Decision Support Systems 146 (2021) 113537

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

DarkNetExplorer (DNE): Exploring dark multi-layer networks beyond the resolution limit

Tahereh Pourhabibi [a,*], Kok-Leong Ong [b], Booi H. Kam [a], Yee Ling Boo [a]

[a] School of Accounting, Information Systems and Supply Chain, College of Business, RMIT University, Melbourne, Australia
[b] Centre for Data Analytics and Cognition, La Trobe University, Melbourne, Australia

ARTICLE INFO

Keywords:
Multi-layer dark networks
Community detection
Resolution limit
Asymptotic surprise
Random walk
Criminal network analysis

ABSTRACT

Timely identification of terrorist networks within civilian populations could assist security and intelligence personnel to disrupt and dismantle potential terrorist activities. Finding "small" and "good" communities in multi-layer terrorist networks, where each layer represents a particular type of relationship between network actors, is a vital step in such disruption efforts. We propose a community detection algorithm that draws on the principles of discrete-time random walks to find such "small" and "good" communities in a multi-layer terrorist network. Our algorithm uses several parallel walkers that take short independent random walks towards hubs on a multi-layer network to capture its structure. We first evaluate the correlation between nodes using the extracted walks. Then, we apply an agglomerative clustering procedure to maximize the asymptotical Surprise, which allows us to go beyond the resolution limit and find small and less sparse communities in multi-layer networks. This process affords us a focused investigation on the more important seeds over random actors within the network. We tested our algorithm on three real-world multi-layer dark networks and compared the results against those found by applying two existing approaches – Louvain and InfoMap – to the same networks. The comparative analysis shows that our algorithm outperforms the existing approaches in differentiating "small" and "good" communities.

1. Introduction

Dark networks are covert social networks [1] that are usually incomplete because they are not easily observable [2]. Members in these networks would actively conceal their network information by engaging in activities (e.g., friendship, kinship, and economic transactions) that distract from their true intentions thus, avoiding discovery by law enforcement agents [1,3]. They also hide their impermissible activities by disguising their interactions with people and events [2]. 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 supplied from different legal databases [4].

Crossley et al. [5] defines a covert network as having individuals who (i) commit illegal acts that are kept secret until the crime has taken place, and (ii) seek to remain anonymous afterward. Given the different types of covert networks, definitions do vary [1,5]. However, we are attracted to Crossley et al.'s [5] definition as it is well-aligned with our application problem, i.e., terrorist networks, where the focus is on individuals and how they conceal their involvement in criminal acts [6].

In terrorist networks, individuals are connected via different human interactions [7], such as friendship, kinship, and economic transactions. These 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 [8]. As a result, multi-layer networks contain rich topological information about individuals and their ties, but their complex structure makes discovering communities difficult [9], especially covert ones in dark multi-layer networks. As mentioned above, this is because these networks are incomplete, or they 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 [9,10].

Jeub et al. [11] argue that one way to discover the topological and dynamic properties of multiplex networks, including covert communities, is to study the behavior of a discrete-time random walk on the network. This proposal is because a random walker that jumps from one

* Corresponding author.
E-mail address: tahereh.pourhabibi@rmit.edu.au (T. Pourhabibi).

https://doi.org/10.1016/j.dss.2021.113537
Received 25 January 2020; Received in revised form 20 August 2020; Accepted 24 February 2021
Available online 27 February 2021

node to another gets "trapped" in denser regions of the network for longer periods, thus exposing anomalies and allowing covert communities to be discovered [11,12]. In this paper, we take advantage of this behavior to explore (or "walk" through) the network both within and between layers, based on some pre-set transition probabilities [12]. We call this a "multiplex random walk." We aim to find clusters with nodes that mostly reside in the network hubs as these hubs play a key "brokerage" role in (i) the flow of information and resources throughout the dark networks, or in (ii) mediating between unconnected actors [13]. According to Sageman [14], it is important to discover these nodes in the hubs as that is where the leaders are usually located. If these nodes or hubs are disrupted, criminal activities are effectively dismantled, so law enforcement agencies are interested in finding these nodes within dark networks.

Our proposed algorithm uses an adaptive centrality choice parameter to guide the random walker in a layer to move to the next neighbors, based on their hub centrality score. To effectively operate on a large network, our method allows multiple independent parallel walks to speed-up the expected time required to visit every node (at least once) in a graph [15]. Because our goal is to find the "small" and "good" communities reflecting the characteristics of a terrorist network, we also designed a community detection model that uses the Jaccard correlation of walked sequences between each pair of nodes to maximize a resolution-limit-free optimization function. This function will enable us to identify the "small" and "good" communities to allow a list of suspects be extracted for enforcement agencies to start their investigation in a more targeted manner [16].

