale networks may also be too complex, thus leading to scalability issues. In addition, designing accurate features would be very dependent on human creativity and expertise and is also time-consuming. To overcome such issues of the feature engineering approaches, and drawing on criminological theories, Chapters 5 and 6 introduce novel rigorous algorithms, which can extract features from multi-layer criminal networks without human interventions.

Chapter 5 introduces a random walk-based approach combined with hierarchical clustering to automatically extract features from communication among criminals involved in a covert network to find the respective communities to which they belong. Using the extracted features (i.e. Jaccard similarities), the algorithm searches for more cohesive portions of the multi-layer criminal networks using a hierarchical clustering method. The proposed clustering procedure creates clusters to maximise AS instead of modularity, which helps identify small and lower-density clusters of key actors while pruning other actors of lower importance, making it easier for law enforcement agencies to interpret the results.

The most important implication of the proposed algorithm for the practitioner is, therefore, the ease of interpretation of the detected clusters. For law enforcement agencies, early detection and disruption of covert networks are crucial to the disruption of criminal activities. Regardless of the number of available resources, law enforcement agencies are always limited by the window of opportunities they have before the occurrence of a serious incident. As such, algorithms that can analyse large-scale networks and detect covert communities and their activities are always important for security agencies to quickly and accurately conduct their investigations. Thus, the developed algorithms should be *precise* (i.e. create a list of crucial actors, relations and events) and *concise* (i.e. identify ‘small’ and low-density communities that are easy to interpret).

Given this objective, compared with current methods that focus on modularity maximisation, the design of the proposed algorithm focused on optimising the AS. The first implication of this algorithm in research begins with the use of a different set of measures, which are motivated by the use-case and the heuristics included from other

research areas (e.g. criminology). The aim is to deliver a solution that aligns with the needs of the stakeholders, i.e. security agencies. As indicated by the results, the use of AS over modularity has led to easily interpretable communities.

The proposed algorithm also manages to bring together different components from the existing methods in a way that achieves multiplex navigation in covert *multi-layered networks*. Thus, the key contribution of the proposed algorithm lies in the way these components are brought together for the specific purpose of detecting covert communities.

Because the features, i.e. Jaccard correlations, are calculated once and then a clustering method is applied to them to detect the respective communities to which each criminal belongs, the features are not optimised during the clustering process. Therefore, the accuracy of the detected communities may decline, especially when the network is very sparse or large. This issue leads to the design of the final algorithm in Chapter 6.

In *Chapter 6*, a network embedding algorithm using an LBL model is proposed to categorise criminals into their respective clusters while learning and optimising the features on multi-layer networks. The experiments in this chapter demonstrate how the proposed algorithm leads to more accurate clusters compared with those obtained from the eight state-of-the-art techniques. The novelty of the proposed algorithm is that it is well suited to clustering tasks in *multi-layer networks,* enabling the detection of covert communities without human intervention. Compared with the results yielded by the eight state-of-the-art methods examined in Chapter 6, the resulting communities detected by the proposed algorithm are less resistant to network disruption efforts.

The proposed algorithm also exhibits high accuracy in identifying missing links in terms of the AUC.

The purpose of finding covert communities is to facilitate the disruption of illegitimate communication, activities and the spread of illegal ideologies within the network. As such, the main contribution of this algorithm is its ability to find covert communities that are less resistant to disruption efforts, enabling security agencies to disrupt the covert network with the suspected criminals having no chance to transfer their covert activities to other communities within the network. The second contribution of the proposed approach in Chapter 6 is its high accuracy in identifying missing links in dark multi-layer networks. The identification of missing information and links, which exist among criminals but are not reported owing to their use of a variety of cover-up activities to avoid detection, is also very significant in criminal investigations. It enables law enforcement agencies to sniff out actors with a large likelihood of co-participating in illegal activities, ultimately helping to destabilise the network, particularly if the actors are playing significant roles within the network.

7.2 Recommendations for Future Research

Like all scientific research, this thesis has a number of limitations. First, the systematic literature review, though extensive, may have omitted some relevant studies due to the content limitations of the scientific databases used, specific keywords utilised in the search and timeframe selected for the review. Furthermore, the GBAD techniques have been widely employed for fraud detection in the OSN area, which covers a wide range of applications, such as e-commerce, online shopping, dating, online recommendation and social media websites. Each application may be under the threat of different types of fraud (e.g. spam, deception and fake reviews,

fake opinions, ‘Like’ farms, advertising fraud and cyberbullying), which may have been inadvertently excluded from the review due to the choice of keywords in the search. Therefore, a detailed analysis of the different types of fraudulent activities in OSNs where the GBAD approaches have been employed to detect such activities can be conducted in future review studies. Furthermore, the literatures reviewed were exclusively selected from academic journals. Future work will benefit by including non-academic sources where the application of GBAD techniques is reported.

Second, although the heuristics and principles of the algorithms developed in this research are grounded on validated criminological theories, future studies would be very much strengthened by drawing from theories beyond criminology, such as human psychology and cognitive science, which could be turned into heuristics to help design meaningful and effective measures to further enhance the techniques to detect illegitimate activities.

Third, as pointed out earlier, the major issue in fraud detection and crime analysis is data availability. This research is also not exempted from this challenge. All the real-world datasets utilised in the experiments in Chapters 5 and 6 were relatively small in scale. Although Chapter 6 has used a large synthetic network to increase the validity of the experiments (as explained in Section 2.3.7.1), there are problems with the use of such network in experimental analysis. Therefore, future research should consider the development of strategies for collecting rich crime-related data from available resources, such as rapidly expanding social media that surrounds the criminal activities of interest.

Forth, the task of identifying communities in a network will always be a challenging one, especially if the network contains covert communities. No one knows for sure

how many communities there are in a real-world network. The proposed algorithm in Chapter 6 shares this limitation. It requires the number of communities to be specified by a domain expert. Therefore, the next step is to explore ways to remove the need for this specification. One possibility in future work is to derive the optimal number of clusters while learning representations in the algorithm.

Fifth, the dimensionality of the feature space (i.e. the number of features) are also defined by domain experts, which (as explained in Sections 4.5.1 and 6.4.2) affects the accuracy of the results. Therefore, introducing a method to search through the feature space for selecting the optimal features can be considered for future work.

Finally, the spread of criminal activities can lead to serious social issues. Therefore, identifying the sources of crime and analysing the spreading influence of crimes within social networks can help stop the consequences, opening a wide range of future research.

8 References

Abdallah, A., Maarof, M. A., & Zainal, A., (2016), 'Fraud detection system: A survey', *Journal of Network and Computer Applications*, vol. 68, pp. 90–113.

Abt, T. P., (2017), 'Towards a framework for preventing community violence among youth', *Psychology, Health & Medicine*, vol. 22, no. sup1, pp. 266–285.

Agrawal, D., Budak, C., El Abbadi, A., Georgiou, T., & Yan, X. (2014), 'Big Data in Online Social Networks: User Interaction Analysis to Model User Behavior in Social Networks test', DNIS 2014, Springer International Publishing, viewed 1 Jan 2014, <https://doi.org/10.1007/978-3-319-05693-7_1>.

Agrawal, R., Potamias, M., & Terzi, E. (2012), 'Learning the Nature of Information in Social Networks', In Proceedings of the ICWSM 2012, Dublin, Ireland, 4–7 June 2012, AAAI Press, pp. 1–8.

Ahmed, A., Shervashidze, N., Narayanamurthy, S., Josifovski, V., & Smola, A. J. (2013), 'Distributed large-scale natural graph factorization', In Proceedings of the WWW 2013, Rio de Janeiro, Brazil, 13–17 May 2013, ACM, pp. 37–48.

Akers, R. L., (1990), 'Rational Choice , Deterrence , and Social Learning Theory in Criminology : The Path Not Taken', *The Journal of Criminal Law and Criminology*, vol. 81, no. 3, pp. 653–676.

Akoglu, L., & Faloutsos, C., (2009), 'RTG: a recursive realistic graph generator using random typing', *Data Mining and Knowledge Discovery*, vol. 19, no. 2, pp. 194–209.

Akoglu, L., Tong, H., & Koutra, D., (2015), 'Graph based anomaly detection and description: a survey', *Data Mining and Knowledge Discovery*, vol. 29, no. 3, pp. 626–688.

Aldecoa, R., & Marín, I., (2014), 'SurpriseMe: an integrated tool for network community structure characterization using Surprise maximization', *Bioinformatics*, vol. 30, no. 7, pp. 1041–1042.

Almeida, H., Guedes, D., Meira, W., & Zaki, M. J. (2012), 'Is There a Best Quality Metric for Graph Clusters?', In Proceedings of the ECML PKDD 2011, Athens, Greece, 5–9 Sep. 2011, Springer-Verlag, pp. 44–59.

Alon, N., Avin, C., Koucky, M., Kozma, G., Lotker, Z., & Tuttle, M. R. (2008), 'Many Random Walks Are Faster Than One', In Proceedings of the SPAA 2008, Munich, Germany, 14–16 June 2008, ACM, pp. 119–128.

Alvarez-Hamelin, J. I., Dall'Asta, L., Barrat, A., & Vespignani, A. (2005), 'Large scale networks fingerprinting and visualization using the k-core decomposition', In

Proceedings of the NIPS 2005, Vancouver, Canada, 5–8 Dec. 2005, MIT Press, pp. 41–50.

Alzahrani, T., & Horadam, K. J. (2014), 'Analysis of two crime-related networks derived from bipartite social networks', In Proceedings of the ASONAM 2014, Beijing, China, 17–20 Aug. 2014, IEEE Press, pp. 890–897.

Arora, S., (2016), '*Word embeddings: Explaining their properties*', viewed 14 Feb. 2016, <https://www.offconvex.org/2016/02/14/word-embeddings-2/>.

Arsovska, J., & Kostakos, P. A., (2008), 'Illicit arms trafficking and the limits of rational choice theory: the case of the Balkans', *Trends in Organized Crime*, vol. 11, no. 4, pp. 352–378.

Awrad Mohammed, A., (2014), 'Synthetic Generators for Simulating Social Networks', Master of Science, University of Central Florida, <https://stars.library.ucf.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=5789&context=etd>.

Baerveldt, C., Völker, B., & Van Rossem, R., (2008), 'Revisiting selection and influence: An inquiry into the friendship networks of high school students and their association with delinquency', *Canadian Journal of Criminology and Criminal Justice*, vol. 50, no. 5, pp. 559–587.

Bahulkar, A., Szymanski, B. K., Baycik, N. O., & Sharkey, T. C. (2018), 'Community Detection with Edge Augmentation in Criminal Networks', ASONAM 2018, IEEE, viewed 25 Oct. 2018, <https://doi.org/10.1109/ASONAM.2018.8508326>.

Bangcharoensap, P., Kobayashi, H., Shimizu, N., Yamauchi, S., & Murata, T. (2015), 'Two Step graph-based semi-supervised Learning for Online Auction Fraud Detection', ECML PKDD 2015, Springer International Publishing, viewed 29 Aug. 2015, <https://doi.org/10.1007/978-3-319-23461-8_11>.

Basu, K., & Sen, A., (2021), 'Identifying individuals associated with organized criminal networks: A social network analysis', *Social Networks*, vol. 64, pp. 42–54.

Benevenuto, F., Magno, G., Rodrigues, T., & Almeida, V. (2010), 'Detecting spammers on Twitter', CEAS 2010, viewed July 2010, <https://homepages.dcc.ufmg.br/~fabricio/download/ceas10.pdf>.

Bengio, Y., Courville, A., & Vincent, P., (2013), 'Representation Learning: A Review and New Perspectives', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 8, pp. 1798–1828.

Benson, M. L., Madensen, T. D., & Eck, J. E. (2009). 'White-Collar Crime from an Opportunity Perspective', In S. S. Simpson & D. Weisburd (Eds.), The Criminology of White-Collar Crime, Springer New York, New York, NY, pp. 175–193, <https://doi.org/10.1007/978-0-387-09502-8_9>.