Currently, most state-of-the-art research studies focus on partitioning networks by optimizing a modularity-based optimization function [17,18]. However, modularity fails to identify community structures below a certain characteristic scale (i.e., a resolution limit [19]), 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 analyze, and miss the "small" and "good" communities of interest to law enforcement agencies [20]. To overcome these limits, we introduce a statistical measure called asymptotic Surprise (AS), a fitness function that can (i) outperform modularity-based methods (thus finding smaller communities) and also (ii) find lower density communities [17].

We make five contributions in this paper. First, our technique uses the heuristic that criminals mostly lay in network hubs [14] to which we introduced a hub-centrality based random walk to explore the structural information of dark multiplex networks. Our proposal can be implemented in MapReduce to deal with very large networks. Second, we go beyond the resolution limit to find "small" and "good" communities by maximizing Surprise value through a hierarchical agglomerative clustering procedure. Third, we propose new measures to evaluate the quality of a community regardless of modularity. These measures (i.e., Surprise, Significance, Performance, intra-cluster conductance) help to evaluate the "good" and "small" communities for our use-case. Fourth, we show that our method better captures small and meaningful communities compared to two state-of-the-art techniques, when tested on three real-world multi-layer criminal networks. Lastly, our method is also shown to readily identify covert network leaders that are highly sought after by enforcement agencies.

The remainder of this paper is structured as follows. We start with a review of existing works in Section 2 and then explain our proposed algorithm in Section 3. In Section 4, we discuss the details of two baseline methods, against which the performance of our proposed approach is to be evaluated. In Section 5, we present and discuss the test results of applying our approach and the two baseline methods to three real-world multi-layer networks. Given the challenges and the lack of benchmarks, we devote Section 6 to review the results of our comparative analysis of the three real-world criminal networks using both modularity and non-modularity based metrics to demonstrate the credibility of our proposed approach. We conclude in Section 7 with a discussion of implications to research and practice, our method's limitations, and further work.

2. Related works

Our aim is to develop a community detection algorithm to find "small" and "good" communities in multi-layer networks. We, therefore, focus our review on the use of network-based methods for community detection in criminal networks. Another reason for this focus is that a broad review of data mining techniques in crime has already been conducted in [21–23].

Through a systematic search of works using network analysis for detecting dark network between 2010 and 2020 (based on search terms: "criminal networks," "crime data," and "dark networks"), we uncovered 25 studies. To enhance our understanding of the state-of-the-research in this field, we systematically assessed the 25 studies in terms of their application domain, the dataset used, type of method employed, type of network tested, and key features and methods employed (see Table 1).

Of particular relevance to our study is the method these studies used for finding communities in a network. According to McIllwain [24], there are two main methods of finding communities in a network: (i) node evaluation, and (ii) analysis of associations. Node evaluation methods [25,26] use simple measures of centrality taken from social network analysis to assess the nodes' positions in networks (e.g., degree centrality [27–29], betweenness [29,30], eigenvector centrality [6], and flow betweenness [31]). Several papers have combined these measures with machine learning and introduced visualizations (e.g., COPLINK [32], LogAnalysis [33], CrimeNet Explorer [34], GANG [35], and PAVENET [36]) to better support the needs of security analysts in enforcement agencies.

Analysis of association focuses on exploring connections among actors, relationships, and ties that are not immediately obvious [24]. Different graph clustering methods have been employed to cluster networks and find communities (e.g., InfoMap [37], Louvain [38], Girvan–Newman [39], WalkTrap [40]).

As revealed in Table 1, only six [10,41–45] of the reviewed studies use node evaluation to find criminal communities, with two [46,47] employing a combination of the two approaches. The balance 17 studies use analysis of association to find communities. This result springs little surprise. As discussed earlier, members of criminal networks try to conceal their networking information to distract law enforcement agents [1,3]. Therefore, introducing a community detection approach based on analysis of associations within the network, which hold the potential of even revealing hidden associations would feature as a preferred approach for detecting criminal groups or covert communities [24].

A second feature of concern to the development of our algorithm is the type of network the reviewed studies used to capture the activities of the covert communities they examined. The information shown in Table 1 reveals that the majority of the studies use monoplex networks, i.e., these studies do not consider the multiplex nature of criminals' activities to evade detection. In real-life, interactions within social communities are multi-faceted in nature and consist of multiple relationship types [63]. Domenico et al. [63], who compared differences between analyzing the same network in a monoplex and multiplex setting on two scientific collaboration networks, found that modeling a network as a multiplex representation is better at uncovering the connected topics and identifying smaller communities with more overlaps compared to conventional aggregated methods. Domenico et al.'s [63] findings advise us that it is more appropriate to model these interactions as a multi-layer network [64,65], since aggregating them into single or monoplex networks may lead to "information loss and may obscure the actual organization" [63] and distort both the network topology and the embedded dynamics [64].

From the reviewed studies shown in Table 1, Bahulkar et al. [55] and Saxena et al. [9] are the only two studies that worked on multi-layer networks. Bahulkar et al. [55] used link augmentation to improve the

Table 1
Survey on research studies on covert community detection using network-based methods.

Reference	Application domain	Dataset	Type of method used*	Type of network used	Features and methods used
[10]	General	Public Prosecutor's Office of Region del Biobío-Chile dataset	NE	Monoplex	Maximizes a linear utility function to find the association between criminals.
[45]	Money laundering	Bank statements and National Court Register data	NE	Monoplex	Assigns roles to people in the network and categorizes people with the same role in the same cluster to uncover the offender groups.
[44]	General	Enron	NE	Monoplex	Defines a data structure, named Community Tree, to depict the organizational structure of the network by ranking the nodes using PageRank.
[48]	Mafia	Infinito network (a mafia network in Italy)	AA	Monoplex	Applies max modularity community detection method to study the cluster structure of the criminal network and explore co-participation and role of individuals in criminal organizations for predicting criminal leaderships.
[49]	Juvenile co-offending	Official court data	AA	Monoplex	Uses the Spin Glass clustering method to study the spatial effects of juveniles' criminal activities.
[16]	Email	Enron	AA	Monoplex	Presents the shortest paths network search algorithm (SPNSA) that begins with a small sub-set of nodes of particular interest (e.g., known criminals, suspects, or persons of influence) to build and investigative sub-network around them.
[50]	Money laundering	A sample of 355 firms controlled by Italian mafia	AA	Monoplex	Develops a transaction management proxy to find the evidence of strategic management of accounting transactions for money laundering. This research uses hierarchical clustering using agglomerative clustering to categorize mafia firms.
[43]	Drug trafficking, mafia and terrorism	Bursa, Diyarbakir criminal network	NE	Monoplex	Develops feature-based group detection models by using crime data features (e.g., crime location, crime date, modus operandi, criminals' surname, and criminals' hometown).
[51]	General	Karate Club, Politic Books Network, Football Network	AA	Monoplex	Investigates on disrupting criminal networks. Uses WalkTrap community detection to detect communities and disintegrate the network by deleting the links between communities.
[47]	Pharmaceutical crime	Rogue manufacturer-manufacturer network, Darknet vendor-vendor network	AA & NE	Bipartite	Proposes a bipartite network model for inferring the hidden links and ties between criminals and applies Girvan Newman, Clauset Newman Moore, Wakita Tsurumi, and WalkTrap to study the structure of the clusters using various centrality metrics.
[52]	Cyber crime	MSN chat log	AA	Monoplex	Develops a criminal information mining framework for extracting forensically relevant information from suspicious online messages using a clique mining approach.
[42]	Criminal activities within a workplace	Open source reports of an office	NE	Monoplex	Defines a measure called the degree of organization for the whole network using centrality-based measures to show this measure would help in discovering and predicting crime networks without concentrating on discovering certain individuals.
[41]	Cyber crime	Online advertisements for escort services	NE	Bipartite	Constructs provider-by-location networks, which allowed prominent movement trends to be observed and uses centrality measures to identify the prominent location providers.
[53]	Cyber crime	Nigerian criminal network obtained from Facebook	AA	Monoplex	Analyzes the social graph of criminals to identify profiles of high-rank criminals, criminal organizations, and large-scale communities of criminals using a modularity maximization approach.
[54]	Cyber crime	Chat log data	AA	Monoplex	Extracts the cliques and the semantic of the conversation of each clique from a chat log. The extracted topics are then matched with crime ontologies to further detecting involvement in suspicious activities.
[55]	Drug trafficking	Caviar, Ndrangheta	AA	Multi-layer	Uses link augmentation to improve the quality of community detection. Performs community detection on the augmented network using Louvain and Speakeasy.
[9]	Terrorism	Noordin Top, FARC, Boko Haram	AA	Multi-layer	Introduces a purpose-driven community detection algorithm for multiplex networks. The algorithm focuses on a user-defined goal, which directs the algorithm to select and combine layers appropriately in support of that goal.
[46]	Phone call	Call data records	AA & NE	Monoplex	Proposes a toolbox called LogAnalysis. It has the ability of statistical analysis of centrality measures and temporal analysis of the network. It is exploited by the Newman algorithm to detect communities.
[56]	General		AA	Multi-modal	