Berlingerio, M., Coscia, M., & Giannotti, F. (2011), 'Finding redundant and complementary communities in multidimensional networks', In Proceedings of the CIKM 2011, Glasgow, Scotland, UK, 24–28 Oct. 2011, ACM, pp. 2181–2184.

Berlingerio, M., Pinelli, F., & Calabrese, F., (2013), 'ABACUS: frequent pAttern mining-BAsed Community discovery in mUltidimensional networkS', *Data Mining and Knowledge Discovery*, vol. 27, no. 3, pp. 294–320.

Berlusconi, G., Aziani, A., & Giommoni, L., (2017), 'The determinants of heroin flows in Europe: A latent space approach', *Social Networks*, vol. 51, pp. 104–117.

Berlusconi, G., Calderoni, F., Parolini, N., Verani, M., & Piccardi, C., (2016), 'Link Prediction in Criminal Networks: A Tool for Criminal Intelligence Analysis', *PloS One*, vol. 11, no. 4, p. e0154244.

Bershtein, L. S., & Tselykh, A. (2013), 'A clique-based method for mining fuzzy graph patterns in anti-money laundering systems', In Proceedings of the SIN 2013, Aksaray, Turkey, 26–28 Nov. 2013, ACM, pp. 384–387.

Bhat, S. Y., & Abulaish, M. (2013), 'Community-based features for identifying spammers in Online Social Networks', In Proceedings of the ASONAM 2013, Niagara Falls, ON, Canada, 25–28 Aug. 2013, IEEE, pp. 100–107.

Bhattacharjee, S. D., Yuan, J., Jiaqi, Z., & Tan, Y. P. (2017), 'Context-aware graph-based analysis for detecting anomalous activities', In Proceedings of the ICME 2017, Hong Kong, China, 10–14 July 2017, IEEE, pp. 1021–1026.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C., (2011), 'Data mining for credit card fraud: A comparative study', *Decision Support Systems*, vol. 50, no. 3, pp. 602–613.

Bichler, G., Lim, S., & Larin, E., (2017), 'Tactical Social Network Analysis: Using Affiliation Networks to Aid Serial Homicide Investigation', *Homicide Studies*, vol. 21, pp. 133–158.

Bichler, G., & Malm, A. (2019). 'Social network analysis ', In Routledge Handbook of Crime Science, 1st ed., Routledge, <https://doi.org/10.4324/9780203431405>.

Bichler, G., & Malm, A. (eds), (2015), 'Disrupting Criminal Networks: Network Analysis in Crime Prevention', FirstForumPress, <https://www.rienner.com/title/Disrupting_Criminal_Networks_Network_Analysis_in_Crime_Prevention>.

Bigot, C., (2017), 'Guardians and Targets: A Routine Activity Approach to Terrorism in Southeast Asia', *Open Journal of Social Sciences*, vol. 05, pp. 140–163.

Bindu, P. V., Mishra, R., & Thilagam, P. S., (2018), 'Discovering spammer communities in twitter', *Journal of Intelligent Information Systems*, vol. 51, no.

3, pp. 503–527.

Bindu, P. V., & Thilagam, P. S., (2016), 'Mining social networks for anomalies: Methods and challenges', *Journal of Network and Computer Applications*, vol. 68, no. Supplement C, pp. 213–229.

Bindu, P. V., Thilagam, P. S., & Ahuja, D., (2017), 'Discovering suspicious behavior in multilayer social networks', *Computers in Human Behavior*, vol. 73, pp. 568–582.

Blau, P. M., (1977), 'Inequality and Heterogeneity: A Primitive Theory of Social Structure', *The ANNALS of the American Academy of Political and Social Science*, vol. 442, no. 1, pp. 167–168.

Bolton, R. J., & Hand, D. J., (2002), 'Statistical Fraud Detection: A Review', *Statistical Science*, vol. 17, no. 3, pp. 235–255.

Booth, A., Sutton, A., & Papaioannou, D. (2011). 'Systematic Approaches to a Successful Literature Review', 2nd ed. Sage Publications, viewed Jan 2012, <https://www.researchgate.net/publication/235930866_Systematic_Approaches_to_a_Successful_Literature_Review>.

Bouchard, M., & Malm, A. (2016). 'Social Network Analysis and Its Contribution to Research on Crime and Criminal Justice', In Oxford Handbooks Online ed., Oxford University Press, viewed Nov. 2016, <https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199935383.001.0001/oxfordhb-9780199935383-e-21>.

Brandes, U., Gaertler, M., & Wagner, D. (2003), 'Experiments on Graph Clustering Algorithms', In Proceedings of the ESA 2003, Budapest, Hungary, 16–19 Sep. 2003, Springer Berlin Heidelberg, pp. 568–579.

Branting, L. K., Reeder, F., Gold, J., & Champney, T. (2016), 'Graph analytics for healthcare fraud risk estimation', ASONAM 2016, IEEE, viewed 24 Nov. 2016, <https://doi.org/10.1109/ASONAM.2016.7752336>.

Brantingham, P., Brantingham, P. L., & Andresen, M. (2016). 'The geometry of crime and crime pattern theory', In R. Wortley & M. Townsley (Eds.), Environmental Criminology and Crime Analysis, Routledge, London, pp. 98–115, viewed 3 Nov. 2016, <https://doi.org/10.4324/9781315709826>.

Brantingham, P. L. (2010). 'Crime Pattern Theory', In B. S. Fisher & S. P. Lab (Eds.), Encyclopedia of Victimology and Crime Prevention, SAGE Publications, Thousand Oaks, California, viewed 23 Mar. 2010, <http://sk.sagepub.com/reference/victimologyandcrime>.

Brantingham, P. L., & Brantingham, P. (1993). 'Environment, Routine, and Situation: Toward a Pattern Theory of Crime: Advances in Criminological Theory', In R. V. Clarke & M. Felson (Eds.), Routine Activity and Rational Choice, 1st ed., pp.

259–294.

Bright, D., Greenhill, C., Britz, T., Ritter, A., & Morselli, C., (2017), 'Criminal network vulnerabilities and adaptations', *Global Crime*, vol. 18, no. 4, pp. 424–441.

Bright, D., Whelan, C. B., & Morselli, C., (2020), 'Understanding the structure and composition of co-offending networks in Australia', *Trends & issues in crime and criminal justice*, vol. 1, no. 597, pp. 1–21.

Broccatelli, C., (2017), 'Going Beyond Secrecy: Methodological Advances for Two-mode Temporal Criminal Networks with Social Network Analysis', Doctor of Philosophy, The University of Manchester, Manchester, <https://www.escholar.manchester.ac.uk/item/?pid=uk-ac-man-scw:307642>.

Bródka, P., & Grecki, T., (2016), '*mLFR Benchamark: Testing Community Detection Algorithms in Multilayer, Multiplex and Multiple Social Networks*', viewed Aug. 2020, < https://github.com/pbrodka/mLFR-benchmark>.

Bursik , R. J., (1988), 'SOCIAL DISORGANIZATION AND THEORIES OF CRIME AND DELINQUENCY: PROBLEMS AND PROSPECTS', *Criminology*, vol. 26, no. 4, pp. 519–552.

Burt, R. S. (2005). 'Brokerage and Closure: An Introduction to Social Capital', Kindle ed. Oxford University Press, Oxford, New York, viewed 6 Sep. 2006.

Cai, H., Zheng, V. W., & Chen-Chuan Chang, K., (2017), 'A Comprehensive Survey of Graph Embedding: Problems, Techniques and Applications', *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 9, pp. 1616–1637.

Calderoni, F. (2014). 'Social Network Analysis of Organized Criminal Groups', In G. Bruinsma & D. Weisburd (Eds.), Encyclopedia of Criminology and Criminal Justice, Springer New York, New York, NY, pp. 4972–4981, <https://doi.org/10.1007/978-1-4614-5690-2_239>.

Calderoni, F., Catanese, S., De Meo, P., Ficara, A., & Fiumara, G., (2020), 'Robust link prediction in criminal networks: A case study of the Sicilian Mafia', *Expert Systems with Applications*, vol. 161, no. 113666, pp. 1–11.

Campana, P., & Varese, F., (2012), 'Listening to the wire: criteria and techniques for the quantitative analysis of phone intercepts', *Trends in Organized Crime*, vol. 15, no. 1, pp. 13–30.

Canu, M., Detyniecki, M., Lesot, M., & d'Allonnes, A. R. (2015), 'Fast community structure local uncovering by independent vertex-centred process', In Proceedings of the ASONAM 2015, Paris, France, 25–28 Aug. 2015, IEEE, pp. 823–830.

Carrington, P. J. (2011). 'Crime and Social Network Analysis', In J. Scott & P. J.

Carrington (Eds.), The Sage handbook of social network analysis, SAGE Publications, London, pp. 236–255, <http://sk.sagepub.com/reference/the-sage-handbook-of-social-network-analysis>.

Carrington, P. J. (2014a). 'Co-offending', In G. Bruinsma & D. Weisburd (Eds.), Encyclopedia of Criminology and Criminal Justice, Springer New York, New York, NY, pp. 548–558, <https://doi.org/10.1007/978-1-4614-5690-2_108>.

Carrington, P. J., (2014b), 'The Structure of Age Homophily in Co-Offending Groups', *Journal of Contemporary Criminal Justice*, vol. 31, no. 3, pp. 337–353.

Carson, J. V., Dugan, L., & Yang, S.-M., (2020), 'A Comprehensive Application of Rational Choice Theory: How Costs Imposed by, and Benefits Derived from, the U.S. Federal Government Affect Incidents Perpetrated by the Radical Eco-Movement', *Journal of Quantitative Criminology*, vol. 36, pp. 701–724.

Carter, J., Louderback, E. R., Vildosola, D., & Sen Roy, S., (2020), 'Crime in an Affluent City: Spatial Patterns of Property Crime in Coral Gables, Florida', *European Journal on Criminal Policy and Research*, vol. 26, pp. 547–570

Carvalho, L. F. M., Teixeira, C. H. C., Meira , W., Ester, M., Carvalho, O., & Brandao, M. H. (2017), 'Provider-Consumer Anomaly Detection for Healthcare Systems', ICHI 2017, IEEE, viewed 14 September 2017, <https://doi.org/10.1109/ICHI.2017.75>.

Cavallari, S., Zheng, V. W., Cai, H., Chang, K. C.-C., & Cambria, E. (2017), 'Learning Community Embedding with Community Detection and Node Embedding on Graphs', CIKM 2017, Association for Computing Machinery, viewed Nov. 2017, <https://doi.org/10.1145/3132847.3132925>.

Cavallaro, L., Ficara, A., Meo, P. D., Fiumara, G., Catanese, S., Bagdasar, O., & Liotta, A., (2020), 'Disrupting Resilient Criminal Networks through Data Analysis: The case of Sicilian Mafia', *arXiv*, vol. abs/2003.05303, pp. 1–12.

Chamberlain, B. P., Levy-Kramer, J., Humby, C., & Deisenroth, M. P., (2018), 'Real-time community detection in full social networks on a laptop', *PloS One*, vol. 13, no. 1, p. e0188702.

Chan, T. K. H., Cheung, C. M. K., & Lee, Z. W. Y., (2017), 'The state of online impulse-buying research: A literature analysis', *Information & Management*, vol. 54, no. 2, pp. 204–217.

Chandola, V., Banerjee, A., & Kumar, V., (2009), 'Anomaly detection: A survey', *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58.

Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., & Schroeder, J., (2003), 'COPLINK: managing law enforcement data and knowledge', *Communications of the ACM*, vol. 46, no. 1, pp. 28–34.

Cherifi, H., Palla, G., Szymanski, B. K., & Lu, X., (2019), 'On community structure in complex networks: challenges and opportunities', *Applied Network Science*, vol. 4, no. 117, pp. 1–35.

Choi, K.-S. (2008). 'Risk Factors in Computer-Crime Victimization'. LFB Scholarly Publishing, United States.

Choi, K.-S., Earl, K., Lee, J. R., & Cho, S., (2019), 'Diagnosis of cyber and non-physical bullying victimization: A lifestyles and routine activities theory approach to constructing effective preventative measures', *Computers in Human Behavior*, vol. 92, pp. 11–19.

Choi, K.-S., Lee, S. S., & Lee, J. R., (2017), 'Mobile phone technology and online sexual harassment among juveniles in South Korea: Effects of self-control and social learning', *International Journal of Cyber Criminology*, vol. 11, pp. 110–127.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S., (2012), 'Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?', *IEEE Trans. on Dependable and Secure Computing*, vol. 9, no. 6, pp. 811–824.

Chun, W., Shirui, P., Ruiqi, H., Guodong, L., Jing, J., & Chengqi, Z. (2019), 'Attributed Graph Clustering: A Deep Attentional Embedding Approach', In Proceedings of the IJCAI 2019, Macao, China, 10–16 Aug. 2019, pp. 1–7.

Cohen, L. E., & Felson, M., (1979), 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review*, vol. 44, no. 4, pp. 588–608.

Conradt, C., (2012), 'Online auction fraud and criminological theories: The Adrian Ghighina case', *International Journal of Cyber Criminology*, vol. 6, pp. 912–923.

Cook, S. A., (1983), 'An overview of computational complexity', *Communications of the ACM*, vol. 26, no. 6, pp. 400–408.

Cornish, D. B., & Clarke, R. V. G. (eds), (2014), 'The reasoning criminal : rational choice perspectives on offending',1st ed., Springer-Verlag, New York, viewed 25 Oct. 2017, <https://doi.org/10.4324/9781315134482>.

Cortes, C., & Vapnik, V. N., (1995), 'Support-vector networks', *Machine Learning*, vol. 20, no. 3, pp. 273–297.

Courtney, B., (2018), 'A Simple Risk Terrain Model for Burglary in Colorado Springs', Master of Art, University of Colorado, viewed May 2018, <https://hdl.handle.net/10976/166913>.

Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M., (2015), 'Fame for sale: Efficient detection of fake Twitter followers', *Decision Support Systems*, vol. 80, pp. 56–71.

Crossley, N., Edwards, G., Harries, E., & Stevenson, R., (2012), 'Covert social movement networks and the secrecy-efficiency trade off: The case of the UK suffragettes (1906–1914)', *Social Networks*, vol. 34, no. 4, pp. 634–644.

Cunningham, D., Everton, S., & Murphy, P. (2016). 'Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis ', 1 st ed. Rowman & Littlefield, viewed 7 Mar. 2016.

Cunningham, D., Everton, S., Wilson, G., Padilla, C., & Zimmerman, D., (2013), 'Brokers and Key Players in the Internationalization of the FARC', *Studies in Conflict & Terrorism*, vol. 36, no. 6, pp. 477–502.

Dai, H., Zhu, F., Lim, E. P., & Pang, H. (2012), 'Detecting Anomalies in Bipartite Graphs with Mutual Dependency Principles', ICDM 2012, IEEE, viewed 17 January 2013, <https://doi.org/10.1109/ICDM.2012.167>.

Dang, Q., Zhou, Y., Gao, F., & Sun, Q., (2017), 'Detecting cooperative and organized spammer groups in micro-blogging community', *Data Mining and Knowledge Discovery*, vol. 31, no. 3, pp. 573–605.

Davis, J., & Goadrich, M. (2006), 'The relationship between Precision-Recall and ROC curves', In Proceedings of the ICML 2006, Pittsburgh, Pennsylvania, USA, 25–29 June 2006 ACM, , pp. 233–240.

Davis, P. K., & Cragin, K. (eds), (2009), 'Social Science for Counterterrorism: Putting the Pieces Together', RAND Corporation, Santa Monica, Canada, <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG849.pdf>.

De Domenico, M., Lancichinetti, A., Arenas, A., & Rosvall, M., (2015), 'Identifying Modular Flows on Multilayer Networks Reveals Highly Overlapping Organization in Interconnected Systems', *Physical Review*, vol. 5, no. 1, p. 011027.

Debajit, S., & Samar, S. S., (2015), 'A Survey on Different Graph Based Anomaly Detection Techniques', *Indian Journal of Science and Technology*, vol. 8, no. 32, pp. 1–7.

Dickison, M. E., Magnani, M., & Rossi, L. (2016). 'Multilayer Social Networks'. Cambridge University Press, Cambridge, Cambridge Core database, <https://www.cambridge.org/core/books/multilayer-social-networks/39383306D9843313057CECEBF7B9BF26>.

Didier, G., Valdeolivas, A., & Baudot, A., (2018), 'Identifying communities from multiplex biological networks by randomized optimization of modularity', *F1000Research*, vol. 7, pp. 1042–1042.

Didimo, W., Liotta, G., & Montecchiani, F., (2014), 'Network visualization for financial crime detection', *Journal of Visual Languages & Computing*, vol. 25, no. 4, pp.

433–451.

Drula, G., (2012), 'Social and online media research – data, metrics and methods', *Review of Applied Socio-Economic Research*, vol. 3, no. 1, pp. 1–11.

Duijn, P., (2017), 'Detecting and Disrupting Criminal Networks; A data-driven approach', Doctor of Philosophy, University of Amsterdam, <https://dare.uva.nl/search?identifier=447f10ad-cecf-4b95-9f8b-7cb97e84eac0>.

Duijn, P., & Sloot, P., (2015), 'From data to disruption', *Digital Investigation*, vol. 15, pp. 39–45.

Eberle, W., & Holder, L. (2007), 'Discovering structural anomalies in graph-based data', ICDMW 2007, IEEE, viewed 31 March 2008, <https://doi.org/10.1109/ICDMW.2007.91>.

Eberle, W., & Holder, L. (2009), 'Mining for insider threats in business transactions and processes', CIDM 2009, IEEE, viewed 15 May 2009, <https://doi.org/10.1109/CIDM.2009.4938645>.

Eck, J., & Weisburd, D., (1995), 'Crime Places in Crime Theory', *Crime and Place, Crime Prevention Studies*, vol. 4, pp. 1–33.

Emig, M. N., Kravitz, M., & Heck, R. O. (1980). 'Crime Analysis: A Selected Bibliography'. The Institute, Washington, DC, <https://catalog.hathitrust.org/Record/002567908>.

Emmons, S., Kobourov, S., Gallant, M., & Börner, K., (2016), 'Analysis of Network Clustering Algorithms and Cluster Quality Metrics at Scale', *PloS One*, vol. 11, no. 7, p. e0159161.

Eom, C. S. H., Lee, W., & Lee, J. J. H. (20116), 'Spammer Detection for Real-Time Big Data Graphs', In Proceedings of the EDB 2016, Jeju Island, Republic of Korea, 17–19 Oct. 2016 ACM, pp. 51–60.

Erickson, B. H., (1981), 'Secret Societies and Social Structure', *Social Forces*, vol. 60, no. 1, pp. 188–210.

Eriksson, K. H., Hjalmarsson, R., Lindquist, M. J., & Sandberg, A., (2016), 'The importance of family background and neighborhood effects as determinants of crime', *Journal of Population Economics*, vol. 29, no. 1, pp. 219–262.

Everton, S. S., (2008), 'Tracking, Destabilizing and Disrupting Dark Networks with Social Networks Analysis', Doctor of Philosophy, Naval Postgraduate School, California, USA, Calhoun database, <http://hdl.handle.net/10945/34415>.

Eze, B., & Peyton, L., (2015), 'Systematic Literature Review on the Anonymization of High Dimensional Streaming Datasets for Health Data Sharing', *Procedia*

Computer Science, vol. 63, pp. 348–355.

Fakhraei, S., Foulds, J., Shashanka, M., & Getoor, L. (2015), 'Collective Spammer Detection in Evolving Multi-Relational Social Networks', In Proceedings of the ACM SIGKDD 2015, Sydney, NSW, Australia, 10–13 Aug. 2015 ACM, pp. 1769–1778.

Fanaee, H., & Gama, J., (2014), 'Event labeling combining ensemble detectors and background knowledge', *Progress in Artificial Intelligence*, vol. 2, no. 2, pp. 113-127.

Faust, K., & Tita, G., (2019), 'Social Networks and Crime: Pitfalls and Promises for Advancing the Field', *Annual Review of Criminology*, vol. 2, pp. 99–122.

Fei, Z., & Geoffrey, I. W. (2010). 'Tree Augmented Naive Bayes', In C. Sammut & G. I. Webb (Eds.), Encyclopedia of Machine Learning, Springer, USA, pp. 990–991, <https://doi.org/10.1007/978-0-387-30164-8_850>.

Ferrara, E., De Meo, P., Catanese, S., & Fiumara, G., (2014), 'Detecting criminal organizations in mobile phone networks', *Expert Systems with Applications*, vol. 41, no. 13, pp. 5733–5750.

Fortunato, S., (2010), 'Community detection in graphs', *Physics Reports*, vol. 486, no. 3, pp. 75–174.

Fortunato, S., & Barthelemy, M., (2007), 'Resolution limit in community detection', *Proceedings of the National Academi of Sciences of the United States*, vol. 104, no. 1, pp. 36–41.

Fronzetti Colladon, A., & Remondi, E., (2017), 'Using social network analysis to prevent money laundering', *Expert Systems with Applications*, vol. 67, pp. 49–58.

Frost, R. B., & Choo, C. W., (2017), 'Revisiting the information audit: A systematic literature review and synthesis', *International Journal of Information Management*, vol. 37, no. 1, pp. 1380–1390.

Gaertler, M. (2005). 'Clustering', In U. Brandes & T. Erlebach (Eds.), Network Analysis: Methodological Foundations, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 178–215, <ttps://doi.org/10.1007/978-3-540-31955-9_8>.

Gallupe, O., Bouchard, M., & Davies, G., (2015), 'Image is everything: Delinquent displays and social status among adolescents', *Canadian Journal of Criminology and Criminal Justice*, vol. 57, pp. 439–474.

Gallupe, O., & Gravel, J., (2018), 'Social Network Position of Gang Members in Schools: Implications for Recruitment and Gang Prevention', *Justice Quarterly*, vol. 35, no. 3, pp. 505–525.

Galvan, G., & Agarwal, J., (2018), 'Community Detection in Action: Identification of Critical Elements in Infrastructure Networks', *Journal of Infrastructure Systems*, vol. 24, no. 1, p. 04017046.

Gamachchi, A., & Boztaş, S. (2015), 'Web access patterns reveal insiders behavior', IWSDA 2015, IEEE, viewed 25 April 2016, <https://doi.org/10.1109/IWSDA.2015.7458417>.

Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y. 'Detecting and characterizing social spam campaigns', In Proceedings of the IMC 2010, Blagoevgrad, Bulgaria, 24–30 July 2010, ACM, pp. 35–47.

García-Pérez, G., Boguñá, M., & Serrano, M. Á., (2015), 'Regulation of burstiness by network-driven activation', *Scientific Reports*, vol. 5, pp. 1–5.

Gera, R., Miller, R., Saxena, A., MirandaLopez, M., & Warnke, S. (2017), 'Three is The Answer: Combining Relationships to Analyze Multilayered Terrorist Networks', ASONAM 2017, IEEE, viewed 16 Apr. 2020, <https://ieeexplore.ieee.org/document/9069153>.

Gerstner, D., & Oberwittler, D., (2018), 'Who's hanging out and what's happening? A look at the interplay between unstructured socializing, crime propensity and delinquent peers using social network data', *European Journal of Criminology*, vol. 15, pp. 111–129.

Giatsoglou, M., Chatzakou, D., Shah, N., Faloutsos, C., & Vakali, A. (2015), 'Retweeting Activity on Twitter: Signs of Deception', PAKDD 2015, Springer International Publishing, viewed 17 April 2015, <https://doi.org/10.1007/978-3-319-18038-0_10>.