(*continued on next page*)

Table 1 (*continued*)

Reference	Application domain	Dataset	Type of method used*	Type of network used	Features and methods used
		Criminal intelligence data, suspicious transaction, offshore-leak database, national companies registration information			Introduces a general approach for mining criminal networks that can integrate data from various sources (e.g., co-offenders from court data, criminals reported crime) to find the offenders relationship.
[57]	Gang-related crimes	Gangs data in the Greater Manchester area	AA	Monoplex	Uses InfoMap to detect the structure of gang groups.
[58]	Drug trafficking	Caviar	AA	Monoplex	Uses spectral embedding to find criminal clusters in a dynamic network.
[59]	Cyber crime	Restock, MojoHost Benign hosting network, Botnet, Masterhost criminal network	AA	Monoplex	Uses Louvain community detection to find criminal communities within the network to use them for further taking down the network.
[60]	Terrorism phone call	Encrypted call data records collected from mobile phone users in china, TerroristRel network collected from Profiles in Terror knowledge base	AA	Monoplex	Uses InfoMap and Greedy Clique Expansion algorithms to detect criminal communities, which were then used to assist in constructing the conditional random field to improve the accuracy of link labelling process.
[61]	General	Noordin Top, New South Wales crime network	AA	Bipartite	Uses a random walk-based approach to find community structure from bipartite criminal networks.
[62]	Illegal pyramid selling, drug abuse	Government data	AA	Monoplex	Uses frequent pattern mining to find the sub-group criminals within a time-evolving network and also provides a visualization interface to help better investigation on the corresponding users.

Note: * NE: node evaluation; AA: analysis of associations.

quality of community detection. They then applied two community detection methods (Louvain [38] and SpeakEasy [66]) on separate layers of the networks to find communities that were then combined and analyzed. The other work by Saxena et al. [9] aggregated the network into a weighted monoplex network. Like Bahulkar et al. [55], Saxena et al. [9] also used Louvain [38] to identify the communities in the aggregated weighted network. Both have their shortcomings, according to Li et al. [67], around the mutual inference among layers of a network. By aggregating the layers for analysis, the resultant network is weakened owing to the loss of structural topology information in each layer. Further, merging communities in each layer fails to account for the behavioral variations of nodes from one layer to another [68].

Another issue with Bahulkar et al.'s [55] and Saxena et al.'s [9] studies is the use of the Louvain method of community detection which attempts to optimize the modularity of a network partition, thus may fail to detect communities that are "small" to the network, which are crucial in many applications [14]. Our review also shows that [9,46–48,51,53,55,59] employed the modularity maximization method to detect communities in dark networks. The theoretical limitations of modularity-based approaches, however, are well-known [17], one of which is their resolution limit [19]. Due to its resolution limit, modularity-based approaches may fail to detect communities that are "small" to the network and result in dense communities, which are difficult to analyze [20]. Traag et al. [17] have demonstrated that this limitation can be circumvented by Surprise, a statistical measure that assesses the quality of a network partition into communities. Compared to modularity, Surprise is relatively unaffected by resolution limit and is more discriminative than modularity in discovering small communities [17].

Table 1 also shows that five studies [47,51,57,60,61] have adopted the popular random walk approach, which has been demonstrated to be a successful way of studying the behavior of a spreading process in a network [11], to capture the structural characteristic of criminal networks. These studies, however, applied a random walk-based method on the monoplex criminal network to find the structural communities. Compared to random walks on monoplex and aggregated weighted networks, random walks on a multi-layer network are better in capturing the mutual influence between layers and its topological properties [11]. Moreover, the random walk-based approaches used in these studies were not specifically designed for detecting criminal communities, suggesting that a new approach, along the lines of Jeub et al. [11], has to be explored.

In sum, our review informs us that to develop a community detection algorithm to find "small" and "good" communities in multi-layer networks, we need to design a random walk approach that captures the inter-layer influences and their topological properties [11], taking into considerations criminals mostly lay in network hubs [14]. We also need to move away from the conventional modularity approach to overcome the resolution limit problem in community detection and look towards developing a Surprise optimization function [17]. Our solution drew inspiration from these principles and is presented in the next section.

3. Methodology

To put our proposed approach in perspective, we begin with a brief description of multi-layer networks and the random walk algorithms before presenting the details of our solution.

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 vertexes from a vertex set V, which is common among all layers [8,69]. $G_i = (V_i, E_i, R_i, T_i)$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 [11]:

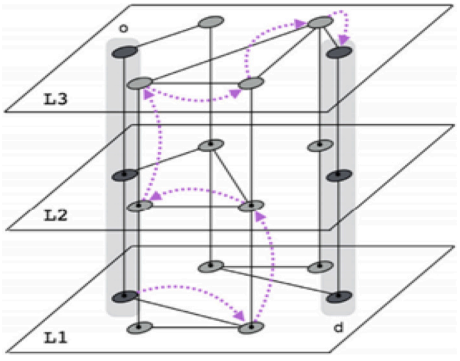

Fig. 1. Schematic of a walk (dotted trajectories) in a multi-layer network [70].

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

where $i_\alpha \in V$ represents 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 $w \in R^+$.

Algorithm 1: ***DarkNetExplorer*** **(*DNE*)**

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

```
1  nodes ← Size(A)
2  Class Mapper
3    method MAP (start_node n, Walker walker)
4      w←1
5      While w < W do
6        seq ← ∅
7        Curr ← n
8        while len(seq) < l do
9          calculate the probability P_iα^jβ using Equation 4 for Curr node
10         v ← move walker to the next node with maximum P_iα^jβ
11         seq[w] ← seq[w] ∪ {v}
12         Curr ← v
13       w← w+1
14 Return seq
15 Class Reducer
16   method Reduce (node n, sequence seq)
17     final_seq[n] ← ∅
18     For s in seq do:
19       final_seq[n] ← final_seq[n] ∪ {s}
20     ∂ ← int(0.1 * len(final_seq[n]))
21     final_seq[n] ← remove nodes from final_seq[n] with a count of less than ∂
22   Return final_seq
23 Class Main()
24     nodes = shuffle(nodes)
25     While ExistNodeToWalkOn() do
26       For walker in Walkers
27         MAP (n, walker)
28         Reduce(n, seq)
29
30   Sim ←Calculate Jaccard similarities for all pairs of nodes referring to [71]
31   Sim=Sort(Sim, desc)
32   S_a = −Inf
33   Clusters = [n for n in nodes]
34   While Sim do
35     Clusters_new=Combine Clusters using Single Linkage Agglomerative
36                  and Sim
37     S_a_new= Calculate AS of Clusters_new using Equation 6
38     IF S_a_new>= S_a
39       Remove from Sim the combined nodes value
40       Clusters = Clusters_new
41       S_a = S_a_new
42       Go to 34
43     ELSE:
44       Remove from Sim the last uncombined nodes value
45       Go to 34
46 Return Clusters
```

3.2. Preliminaries on random walks on multi-layer network

A random walker in a multi-layer network forms a Markov system by selecting a sequence of vertices randomly [70]. Generally, a random walker on a multi-layer network can exploit all the connections leaving the current node across all layers (Fig. 1).

Following Jeub et al. [11], a discrete-time random walk on a multi-layer network can be written as:

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

where $p_{j\beta}(t)$ is the probability for a random walker to be at node j in layer β at time t and $P_{i\alpha}^{j\beta}$ is 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 intra-layer and inter-layer behavior of a random walk. A classical random walk is the most direct way to generalize 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:

$$P_{i\alpha}^{j\beta} = \frac{A_{i\alpha}^{j\beta}}{\sum_{j\beta \epsilon V} A_{i\alpha}^{j\beta}} \quad (3)$$

3.3. Proposed approach

Fig. 2 presents the overall structure of our algorithm, named 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 in the integrated walk sequence are removed to prevent accidental moves to other communities. Then, in Stage 3, Jaccard correlations [71] between each pair of nodes are calculated using *minwise* hashing. Finally, in Stage 4, agglomerative clustering is applied based on Jaccard similarities. An optimization function is used to maximize the asymptotical Surprise [72] of the detected clusters to obtain the best partitions. This function helps to prevent very dense and large clusters and overcome the resolution limit of the modularity based approaches.