Gilmour, N., (2016), 'Understanding the practices behind money laundering – A rational choice interpretation', *International Journal of Law, Crime and Justice*, vol. 44, pp. 1–13.

Glueck, S., & Glueck, E. (1950). 'Unraveling Juvenile delinquency'. Commonwealth Fund, <https://psycnet.apa.org/record/1951-02578-000>.

Goix, N., (2016), 'How to Evaluate the Quality of Unsupervised Anomaly Detection Algorithms?', *arXiv*, vol. abs/1607.01152, pp. 1–13.

Goyal, P., & Ferrara, E., (2018), 'Graph Embedding Techniques, Applications, and Performance: A Survey', *Knowledge Based Systems*, vol. 151, pp. 78–94.

Gravel, J., & Tita , G. E. (2017). 'Network Perspectives on Crime ', In Oxford Research Encyclopedia of Criminology, Oxford University Press, pp. 1–42, <https://doi.org/10.1093/acrefore/9780190264079.013.251>.

Grover, A., & Leskovec, J. (2016), 'node2vec: Scalable Feature Learning for Networks', In Proceedings of the SIGKDD 2016, San Francisco, California,

USA, 13–17 Aug. 2016, ACM, pp. 855–864.

Grund, T. U., & Densley, J. A., (2012), 'Ethnic heterogeneity in the activity and structure of a Black street gang', *European Journal of Criminology*, vol. 9, pp. 388–406.

Grund, T. U., & Densley, J. A., (2014), 'Ethnic Homophily and Triad Closure: Mapping Internal Gang Structure Using Exponential Random Graph Models', *Journal of Contemporary Criminal Justice*, vol. 31, no. 3, pp. 354–370.

Hajiseyedjavadi, S., Lin, Y.-R., & Pelechrinis, K., (2019), 'Learning embeddings for multiplex networks using triplet loss', *Applied Network Science*, vol. 4, pp. 1–16.

Hamilton, W. L., Ying, R., & Leskovec, J., (2017), 'Representation Learning on Graphs: Methods and Applications', *IEEE Data Engineering Bulletin*, vol. 40, pp. 52–74.

Han, X., Wang, L., Xu, S., Zhao, D., & Liu, G., (2019), 'Recognizing roles of online illegal gambling participants: An ensemble learning approach', *Computers & Security*, vol. 87, pp. 1–11.

Hanneman, R. A., & Riddle, M. (2011). 'Concepts and measures for basic network analysis', In J. Scott & P. J. Carrington (Eds.), The Sage handbook of social network analysis, SAGE Publications, pp. 340–369, <https://dx.doi.org/10.4135/9781446294413.n24>.

Harper, W. R., & Harris, D. H., (1975), 'The Application of Link Analysis to Police Intelligence', *Human Factors*, vol. 17, no. 2, pp. 157–164.

Hartel, P., Junger, M., & Wieringa, R., (2010), 'Cyber-crime Science = Crime Science + Information Security', C. f. T. a. I. T. (CTIT), Enschede, <https://research.utwente.nl/en/publications/cyber-crime-science-crime-science-information-security>.

Hawdon, J., (2012), 'Applying Differential Association Theory to Online Hate Groups: A Theoretical Statement', *Journal of Research on Finnish Society*, vol. 5, pp. 39–47.

Haynie, D. L., (2001), 'Delinquent Peers Revisited: Does Network Structure Matter?', *American Journal of Sociology*, vol. 106, no. 4, pp. 1013–1057.

Haynie, D. L., Doogan, N. J., & Soller, B., (2014), 'GENDER, FRIENDSHIP NETWORKS, AND DELINQUENCY: A DYNAMIC NETWORK APPROACH', *Criminology*, vol. 52, no. 4, pp. 688–722.

Haynie, D. L., & Osgood, D. W., (2005), 'Reconsidering Peers and Delinquency: How do Peers Matter?', *Social Forces*, vol. 84, no. 2, pp. 1109–1130.

Haynie, D. L., & Soller, B. (2014). 'Network Analysis in Criminology', In G. Bruinsma

& D. Weisburd (Eds.), Encyclopedia of Criminology and Criminal Justice, Springer New York, New York, NY, pp. 3265–3275, <https://doi.org/10.1007/978-1-4614-5690-2_237>.

He, X., Cai, D., & Niyogi, P. (2005), 'Laplacian score for feature selection', In Proceedings of the NIPS 05, Vancouver, British Columbia, Canada, 5–8, Dec. 2005 MIT Press, pp. 507–514.

Herath, T., & D'Arcy, J. 'Social Networking Behaviors: Role of personality, perceived risk, and social influences', In Proceedings of the CONF-IRM 2015, Ottawa, Ontario, Canada, 18–20 May 2015, AIS Electronic Library, pp. 1–9.

Hevner, A., (2007), 'A Three Cycle View of Design Science Research', *Scandinavian Journal of Information Systems*, vol. 19, no. 2, pp. 87–92.

Hevner, A., T. March, S., Park, J., & Ram, S., (2004), 'Design science in information systems research', *MIS Quaterly*, vol. 28, no. 1, pp. 75–105.

Hewitt, A. N., Beauregard, E., Andresen, M. A., & Brantingham, P. L., (2018), 'Identifying the nature of risky places for sexual crime: The applicability of crime pattern and social disorganization theories in a Canadian context', *Journal of Criminal Justice*, vol. 57, pp. 35–46.

Higgins, E. M., & Swartz, K., (2018), 'Edgeways as a theoretical extension: connecting crime pattern theory and New Urbanism', *Crime Prevention and Community Safety*, vol. 20, no. 1, pp. 1–15.

Hinduja, S., & Schafer, J., (2009), 'US cybercrime units on the world wide web', *Policing: An International Journal of Police Strategies and Management*, vol. 32, no. 2, pp. 278–296.

Hmimida, M., & Kanawati, R., (2015), 'Community detection in multiplex networks: A seed-centric approach', *Networks and Heterogeneous Media*, vol. 10, pp. 71–85.

Holmes, L., (2009), 'Good guys, bad guys: transnational corporations, rational choice theory and power crime', *Crime, Law and Social Change*, vol. 51, no. 3, pp. 383–397.

Home Office, (2020), 'The National Crime Agency: Leading the UK's fight to cut serious and organised crime', <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/289-nca-annual-plan-2019-20>.

Hongming Zhang, Liwei Qiu, Lingling Yi, & Song, Y. (2018), 'Scalable Multiplex Network Embedding', In Proceedings of the IJCAI 2018, Stockholm, Sweden, 13–19 July 2018, pp. 3082–3088.

Hooi, B., Shin, K., Song, H. A., Beutel, A., Shah, N., & Faloutsos, C., (2017), 'Graph-based fraud detection in the face of camouflage', *ACM Transactions on*

Knowledge Discovery, vol. 11, no. 4, pp. 1–26.

Hosseinkhani, J., Chuprat, S., & Taherdoost, H. 'Discovering criminal networks by Web structure mining', In Proceedings of the ICCCT 2017, 3–5 Dec. 2012, IEEE, pp. 1074–1079.

Hu, X., Tang, J., & Liu, H. (2014), 'Online social spammer detection', In Proceedings of the AAAI 2014, Québec City, Québec, Canada, 27– 31 July 2014, AAAI Press, pp. 59–65.

Huang, D., Mu, D., Yang, L., & Cai, X., (2018), 'CoDetect: Financial Fraud Detection With Anomaly Feature Detection', *IEEE Access*, vol. 6, pp. 19161–19174.

Hulst, R. C. v. d., (2009), 'Introduction to Social Network Analysis (SNA) as an investigative tool', *Trends in Organized Crime*, vol. 12, no. 2, pp. 101–121.

Hutchings, A., & Hayes, H., (2009), 'Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?', *Current Issues in Criminal Justice*, vol. 20, no. 3, pp. 433–452.

Interdonato, R., Tagarelli, A., Ienco, D., Sallaberry, A., & Poncelet, P., (2017), 'Local community detection in multilayer networks', *Data Mining and Knowledge Discovery*, vol. 31, no. 5, pp. 1444–1479.

International Crisis Group, (2006), 'Terrorism in Indonesia : Noordin's networks', I. C. Group, Jakarta.

Jeni, L. A., Cohn, J. F., & De La Torre, F. (2013), 'Facing Imbalanced Data Recommendations for the Use of Performance Metrics', ACII 2013, IEEE, viewed 12 Dec. 2013, <https://ieeexplore.ieee.org/document/6681438>.

Jensen, T. R., & Toft, B. (1994). 'Graph Coloring Problems'. John Wiley & Sons, viewed 3 Dec. 1994, <https://onlinelibrary.wiley.com/doi/book/10.1002/9781118032497>.

Jeub, L. G. S., Mahoney, M. W., Mucha, P. J., & Porter, M. A., (2017), 'A local perspective on community structure in multilayer networks', *Network Science*, vol. 5, no. 2, pp. 144–163.

Jiang, M., Cui, P., Beutel, A., Faloutsos, C., & Yang, S. (2014), 'CatchSync: catching synchronized behavior in large directed graphs', In Proceedings of the SIGKDD 2014, New York, USA, 24 –27 Aug. 2014 ACM, pp. 941–950.

Jiang, M., Cui, P., Beutel, A., Faloutsos, C., & Yang, S., (2016), 'Catching Synchronized Behaviors in Large Networks: A Graph Mining Approach', *ACM Transactions on Knowledge Discovery from Data*, vol. 10, no. 4, pp. 1–27.

Jindal, A., Madden, S., Castellanos, M., & Hsu, M. (2015), 'Graph analytics using vertica relational database', IEEE International Conference on Big Data, IEEE,

viewed 28 Sep. 2015, <https://doi.org/10.1109/BigData.2015.7363873>.

Johnson, S. D., (2014), 'How do offenders choose where to offend? Perspectives from animal foraging', *Legal and Criminological Psychology*, vol. 19, no. 2, pp. 193–210.

Jose, R., Hipp, J. R., Butts, C. T., Wang, C., & Lakon, C. M., (2016), 'Network Structure, Influence, Selection, and Adolescent Delinquent Behavior:Unpacking a Dynamic Process', *Criminal Justice and Behavior*, vol. 43, no. 2, pp. 264–284.

Kajeepeta, S., Theall, K. P., Kondo, M. C., Branas, C. C., Wallace, M. E., Jacoby, S. F., & Morrison, C. N., (2020), 'The association between blighted property remediation and domestic crime by alcohol availability', *Health & Place*, vol. 64, no. 102364, pp. 1–8.

Kao, D.-Y. (2014), 'Rational Choice Observation of Malware Authors in Taiwan', In Proceedings of the PAISI 2014, Tainan, Taiwan, 13 May 2014, Intelligence and Security Informatics, Springer International Publishing, pp. 1–7.

Kariin, S., & Burge, C., (1995), 'Dinucleotide relative abundance extremes: a genomic signature', *Trends in Genetics*, vol. 11, no. 7, pp. 283–290.

Karim, M. R., & Zilles, S. (2014), 'Robust Features for Detecting Evasive Spammers in Twitter', Canadian AI 2014, Springer, Cham, viewed May 2014, <https://doi.org/10.1007/978-3-319-06483-3_28>.

Karmen, A. (1984). 'Crime victims: An introduction to victimology', 18th ed. Brooks/Cole Publishing, Monterey, Calif.

Karsai, M., Jo, H. H., & Kaski, K. (2018). 'Bursty Human Dynamics'. Springer International Publishing, Cham, <https://doi.org/10.1007/978-3-319-68540-3_1>.

Kasarda, J., & Janowitz, M., (1974), 'Community Attachment in Mass Society', *American Sociological Review*, vol. 39, no. 3, pp. 328–339.

Kaveh, A. (2013). 'Introduction to Graph Theory and Algebraic Graph Theory', In Optimal Analysis of Structures by Concepts of Symmetry and Regularity, 1 ed., Springer, Vienna, pp. 15–35, viewed 19 March 2013, <https://doi.org/10.1007/978-3-7091-1565-7_2>.

Keikha, M. M., Rahgozar, M., & Asadpour, M., (2019), 'DeepLink: A novel link prediction framework based on deep learning', *Journal of Information Science*, vol., pp. 1–19.

Kennedy, B. P., Kawachi, I., Prothrow-Stith, D., Lochner, K., & Gupta, V., (1998), 'Social capital, income inequality, and firearm violent crime', *Social science & medicine*, vol. 47, no. 1, pp. 7–17.

Kim, E.-K., & Jo, H.-H., (2016), 'Measuring burstiness for finite event sequences', *Physical Review E*, vol. 94, no. 3, p. 032311.

Kivelä, M., Arenas, A., Barthelemy, M., P. Gleeson, J., Moreno, Y., & A. Porter, M., (2014), 'Multilayer networks', *Journal of Complex Networks*, vol. 2, no. 3, pp. 203–271.

Klein, J. L., & Cooper, D. T., (2019), 'Deviant Cyber-Sexual Activities in Young Adults: Exploring Prevalence and Predictions Using In-Person Sexual Activities and Social Learning Theory', *Archives of Sexual Behavior*, vol. 48, no. 2, pp. 619–630.

Kobayashi, T., & Masuda, N., (2016), 'Fragmenting networks by targeting collective influencers at a mesoscopic level', *Scientific Reports*, vol. 6, pp. 1–12.

Kreager, D. A., Rulison, K., & Moody, J., (2011), 'DELINQUENCY AND THE STRUCTURE OF ADOLESCENT PEER GROUPS*', *Criminology*, vol. 49, no. 1, pp. 95–127.

Krebs, V., (2002), 'Mapping Networks of Terrorist Cells', *Connections*, vol. 24, no. 43, pp. 43–52.

Kubrin, C., & Weitzer, R., (2003), 'New Directions in Social Disorganization Theory', *Journal of Research in Crime and Delinquency*, vol. 40, no. 4, pp. 374–402.

Kuncheva, Z., & Montana, G. 'Community Detection in Multiplex Networks using Locally Adaptive Random Walks', In Proceedings of the ASONAM 2015, Paris, France, 25–28 Aug. 2015 ACM, pp. 1308–1315.

Lamba, H., Hooi, B., Shin, K., Faloutsos, C., & Pfeffer, J. (2017), 'ZooRank: Ranking Suspicious Entities in Time-Evolving Tensors', In Proceedings of the ECML PKDD 2017, SKOPJE, MACEDONIA, 18–22 Sep. 2017, Machine Learning and Knowledge Discovery in Databases, Springer International Publishing, pp. 68–84.

Lancichinetti, A., & Fortunato, S., (2009), 'Community detection algorithms: A comparative analysis', *Physical Review E*, vol. 80, no. 5, p. 056117.

Lancichinetti, A., Fortunato, S., & Radicchi, F., (2008), 'Benchmark graphs for testing community detection algorithms', *Physical review E*, vol. 78, no. 4, p. 046110.

Lee, L.-F., Liu, X., Patacchini, E., & Zenou, Y., (2020), 'Who is the Key Player? A Network Analysis of Juvenile Delinquency', *Journal of Business & Economic Statistics*, vol., pp. 1–9.

Lee, S., Park, S., Kahng, M., & Lee, S.-g., (2013), 'PathRank: Ranking nodes on a heterogeneous graph for flexible hybrid recommender systems', *Expert Systems with Applications*, vol. 40, no. 2, pp. 684–697.

Leuprecht, C., & Hall, K. (2014). 'Why Terror Networks are Dissimilar: How Structure Relates to Function', In A. J. Masys (Ed.), Networks and Network Analysis for Defence and Security. Lecture Notes in Social Networks, Springer, Cham, pp. 83–120, <https://doi.org/10.1007/978-3-319-04147-6_5>.

Levin, R., Richardson, J., Warner, G., & Kerley, K. (2012), 'Explaining Cybercrime through the Lens of Differential Association Theory, Hadidi44-2.php PayPal Case Study', In Proceedings of the 2012 eCrime Researchers Summit, Las Croabas, Puerto Rico, 23–24 Oct. 2012, IEEE, pp. 1–7.

Li, T., Zhang, J., Yu, P. S., Zhang, Y., & Yan, Y., (2018), 'Deep Dynamic Network Embedding for Link Prediction', *IEEE Access*, vol. 6, pp. 29219–29230.

Li, Z., Xiong, H., & Liu, Y., (2012), 'Mining blackhole and volcano patterns in directed graphs: a general approach', *Data Mining and Knowledge Discovery*, vol. 25, no. 3, pp. 577–602.

Liang, S., Zeng, J., Li, C., & Chen, H. (2010), 'A framework for spotting anomaly', In Proceedings of the FSKD 2010, Yantai, China, 10–12 Aug. 2010, IEEE, pp. 2260–2264.

Liaw, A., & Wiener, M., (2002), 'Classification and Regression by randomFores', *R News*, vol. 2, no. 3, pp. 18–22.

Lim, M., Abdullah, A., Jhanjhi, N., & Khan, M. K., (2020), 'Situation-Aware Deep Reinforcement Learning Link Prediction Model for Evolving Criminal Networks', *IEEE Access*, vol. 8, pp. 16550–16559.

Lim, M., Abdullah, A., Jhanjhi, N. Z., Khan, M. K., & Supramaniam, M., (2019), 'Link Prediction in Time-Evolving Criminal Network With Deep Reinforcement Learning Technique', *IEEE Access*, vol. 7, pp. 184797–184807.

Lima, R. F., & Pereira, A. C. M. (2015), 'A Fraud Detection Model Based on Feature Selection and Undersampling Applied to Web Payment Systems', WI-IAT 2015, IEEE, viewed 04 Feb. 2016, <https://doi.org/10.1109/WI-IAT.2015.13>.

Lindquist, M. J., & Zenou, Y., (2019), 'Crime and networks: ten policy lessons', *Oxford Review of Economic Policy*, vol. 35, no. 4, pp. 746–771.

Liu, G., Wong, L., & Chua, H. N., (2009), 'Complex discovery from weighted PPI networks', *Bioinformatics*, vol. 25, no. 15, pp. 1891–1897.

Liu, Q., Wu, S., & Wang, L., (2017a), 'Multi-Behavioral Sequential Prediction with Recurrent Log-Bilinear Model', *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 6, pp. 1254–1267.

Liu, S., Hooi, B., & Faloutsos, C. (2017), 'HoloScope: Topology-and-Spike Aware Fraud Detection', In Proceedings of the CIKM 2017, Singapore, Singapore, 6–10 Nov. 2017, ACM, pp. 1539–1548.

Liu, T., Li, P., Chen, Y., & Zhang, J., (2016), 'Community Size Effects on Epidemic Spreading in Multiplex Social Networks', *PlosOne*, vol. 11, no. 3, p. e0152021.

Liu, W., Chen, P.-Y., Yeung, S., Suzumura, T., & Chen, L. (2017), 'Principled Multilayer Network Embedding', In Proceedings of the ICDMW 2017, New Orleans, LA, USA, 18–21 Nov. 2017, IEEE, pp. 134–141.

Liu, W., Suzumura, T., Ji, H., & Hu, G., (2018), ' Finding overlapping communities in multilayer networks', *PlosOne*, vol. 13, no. 4, p. e0188747.

Liu, X., Patacchini, E., & Zenou, Y., (2014), 'Endogenous peer effects: local aggregate or local average?', *Journal of Economic Behavior & Organization*, vol. 103, pp. 39–59.

Liu, Z., Wang, C., Zou, Q., & Wang, H. (2010), 'Clustering Coefficient Queries on Massive Dynamic Social Networks', WAIM 2010, Springer, viewed July 2010, <https://doi.org/10.1007/978-3-642-14246-8_14>.

Luan, T., Yan, Z., & Zhang, S. (2019), 'Fraudster Detection Based on Modularity Optimization Algorithm', In Proceedings of the CSCWD 2019, Porto, Portugal, 6–8 May 2019, IEEE, pp. 422–427.

Magalingam, P., Davis, S., & Rao, A., (2015), 'Using shortest path to discover criminal community', *Digital Investigation*, vol. 15, pp. 1–17.

Mallett, R., Hagen-Zanker, J., Slater, R., & Duvendack, M., (2012), 'The benefits and challenges of using systematic reviews in international development research', *Journal of Development Effectiveness*, vol. 4, no. 3, pp. 445–455.

Malm, A., & Bichler, G., (2011), 'Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets', *Journal of Research in Crime and Delinquency*, vol. 48, no. 2, pp. 271–297.

Manjunatha, H. C., & Mohanasundaram, R. (2018), 'BRNADS: Big data real-time node anomaly detection in social networks', In Proceedings of the ICISC 2018, Coimbatore, India, 19–20 Jan. 2018, IEEE, pp. 929–932.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L., (2010), 'Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory', *Deviant Behavior*, vol. 31, no. 5, pp. 381–410.

Masucci, D. J., (2013), 'The Rational Choice Theory and Mexican Drug Activity', *International Journal of Applied Sociology*, vol. 3, no. 5, pp. 89–101.

Matsueda, R. L., (1988), 'The Current State of Differential Association Theory', *Crime & Delinquency*, vol. 34, no. 3, pp. 277–306.

McGlohon, M., Bay, S., G. Anderle, M., M. Steier, D., & Faloutsos, C. (2009), 'SNARE: a link analytic system for graph labeling and risk detection', In Proceedings of

the SIGKDD 2009, Paris, France, 28 June–1 July 2009 ACM, pp. 1265–1274.

McGloin, J., (2005), 'Policy Intervention Considerations of a Network Analysis of Street Gangs', *Criminology & Public Policy*, vol. 4, pp. 607–635.

McGloin, J. M., & Kirk, D. S., (2010), 'An Overview of Social Network Analysis', *Journal of Criminal Justice Education*, vol. 21, no. 2, pp. 169–181.

McQuade, S. C. (2006). 'Understanding and Managing Cyber crime', Policing: An International Journal of Police Strategies and Management. Pearson Education, Boston, MA.

Memon, B. R. (2012), 'Identifying Important Nodes in Weighted Covert Networks Using Generalized Centrality Measures', In Proceedings of the EISIC 2012, Odense, Denmark, 22–24 Aug. 2012, IEEE, pp. 131–140.

Meng, J., Peng, C., Alex, B., Christos, F., & Shiqiang, Y., (2016), 'Catching Synchronized Behaviors in Large Networks: A Graph Mining Approach', *ACM Transactions on Knowledge Discovery from Data*, vol. 10, no. 4, pp. 1–27.

Miró-Llinares, F., & Moneva, A. (2020). 'Environmental Criminology and Cybercrime: Shifting Focus from the Wine to the Bottles', In T. J. Holt & A. M. Bossler (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance, Springer International Publishing, Cham, pp. 491–511, <https://doi.org/10.1007/978-3-319-78440-3_30>.

Mirzal, A., & Furukawa, M., (2010), 'A Method for Accelerating the HITS Algorithm', *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 14, no. 1, pp. 89–98.

Mnih, A., & Hinton, G. (2007), 'Three new graphical models for statistical language modelling', In Proceedings of the ICML 2007, Corvalis Oregon, USA, 20–24 June 2007, ACM, pp. 641–648.

Molloy, I., Chari, S., Finkler, U., Wiggerman, M., Jonker, C., Habeck, T., Park, Y., Jordens, F., & van Schaik, R. (2017), 'Graph Analytics for Real-Time Scoring of Cross-Channel Transactional Fraud', FC 2016, Springer Berlin Heidelberg, viewed 17 May 2017, <https://doi.org/10.1007/978-3-662-54970-4_2>.

Monk, B., Mitchell, J., Frank, R., & Davies, G., (2018), 'Uncovering Tor: An Examination of the Network Structure', *Security and Communication Networks*, vol. 2018, pp. 1–12.