The implementation of DNE is presented in Algorithm 1 and is discussed in the following subsections.

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, we introduce a stream of short random walks to extract information from the network. This approach has two significant advantages [73]. First, several random walkers can explore different parts of a network simultaneously, allowing for a MapReduce parallel setup, as shown in Fig. 2. This feature is essential on large networks, since k parallel random walks reduce the cover time of a graph by $\Omega(k)$ times compared to a single walk [15]. 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 better runtime performance [15]. Thus, our 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 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 [74]. Therefore, a random walker can choose (hence, choice-based walk) to move towards the key actors, and form clusters around them. This feature helps to destabilize the network by isolating or eliminating potential criminals.

According to Sageman [14], 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 can break the dark network down into isolated nodes, thus incapacitating criminals from mounting sophisticated or large scale operations [75]. By extension, terrorist leaders are more likely hidden in hubs, which should be the focus of our detection efforts to achieve the effect stated [76].

To reflect Sageman’s [14] heuristics, we transform the transition probability of a random walker in a multi-layer network (Eq. (3)) to guide the random walkers to move towards the nodes with higher hubs (h) (see Algorithm 1, lines 8–11), as shown:

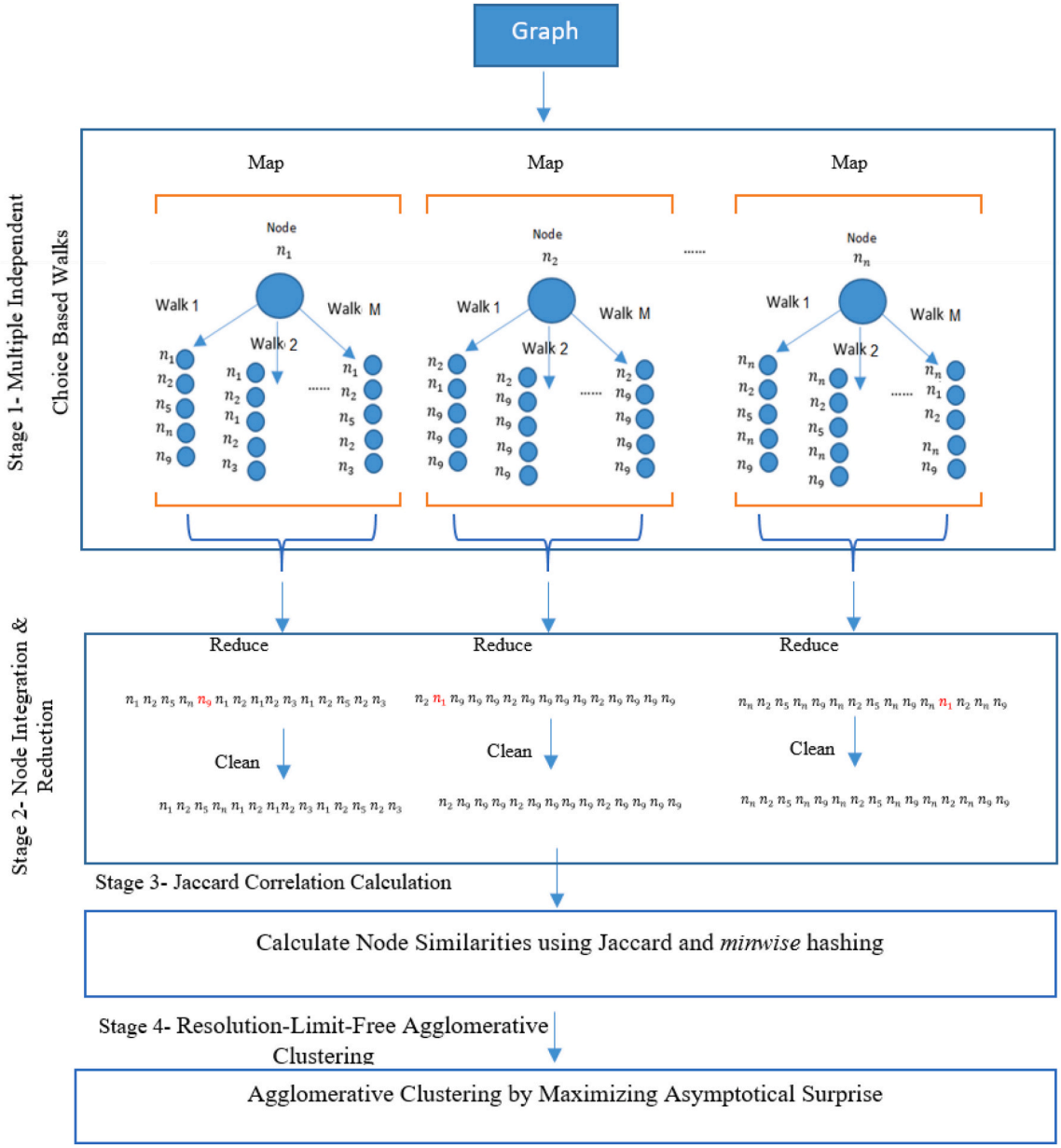

Fig. 2. Structure of DarkNetExplorer (DNE).

$$P_{i_\alpha}^{j_\beta} = \frac{A_{i_\alpha}^{j_\beta}}{\sum_{j_\beta \in V} A_{i_\alpha}^{j_\beta}} * h_j \tag{4}$$

where h_j is the normalized hub score of node j (for calculating hub scores refer to [77]). Eq. (4) suggests that the higher the hub score of a neighboring node (h_j), the more likely a random walker moves towards node j.

3.3.2. Nodes integration and reduction

When random walkers finish walking through the network, the history of all walked sequences for a particular node i are combined into one unified sequence (Algorithm 1, line 19). Nodes with a minimum occurrence threshold in a walked sequence are then eliminated in the Reduce function (Algorithm 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 be eliminated.

3.3.3. Jaccard correlation calculation

Similarities between nodes are estimated and sorted in a descending order based on the Jaccard correlation [71] between each pair of connected nodes using their history of walked sequences (Algorithm 1, line 30–31). We approximate the similarity by hashing via *minwise* hashing [71], which reduces the time complexity for calculating the similarity between all pairs of nodes in the graph from $O(n^2)$ to a linear-time of $O(n)$, where n is the number of nodes in the graph [71].