Moradabadi, B., & Meybodi, M. R., (2018), 'Link prediction in weighted social networks using learning automata', *Engineering Applications of Artificial Intelligence*, vol. 70, pp. 16–24.

Moriano, P., & Finke, J. (2014), 'Model-based fraud detection in growing networks', In Proceedings of the CDC 2014, Los Angeles, CA, USA, 15–17 Dec. 2014, IEEE,

pp. 6068–6073.

Morone, F., & Makse, H. A., (2015), 'Influence maximization in complex networks through optimal percolation', *Nature*, vol. 524, no. 7563, pp. 65–68.

Morselli, C. (2009). 'Inside Criminal Networks'. Springer-Verlag, New York, United States.

Morselli, C., & Giguere, C., (2006), 'Legitimate strengths in criminal networks', *Crime Law Soc Change*, vol. 45, no. 3, pp. 185–200.

Morselli, C., Paquet-Clouston, M., & Provost, C., (2017), 'The independent's edge in an illegal drug distribution setting: Levitt and Venkatesh revisited', *Social Networks*, vol. 51, pp. 118–126.

Moscato, V., Picariello, A., & Sperlí, G., (2019), 'Community detection based on Game Theory', *Engineering Applications of Artificial Intelligence*, vol. 85, pp. 773–782.

Murphy, T. (2019). 'Terror and Trafficking in Afghanistan, Pakistan and India: A Routine Activity Approach', In K. Jaishankar (Ed.), Routledge Handbook of South Asian Criminology, 1st ed., Routledge.

Nan, J., Yu, J., Ann, S., Wen-Ling, H., Guy, J., Siva, P., & Zhi-Li, Z. (2012), 'Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis', In Proceedings of the MobiSys 2012, Low Wood Bay, Lake District, UK, 25–29 June 2012, ACM, pp. 253–266.

Natarajan, M., (2006), 'Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data', *Journal of Quantitative Criminology*, vol. 22, pp. 171–192.

Nemeth, S. (2017). 'Rational choice and religious terrorism: Its bases, applications, and future directions', In J. R. Lewis (Ed.), The Cambridge Companion to Religion and Terrorism, Cambridge University Press, Cambridge, pp. 102–115, <https://doi.org/10.1017/9781316492536.008>.

Nettleton, D. F., (2016), 'A synthetic data generator for online social network graphs', *Social Network Analysis and Mining*, vol. 6, no. 44, pp. 1–33.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X., (2011), 'The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature', *Decision Support Systems*, vol. 50, no. 3, pp. 559–569.

Ngai, E. W. T., Xiu, L., & Chau, D. C. K., (2009), 'Application of data mining techniques in customer relationship management: A literature review and classification', *Expert Systems with Applications*, vol. 36, no. 2, Part 2, pp. 2592–2602.

Nicolini, C., Bordiera, C., & Bifonea, A., (2017), 'Community detection in weighted

brain connectivity networks beyond the resolution limit', *NeuroImage*, vol. 146, no. 1, pp. 28–39.

Nikolentzos, G., Meladianos, P., & Vazirgiannis, M. (2017), 'Matching node embeddings for graph similarity', In Proceedings of the AAAI 2017, San Francisco, California, USA, 4–9 Feb. 2017, AAAI, pp. 2429–2435.

Noble, C. C., & Cook, D. J. (2003), 'Graph-based anomaly detection', In Proceedings of the SIGKDD 2003, Washington, D.C., 1–14 Aug. 2003, ACM, pp. 631–636.

Nouh, M., Nurse, J. R. C., & Goldsmith, M. (2016), 'Towards Designing a Multipurpose Cybercrime Intelligence Framework', In Proceedings of the EISIC 2016, Uppsala, Sweden, 17–19 Aug. 2016, IEEE, pp. 60–67.

Novikova, E., & Kotenko, I. (2014), 'Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services', CD-ARES 2014, Springer International Publishing, viewed 1 Jan. 2015, <https://doi.org/10.1007/978-3-319-10975-6_5>.

Ohm, P., (2009), 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review*, vol. 57, pp. 1–77.

Orehek, E., Kruglanski, A., Chen, X., Dechesne, M., & Fishman, S., (2009), 'Fully Committed: Suicide Bombers' Motivation and the Quest for Personal Significance', *Political Psychology*, vol. 30, pp. 331–357.

Overland Park, K., (2018), 'Social Network Analysis for Law Enforcement', <https://crimegunintelcenters.org/wp-content/uploads/2018/07/iacawp_2018_02_social_network_analysis.pdf>.

Page, L., Brin, S., Motwani, R., & Winograd, T., (1999), 'The PageRank Citation Ranking: Bringing Order to the Web', S. I. P. Server, <http://ilpubs.stanford.edu:8090/422/>.

Palm, R. B., Paquet, U., & Winther, O., (2018), 'Recurrent Relational Networks', *arXiv*, vol. abs/1711.08028 pp. 1–22.

Papachristos, A., (2009), 'Murder by Structure: Dominance Relations and the Social Structure of Gang Homicide', *American Journal of Sociology*, vol. 115, no. 1, pp. 74–128.

Papachristos, A., (2013), 'The Importance of Cohesion for Gang Research, Policy, and Practice', *Criminology & Public Policy*, vol. 12, no. 1, pp. 49–58.

Paraskevas, A., & Brookes, M., (2018), 'Nodes, guardians and signs: Raising barriers to human trafficking in the tourism industry', *Tourism Management*, vol. 67, pp. 147–156.

Park, A. J., Tsang, H. H., & Brantingham, P. L. 'Dynalink: A Framework for Dynamic

Criminal Network Visualization', In Proceedings of the 2012 European Intelligence and Security Informatics Conference, 22-24 Aug. 2012, pp. 217-224.

Parker, K. F., & Stansfield, R. (2014). 'Disadvantage, Disorganization and Crime', In G. Bruinsma & D. Weisburd (Eds.), Encyclopedia of Criminology and Criminal Justice, Springer New York, New York, NY, pp. 1084–1093, <https://doi.org/10.1007/978-1-4614-5690-2_432>.

Paternoster, R., & Simpson, S. (1993). 'A Rational Choice Theory of Corporate Crime in Routine activity and rational choice ', In R. V. Clarke & M. Felson (Eds.), Routine Activity and Rational Choice: Advances in Criminological Theory, Transaction Publishers, New Brunswick, NJ pp. 37–58.

Payne, B. K., Hawkins, B., & Xin, C., (2019), 'Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes', *American Journal of Criminal Justice*, vol. 44, no. 2, pp. 230–247.

Peoples, C., & Sutton, J., (2015), 'Congressional bribery as state-corporate crime: a social network analysis', *Crime, Law and Social Change*, vol. 64, pp. 103–125.

Perera, B. K., (2013), 'A Class Imbalance Learning Approach to Fraud Detection in Online Advertising', Master of Science, Masdar Institute of Science and Technology, <http://aungz.com/PDF/KasunPerera_Master_Thesis.pdf>.

Perozzi, B., Al-Rfou, R., & Skiena, S. (2014), 'DeepWalk: online learning of social representations', In Proceedings of the SIGKDD 2014, New York, USA, 24–27 Aug. 2014 ACM, pp. 701–710.

Perry, S., & Hasisi, B., (2015), 'Rational choice rewards and the jihadist suicide bomber', *Terrorism and Political Violence*, vol. 57, no. 1, pp. 53–80.

Peterson, D., Taylor, T., & Esbensen, F.-A., (2004), 'Gang membership and violent victimization', *Justice Quarterly*, vol. 21, pp. 793–815.

Philippe, A., (2017), 'Incarcerate one to calm the others? Spillover effects of incarceration among criminal groups: Job Market Paper', <https://ideas.repec.org/p/tse/wpaper/32042.html>.

Phua, C., Gayler, R., Lee, V., & Smith-Miles, K., (2009), 'On the communal analysis suspicion scoring for identity crime in streaming credit applications', *European Journal of Operational Research*, vol. 195, no. 2, pp. 595–612.

Pinheiro, C. A. R. (2012), 'Community Detection to Identify Fraud Events in Telecommunications Networks', In Proceedings of the SAS Global Forum, pp. 1–8.

Pizarro, J. M., Zgoba, K. M., & Pelletier, K. R., (2020), 'Firearm Use in Violent Crime: Examining the Role of Premeditation and Motivation in Weapon Choice', *The*

Journal of Primary Prevention, vol., pp. 1–15.

Polak, A. (2016), 'Counting Triangles in Large Graphs on GPU', IEEE International Parallel and Distributed Processing Symposium Workshops IEEE, viewed 4 Aug. 2016, <https://doi.org/10.1109/IPDPSW.2016.108>.

Pourhabibi, T., Boo, Y. L., Ong, K. L., Kam, B., & Zhang, X. (2019), 'Behavioral Analysis of Users for Spammer Detection in a Multiplex Social Network', AUSDM 2018, Springer Singapore, viewed 16 February 2019, <https://doi.org/10.1007/978-981-13-6661-1_18>.

Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L., (2020), 'Fraud detection: A systematic literature review of graph-based anomaly detection approaches', *Decision Support Systems*, vol. 133, no. 113303, pp. 1–15.

Pourheidari, A., & Croisdale, T. (2010), 'Understanding criminal co-offending: A historiography of research literature', International Police Executive Symposium, viewed Dec. 2010, <https://ipes.info/WPS/WPS_No_27.pdf>.

Rahman, M., Recabarren, R., Carbunar, B., & Lee, D. (2017), 'Stateless Puzzles for Real Time Online Fraud Preemption', In Proceedings of the WebSci 2017, Troy, New York, USA, 25–28 June 2017 ACM, pp. 23–32.

Rallapalli, S., Ma, L., Srivatsa, M., Swami, A., Kwon, H., Bent, G., & Simpkin, C., (2019), 'SENSE: Semantically Enhanced Node Sequence Embedding', *arXiv preprint arXiv:1911.02970*, vol.

Ranshous, E., Shen, S., Koutra, D., & Harenberg, S., (2015), 'Anomaly detection in dynamic networks: a survey', *Computational Statistics*, vol. 7, no. 3, pp. 223–247.

Rasheed, A., & Wiil, U. K. (2014), 'PEVNET: A framework for visualization of criminal networks', In Proceedings of the ASONAM 2014, Beijing, China, 17–20 Aug. 2014, IEEE, pp. 876–881.

Rashidi, L., (2017), 'Anomaly Detection in Large Evolving Graphs', Doctor of Philosophy, University of Melbourne, <http://hdl.handle.net/11343/194243>.

Rees, C., & Pogarsky, G., (2011), 'One Bad Apple May Not Spoil the Whole Bunch: Best Friends and Adolescent Delinquency', *Journal of Quantitative Criminology*, vol. 27, no. 2, pp. 197-223.

Reiss, A. J., (1986), 'Why Are Communities Important in Understanding Crime?', *Crime and Justice*, vol. 8, pp. 1–33.

Reiss, A. J., & Farrington, D. P., (1991), 'Advancing Knowledge about Co-Offending: Results from a Prospective Longitudinal Survey of London Males', *The Journal of Criminal Law and Criminology*, vol. 82, no. 2, pp. 360–395.

Reyns, B. W., Henson, B., & Fisher, B. S., (2016), 'Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept From Routine Activity Theory as It Applies to Online Forms of Victimization', *Journal of Contemporary Criminal Justice*, vol. 32, no. 2, pp. 148–168.

Ribeiro, L. F. R., Saverese, P. H. P., & Figueiredo, D. R. 'struc2vec: Learning Node Representations from Structural Identity', In Proceedings of the ACM SIGKDD 2017, Halifax, NS, Canada, 13–17 Aug. 2017, ACM, pp. 385–394.

Roberts, N., & Everton, S. (2011). 'The Noordin Top Terrorist Network.', In Disrupting Dark Networks, Structural Analysis in the Social Sciences, Cambridge University Press, Cambridge, pp. 385–396, viewed Apr. 2013, Cambridge Core database, <https://doi.org/10.1017/CBO9781139136877>.