3.3.4. Resolution-limit-free agglomerative clustering

Finally, an agglomerative cluster analysis [78] is used to form the clusters based on similarities. As mentioned, our focus is to find "good" and "small" structural communities so that law enforcement can easily identify a list of suspects to begin an investigation [16]. This objective sets our approach apart from existing modularity-based optimization techniques, which resulted dense sub-networks that are difficult to

analyze [20]. To achieve our objective, we introduce the asymptotic Surprise in our agglomerative clustering in place of the modularity measure.

3.3.4.1. Asymptotical surprise. The discovery of an optimal cluster arrangement $\boldsymbol{C} = [c_1, c_2, \ldots, c_N]$, where $c_i \cap c_j = \varnothing$ and $\bigcup_{i=1}^{N} c_i = V$, can be cast as an optimization problem [79]. As a quality measure rooted in probability theory, Surprise assumes a null model that links nodes in a graph drawn uniformly 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 [80]:

$$S(\boldsymbol{C}) = -log\sum_{j=m_e}^{min(M,m)} \frac{\binom{M}{j}\binom{F-M}{m-j}}{\binom{F}{m}} \tag{5}$$

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

Eq. (5) is hard to compute, especially in the case of large networks [17]. Hence, Surprise can be approximated by a binomial distribution, leading to Eq. (6) called asymptotical Surprise (AS). This expanded version of Surprise assumes when the graph grows, the relative number of internal edges, and the related number of expected internal edges remain fixed [17]. In information theory, AS represents the kullback–leibler (KL) (Eq. (7)) divergence between the observed (q) and the 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 [72].

$$S_a(\mathbf{C}) = mD_{KL}(q \| < q >) \tag{6}$$

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

We extend the formulation of AS to a weighted directed version while keeping the same formulation in Eqs. (6) and (7) (see Table 2) [17]. We assume a uniform distribution of weights across the graph in the random graph and then calculate the expected weights as $<w>$. The total possible internal weight is then $<w> * M$, while the total possible weight is $<w> * F$. Hence, $<q>$ remains unchanged [17].

3.3.4.2. Hierarchical clustering by maximizing AS. We use a single linkage agglomerative (SLA) clustering [78] to merge communities, which, in the worst case, has a time complexity of $O(n^2)$. While merging communities, we use the AS optimization function 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 1, line 33). It then iteratively merges nodes based on the calculated Jaccard similarities to find the optimal clustering $\boldsymbol{C}^*$over the whole L-layer network (Algorithm 1, lines 34–45):

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

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

Table 2
Variables definition.