Roberts, N., & Everton, S. (2016). 'Monitoring and Disrupting Dark Networks: A Bias Toward the Center and What It Costs Us', In A. R. Dawoody (Ed.), Eradicating Terrorism from the Middle East. Public Administration, Governance and Globalization, Springer International Publishing, pp. 29–42, viewed 23 Aug. 2016, <https://doi.org/10.1007/978-3-319-31018-3_2>.

Robins, G., (2009), 'Understanding individual behaviors within covert networks: the interplay of individual qualities, psychological predispositions, and network effects', *Trends in Organized Crime*, vol. 12, no. 2, pp. 166–187.

Rocklin, M., & Pinar, A. (2011), 'Latent Clustering on Graphs with Multiple Edge Types', In A. Frieze, P. Horn & P. Prałat (Eds.), In Proceedings of the WAW 2011, Atlanta, GA, USA, 28 May 2011, Springer Berlin Heidelberg, pp. 38–49.

Rosvall, M., Esquivel, A. V., Lancichinetti, A., West, J. D., & Lambiotte, R., (2014), 'Memory in network flows and its effects on spreading dynamics and community detection', *Nature Communications*, vol. 5, no. 1, pp. 1–13.

Roy, A., Kumar, V., Mukherjee, D., & Chakraborty, T. (2020), 'Learning Multigraph Node Embeddings Using Guided Lévy Flights', In H. W. Lauw, R. C.-W. Wong, A. Ntoulas, E.-P. Lim, S.-K. Ng & S. J. Pan (Eds.), In Proceedings of the PAKDD 2020, Online, 11–14 MAY 2020, Springer International Publishing, pp. 524–537.

Rozemberczki, B., Davies, R., Sarkar, R., & Sutton, C. A. (2019), 'GEMSEC: Graph Embedding with Self Clustering', In Proceedings of the ASONAM 2019, Vancouver, Canada 27–30 Aug. 2019, ACM, pp. 65–72.

Rozemberczki, B., & Sarkar, R. (2018), 'Fast Sequence-Based Embedding with Diffusion Graphs', CompleNet 2018, Springer, Cham, viewed 15 Feb. 2018, <https://doi.org/10.1007/978-3-319-73198-8_9>.

Sageman, M. (2004). 'Understanding Terror Networks'. University of Pennsylvania, Philadelphia, USA <https://dl.acm.org/citation.cfm?id=983494>.

Saidi, F., Trabelsi, Z., Salah, K., & Ghezala, H. B., (2017), 'Approaches to analyze cyber terrorist communities: Survey and challenges', *Computers & Security*, vol. 66, pp. 66-80.

Saito, T., & Rehmsmeier, M., (2015), 'The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets', *PloS One*, vol. 10, no. 3, p. e0118432.

Salha, G., Limnios, S., Hennequin, R., Tran, V.-A., & Vazirgiannis, M. (2019), 'Gravity-Inspired Graph Autoencoders for Directed Link Prediction', In Proceedings of the CIKM 2019, Beijing, China, 3–7 Nov. 2019, ACM, pp. 589–598.

Salim, A., Shiju, S. S., & Sumitra, S., (2020), 'Design of multi-view graph embedding using multiple kernel learning', *Engineering Applications of Artificial Intelligence*, vol. 90, p. 103534.

Sampson, R. J., Raudenbush, S. W., & Earls, F. (1998). 'Neighborhood Collective EfficacyDoes It Help Reduce Violence?'. FS 000203, United States of America, viewed Apr. 1998, <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=184377>.

Sarnecki, J., (1990), 'Delinquent networks in Sweden', *Journal of Quantitative Criminology*, vol. 6, no. 1, pp. 31–50.

Sarnecki, J. (2001). 'Delinquent Networks Youth Co-offending in Stockholm'. Cambridge University Press, viewed 8 Jan. 2002.

Satuluri, V., Parthasarathy, S., & Ruan, Y. (2011), 'Local graph sparsification for scalable clustering', In Proceedings of the SIGMOD 2011, Athens, Greece, 12–16 June 2011, ACM, , pp. 721–732.

Savage, D., Zhang, X., Yu, X., Chou, P., & Wang, Q., (2014), 'Anomaly detection in online social networks', *Social Networks*, vol. 39, pp. 62–70.

Saxena, A., Gera, R., Miller, B., & Chakraborty, D. (2018), 'Discovering and leveraging communities in dark multi-layered networks for network disruption', ASONAM 2018, viewed 25 October 2018, <https://doi.org/10.1109/ASONAM.2018.8508309>.

Schaefer, D., (2012), 'Youth Co-Offending Networks: An Investigation of Social and Spatial Effects', *Social Networks*, vol. 34, pp. 141–149.

Schlichtkrull, M., Kipf, T. N., Bloem, P., Berg, R. v. d., Titov, I., & Welling, M. (2018a), 'Modeling Relational Data with Graph Convolutional Networks', ESWC 2018, Springer, Cham, viewed 3 June 2018, <https://doi.org/10.1007/978-3-319-93417-4_38>.

Schlichtkrull, M., Kipf, T. N., Bloem, P., van den Berg, R., Titov, I., & Welling, M. (2018b), 'Modeling Relational Data with Graph Convolutional Networks', ESWC

2018, Springer, Cham, viewed, <https://doi.org/10.1007/978-3-319-93417-4_38>.

Seo, J., & Mendelevitch, O. (2017), 'Identifying frauds and anomalies in Medicare-B dataset', EMBC 2017, IEEE, viewed 14 September 2017, <https://doi.org/10.1109/EMBC.2017.8037652>.

Ser, J. D., Lobo, J. L., Villar-Rodriguez, E., Bilbao, M. N., & Perfecto, C. (2016), 'Community detection in graphs based on surprise maximization using firefly heuristics', CEC 2016, IEEE, viewed 21 Nov. 2016, <https://doi.org/10.1109/CEC.2016.7744064>.

Shah, N., Beutel, A., Hooi, B., Akoglu, L., Gunnemann, S., Makhija, D., Kumar, M., & Faloutsos, C. (2016), 'EdgeCentric: Anomaly Detection in Edge-Attributed Networks', ICDMW 2016, IEEE, viewed 2 Feb. 2017, <https://doi.org/10.1109/ICDMW.2016.0053>.

Shakarian, P., Martin, M., Bertetto, J. A., Fischl, B., Hannigan, J., Hernandez, G., Kenney, E., Lademan, J., Paulo, D., & Young, C. (2015). 'Criminal social network intelligence analysis with the gang software', In L. M. Gerdes (Ed.), Illuminating Dark Networks, Cambridge University Press, pp. 143–156, <https://doi.org/10.1017/CBO9781316212639.010>.

Shaw, C. R., & McKay, H. D., (1942), 'Juvenile Delinquency and Urban Areas: A Study of Rates of Delinquents in Relation to Differential Characteristics of Local Communities in American Cities', *American Journal of Sociology*, vol. 49, no. 1, pp. 100–101.

Shehnepoor, S., Salehi, M., Farahbakhsh, R., & Crespi, N., (2017a), 'NetSpam: A Network-Based Spam Detection Framework for Reviews in Online Social Media', *IEEE Trans. on Information Forensics and Security*, vol. 12, no. 7, pp. 1585–1595.

Shehnepoor, S., Salehi, M., Farahbakhsh, R., & Crespi, N., (2017b), 'NetSpam: A Network-Based Spam Detection Framework for Reviews in Online Social Media', *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1585–1595.

Shin, K., Hooi, B., Kim, J., & Faloutsos, C. (2017), 'DenseAlert: Incremental Dense-Subtensor Detection in Tensor Streams', In Proceedings of the KDD 2017, Halifax, NS, Canada, 13–17 Aug. 2017, ACM, pp. 1057–1066.

Sibson, R., (1973), 'SLINK: An optimally efficient algorithm for the single-link cluster method', *The Computer Journal*, vol. 16, no. 1, pp. 30–34.

Sierra-Arévalo, M., & Papachristos, A. (2015). 'Social Network Analysis and Gangs', In S. H. Decker & D. C. Pyrooz (Eds.), The Handbook of Gangs, Wiley Editing Services, pp. 157–177, <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118726822.ch9>.

Singh, S., Thapar, V., & Bagga, S., (2020), 'Exploring the hidden patterns of cyberbullying on social media', *Procedia Computer Science*, vol. 167, pp. 1636–1647.

Skiena, S. (1990). 'Implementing discrete mathematics: Combinatorics and graph theory with mathematica', 1st ed. Addison-Wesley Longman, United States, viewed 21 Jan. 1990.

Solé-Ribalta, A., De Domenico, M., Gómez, S., & Arenas, A., (2016), 'Random walk centrality in interconnected multilayer networks', *Physica D: Nonlinear Phenomena*, vol. 323–324, pp. 73–79.

Song, W., Xiao, Z., Wang, Y., Charlin, L., Zhang, M., & Tang, J. (2019), 'Session-Based Social Recommendation via Dynamic Graph Attention Networks', In Proceedings of the WSDM 2019, Melbourne VIC, Australia, 11–15 Feb. 2019, ACM, pp. 555–563.

Song, Y., & Bressan, S. (2013), 'Fast Community Detection', In Proceedings of the DEXA 2013, Berlin, Heidelberg, 26–29 Aug. 2013, Springer Berlin Heidelberg, pp. 404–418.

Spano, R., & Freilich, J. D., (2009), 'An assessment of the empirical validity and conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005', *Journal of Criminal Justice*, vol. 37, no. 3, pp. 305–314.

Stevenson, M., (2017), 'Breaking Bad: Mechanisms of Social Influence and the Path to Criminality in Juvenile Jails', *The Review of Economics and Statistics*, vol. 99, no. 5, pp. 824–838.

Strang, S. J. (2014). 'Network Analysis in Criminal Intelligence', In A. J. Masys (Ed.), Networks and Network Analysis for Defence and Security, Springer International Publishing, Cham, pp. 1–26, <https://doi.org/10.1007/978-3-319-04147-6_1>.

Stringhini, G., Kruegel, C., & Vigna, G. (2010), 'Detecting spammers on social networks', In Proceedings of the ACSAC 2010, USA, ACM, USA, pp. 1–9.

Subelj, L., Furlan, S., & Bajec, M., (2011), 'An expert system for detecting automobile insurance fraud using social network analysis', *Expert Systems with Applications*, vol. 38, no. 1, pp. 1039–1052.

Sutherland, E. H. (1939). 'Principles of criminology', 3rd ed. J.B. Lippincott Company, Chicago, Philadelphia <http://sk.sagepub.com/reference/criminologicaltheory>.

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). 'Principles of criminology', 11th ed. Rowman & Littlefield.

Takase, S., Okazaki, N., & Inui, K., (2016), 'Modeling semantic compositionality of relational patterns', *Engineering Applications of Artificial Intelligence*, vol. 50, pp. 256–264.

Tang, J., Qu, M., Wang, M., Zhang, M., Yan, J., & Mei, Q. (2015), 'LINE: Large-scale Information Network Embedding', WWW 2015, International World Wide Web Conferences Steering Committee, viewed 12 May 2015, <https://doi.org/10.1145/2736277.2741093>.

Teng, X., Pei, S., Morone, F., & Makse, H. A., (2016), 'Collective Influence of Multiple Spreaders Evaluated by Tracing Real Information Flow in Large-Scale Social Networks', *Scientific Reports*, vol. 6, no. 1, p. 36043.

Thomas, K., Loughran, T., & Hamilton, B., (2020), 'Perceived arrest risk, psychic rewards, and offense specialization: A partial test of rational choice theory', *Criminology*, vol. 58, no. 3, pp. 485–509.

Tian, T., Zhu, J., Xia, F., Zhuang, X., & Zhang, T. (2015), 'Crowd Fraud Detection in Internet Advertising', In Proceedings of the WWW 2015, Florence, Italy, 18–22 May 2015, International World Wide Web Conferences Steering Committee, pp. 1100–1110.

Traag, V. A., Aldecoa, R., & Delvenne, J. C., (2015), 'Detecting communities using asymptotical surprise', *Physical Review E*, vol. 92, no. 2, p. 022816.

Traag, V. A., Krings, G., & Van Dooren, P., (2013), 'Significant Scales in Community Structure', *Scientific Reports*, vol. 3, no. 2930, pp. 1–10.

Trajković, G. (2008). 'Measurement: Accuracy and Precision, Reliability and ValidityMeasurement: accuracy and precision, reliability and validity', In W. Kirch (Ed.), Encyclopedia of Public Health, Springer Netherlands, Dordrecht, pp. 888–892, <https://doi.org/10.1007/978-1-4020-5614-7_2081>.

Trajtenberg, N., & Menese, P., (2019), 'Self-control, differential association and the drug–crime link in Uruguay in the context of the legalization of Marijuana', *Aggression and Violent Behavior*, vol. 46, pp. 180–189.

Tremblay, P. (1993). 'Searching for Suitable Co-offenders', In R. V. Clarke & M. Felson (Eds.), Routine activity and rational choice: Advances in Criminological Theory, 1st ed., Routledge, pp. 17–36.

Troncoso, F., & Weber, R., (2020), 'A novel approach to detect associations in criminal networks', *Decision Support Systems*, vol. 128, no. 113159, pp. 1–10.

Tsang, S., Koh, Y. S., Dobbie, G., & Alam, S., (2014), 'SPAN: Finding collaborative frauds in online auctions', *Knowledge-Based Systems*, vol. 71, pp. 389–408.

Tselykh, A., Knyazeva, M., Popkova, E., Durfee, A., & Tselykh, A. (2016), 'An Attributed Graph Mining Approach to Detect Transfer Pricing Fraud', In

Proceedings of the SIN 2016, Newark, NJ, USA, 20–22 July 2016, ACM, pp. 72–75.

Ubaldi, E., Vezzani, A., Karsai, M., Perra, N., & Burioni, R., (2017), 'Burstiness and tie activation strategies in time-varying social networks', *Scientific Reports*, vol. 7, no. 46225, pp. 1–11.

van Mastrigt, S., & Carrington, P. (2014). 'Sex and Age Homophily in Co-offending Networks: Opportunity or Preference?', In C. Morselli (Ed.), Crime and Networks, Criminology and Justice Studies, Routledge, New York, pp. 28–51.

van Um, E., (2011), 'DISCUSSING CONCEPTS OF TERRORIST RATIONALITY: IMPLICATIONS FOR COUNTERTERRORISM POLICY', *Defence and Peace Economics*, vol. 22, no. 2, pp. 161–179.

Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017), 'Online Human-Bot Interactions: Detection, Estimation, and Characterization', ICWSM 2017, AAAI Press, viewed 9 Mar. 2017 <https://arxiv.org/abs/1703.03107v2>.

Velampalli, S., & Eberle, W. 'Novel graph based anomaly detection using background knowledge', In Proceedings of the FLAIRS 2017, Florida, USA, 22–24 May 2017, AAAI press, 2017, pp. 538–543.

Veličković, P., Cucurull, G., Casanova, A., Romero, A., Lio, P., & Bengio, Y., (2017), 'Graph Attention Networks', *arXiv*, vol. 1710.10903, pp. 1–12.

Venkatesh, V., & Brown, S. A., (2001), 'A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges', *MIS Quarterly*, vol. 25, no. 1, pp. 71–102.

Walker, A., (2012), 'What is Boko Haram? ', Washington, DC, viewed 30 May 2012, <https://www.usip.org/sites/default/files/resources/SR308.pdf>.

Wang, A. H. (2010), 'Don't follow me: Spam detection in Twitter', International Conference on Security and Cryptography, IEEE, viewed 5 Apr. 2011, <https://ieeexplore.ieee.org/abstract/document/5741690>.

Wang, Z., Gu, S., Zhao, X., & Xu, X., (2018), 'Graph-based review spammer group detection', *Knowledge and Information Systems*, vol. 55, no. 3, pp. 571–597.

Wani, M., Jabin, S., & Ahmad, N., (2018), 'A sneak into the Devil's Colony - Fake Profiles in Online Social Networks', *arXiv*, vol. abs/1803.08810, pp. 1–31.

Waring, E., & Weisburd, D. (eds), (2000), 'Crime and Social Organization',1st ed., Routledge, viewed 11 Feb. 2018, <https://www.ncjrs.gov/pdffiles1/nij/grants/183328.pdf>.

Warnke, S. D., (2016), 'Partial information community detection in a multilayer network', Master Of Science, Naval Postgraduate School Monterey, California,

viewed Jun 2006, <http://hdl.handle.net/10945/49410>.

Weerman, F., (2011), 'Delinquent Peers In Context: A Longitudinal Network Analysis Of Selection And Influence Effects', *Criminology*, vol. 49, pp. 253–286.

Weimann, G. (2006). 'Terror on the Internet: The New Arena, The New Challenges', 1st ed. United States Institute of Peace Press, Washington, DC, viewed Jan. 2006, <https://www.researchgate.net/publication/238077713_Terror_on_the_Internet_The_New_Arena_The_New_Challenges>.

West, J., & Bhattacharya, M., (2016), 'Intelligent financial fraud detection: A comprehensive review', *Computers & Security*, vol. 57, pp. 47–66.

Wilson, R. J. (1986). 'Introduction to graph theory'. John Wiley & Sons, Inc., USA.

Worrell, J., Wasko, M., & Johnston, A., (2013), 'Social network analysis in accounting information systems research', *International Journal of Accounting Information Systems*, vol. 14, no. 2, pp. 127–137.

Wortley, R., & Mazerolle, L., (2009), 'Environmental Criminology and Crime Analysis: Situating the Theory, Analytic Approach and Application', *Crime Prevention and Community Safety: An International Journal*, vol. 11, no. 2, pp. 1–32.

Wortley, R., & Townsley, M. (eds), (2016), 'Environmental criminology and crime analysis',2nd ed., Routledge, viewed 31 Oct. 2016, <https://www.routledge.com/Environmental-Criminology-and-Crime-Analysis/Wortley-Townsley/p/book/9781138891135>.

Wu, X., Dong, Y., Tao, J., Huang, C., & Chawla, N. V. (2018), 'Reliable fake review detection via modeling temporal and behavioral patterns', In Proceedings of the IEEE BigData 2017, Boston, MA, USA, 11–14 Dec. 2017, IEEE, pp. 494–499.

Xiang, J., Zhang, Y., Li, J.-M., Li, H.-J., & Li, M., (2019), 'Identifying multi-scale communities in networks by asymptotic surprise', *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2019, no. 3, p. 033403.

Xu, J. J., & Chen, H., (2004), 'Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networks', *Decision Support Systems*, vol. 38, no. 3, pp. 473–487.

Xu, J. J., & Chen, H., (2005), 'CrimeNet explorer: a framework for criminal network knowledge discovery', *ACM Transanctions on Information Systems*, vol. 23, no. 2, pp. 201–226.

Yan, H., Jiang, Y., & Liu, G. (2018), 'Telecomm Fraud Detection via Attributed Bipartite Network', In Proceedings of the ICSSSM 2018, Hangzhou, China, 21–22 July 2018, IEEE, pp. 1–6.

Yang, C., Harkreader, R. C., & Gu, G. (2011). 'Die Free or Live Hard? Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers', In R. Sommer, D. Balzarotti & G. Maier (Eds.), Recent Advances in Intrusion Detection. RAID 2011. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp. 318–337.

Yang, C., Harkreader, R. C., & Gu, G., (2013), 'Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers', *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1280–1293.

Yar, M., (2005), 'The Novelty of 'Cybercrime':An Assessment in Light of Routine Activity Theory', *European Journal of Criminology*, vol. 2, no. 4, pp. 407–427.

Ye, J., & Akoglu, L. (2015), 'Discovering Opinion Spammer Groups by Network Footprints', ECML PKDD 2015, Springer International Publishing, viewed 29 Aug. 2015, <https://doi.org/10.1007/978-3-319-23528-8_17>.

Ye, J., Chow, J.-H., Chen, J., & Zheng, Z. (2009), 'Stochastic gradient boosted distributed decision trees', In Proceedings of the CIKM 2019, Hong Kong, China, ACM, pp. 2061–2064.

Yin, Z., & Shen, Y. (2018), 'On the dimensionality of word embedding', In Proceedings of the NIPS 2018, Montréal, Canada, Curran Associates Inc., pp. 895–906.

Young, J. T. N., (2011), 'How Do They 'End Up Together'? A Social Network Analysis of Self-Control, Homophily, and Adolescent Relationships', *Journal of Quantitative Criminology*, vol. 27, no. 3, pp. 251–273.

Yuan, S., Wu, X., & Xiang, Y. (2017), 'SNE: Signed Network Embedding', PAKDD 2017, Springer International Publishing, viewed 23 Apr. 2017, <https://doi.org/10.1007/978-3-319-57529-2_15>.

Zavala, E., Spohn, R., & Alarid, L., (2019), 'Gender and Serious Youth Victimization: Assessing the Generality of Self-control, Differential Association, and Social Bonding Theories', *Sociological Spectrum*, vol. 39, pp. 1–17.

Zhang, Z., Li, Q., Zeng, D., & Gao, H., (2013), 'User community discovery from multi-relational networks', *Decision Support Systems*, vol. 54, no. 2, pp. 870–879.

Zheng, X., Zeng, Z., Chen, Z., Yu, Y., & Rong, C., (2015), 'Detecting spammers on social networks', *Neurocomputing*, vol. 159, pp. 27–34.

Zhong, G., Wang, L.-N., Ling, X., & Dong, J., (2016), 'An overview on data representation learning: From traditional feature learning to recent deep learning', *Journal of Finance and Data Science*, vol. 2, no. 4, pp. 265–278.

Zhu, Z., (2019), 'Automatic Feature Engineering for Discovering and Explaining Malicious Behaviors', Doctor of Philosophy, University of Maryland, ProQuest Dissertations Publishing, <http://hdl.handle.net/1903/22000>.

Zou, K. H., O'Malley, A. J., & Mauri, L., (2007), 'Receiver-Operating Characteristic Analysis for Evaluating Diagnostic Tests and Predictive Models', *Circulation*, vol. 115, no. 5, pp. 654–657.

Appendix. 1. List of Publications

Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L., (2020), 'Fraud detection: A systematic literature review of graph-based anomaly detection approaches', *Decision Support Systems*, vol. 133, no. 113303, pp. 1–15.

(A in Australian Business Deans Council (ABDC) Journal Quality List, Q1 (top 6–10%) in Scientific Journal Rankings (SJR) List)*

Pourhabibi, T., Ong, K.-L., Kam, B.H., Boo, Y.L., (2021), 'DarkNetExplorer (DNE): Exploring Dark Multi-layer Networks beyond the Resolution Limit', *Decision Support Systems,* no. 113537, <https://doi.org/10.1016/j.dss.2021.113537>.

(A in Australian Business Deans Council (ABDC) Journal Quality List, Q1 (top 6–10%) in Scientific Journal Rankings (SJR) List)*

Pourhabibi, T., Ong, K.-L., Boo, Y.L., Kam, B.H., (2021), 'Detecting covert communities in multi-layer networks: A network embedding approach', *Future Generation Computer Systems*, vol. 124, pp. 467–479.

(Q1 (top 6–10%, impact factor: 7.187) in Scientific Journal Rankings (SJR) List)

Pourhabibi, T., Boo, Y. L., Ong, K. L., Kam, B., & Zhang, X. (2019), 'Behavioral Analysis of Users for Spammer Detection in a Multiplex Social Network', AUSDM 2018, Springer Singapore, viewed 16 February 2019, <https://doi.org/10.1007/978-981-13-6661-1_18>.

(Awarded the Prize of Best Paper Award)