Variable	Un-weighted & un-directed	Weighted & directed	Description
F	$\binom{n}{2}$	$\frac{\binom{n}{2}}{2}$	Maximum possible number of links in a graph
M	$\sum_{c \in \boldsymbol{C}} \binom{n_c}{2}$	$\sum_{c \in C} \frac{\binom{n_c}{2}}{2}$	Total possible intra-community edges. Where $\boldsymbol{C}$ is the list of identified clusters, and n_c is 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_e	$\sum_{i,j \in n_c} A_{ij}$	$\sum_{i,j \in n_c} w_{ij}$	Total internal weights/edges of a cluster
q	$\frac{m_e}{m}$	___	Observed fraction of internal edges.
$<q>$	$\frac{M}{F}$	___	Expected fraction of internal edges.

4. Baseline methods

To determine the effectiveness of our algorithm, we compare its performance against two well-known community detection algorithms, which have been used to detect covert communities. The first is the "multi-slice modularity"-based Louvain[1] method [68], and the other is the multiplex InfoMap[2] [63], where both methods attempt to find communities using all the structural information across layers of the multiplex network [68]. As we noted in our literature survey, they are the only two techniques that are comparable as other techniques operate on monoplex networks.

The Louvain method is a widely used modularity-based community detection algorithm [55]. It follows a bottom-up approach in identifying communities by optimizing the local modularity of communities. The drawback of the Louvain method is that the identified communities can be unstable, resulting from local modularity optimization. This instability is further exacerbated by the limited connectivity between communities in a criminal network [55]. Like other modularity-based community detection approaches, Louvain suffers from a resolution limit that prevents it from detecting the small clusters [20] needed in our use-case.

From the benchmark by Lancichinetti et al. [81], InfoMap is the best performing community detection algorithm for large monoplex networks. InfoMap clustering method identifies communities according to the flow of information in the structure of the network. Like our proposal, InfoMap uses a random walk-based approach to reveal the hierarchical structure of large networks as it agglomerates clusters into super-nodes. As a result, InfoMap does not suffer the resolution limit problem of modularity maximization approaches like Louvain. This feature makes it a better candidate for finding small communities. With these two baseline methods explained, we now turn to the discussion of the evaluation of our algorithm against Louvain and InfoMap using three real-world multiplex dark network datasets.

5. Empirical analysis on real world multi-layer dark network

Cunningham et al. [82] contend that there is an optimal level of interconnectedness for dark networks as they cannot be too interconnected, nor can they afford to be too sparse. This characteristic is reflected in the three datasets used in our benchmark: the Noordin Top terrorist network, the Caviar network, and the Boko Haram network, with different structural and interconnectedness features, as shown in Table 3.

To evaluate the baseline methods against these datasets, we used their default parameter settings. While with our algorithm, we used 40 random walkers to sample sequences of length $l = 5$ from the neighboring nodes of each node $W = 10$ times. The results show that our

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

Table 3
Networks structural and interconnectedness features.

Dataset	No. of nodes	No. of links	No. of layers	Network features	Network density	Network average degree
Noordin Top network	78	1014	4	Un-directed, unweighted	0.337	26
Caviar network	107	651	11	Directed, weighted	0.057	6.08
Boko Haram network	44	82	3	Un-directed, weighted	0.08	3.72

approach discovers more ties between actors than the two benchmark methods and provides more insightful information.

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 Jemaah Islamiyah (JI) organization worked 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 [83].

The ties between actors represent one or more common affiliations or relationships. The network includes 78 actors (criminals) attending 45 different events, classified into four categories to form a 4-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 training [84].

Fig. 3(a–c) show the results of running Louvain, InfoMap, and DNE on the Noordin network. As shown in Fig. 3(c), our method produced seven different non-singleton communities (i.e., communities with more than two participants). Compared to InfoMap (six communities, S_a=203.922) in Fig. 3(b), and Louvain (five communities, $S_a = 127.835$) as shown in Fig. 3(a). Here, we see that our algorithm produces better "good" communities than 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, we can look into the dataset to verify the quality of the communities discovered by the different algorithms. According to [83], there are seven different groups, which the actors in the network can belong. Each group gives us some ground-truth that we can use to check how well each algorithm performs, which are described below.

5.1.1. Developing Darul Islam (DI)

The result of cluster *C1* is identical in InfoMap and DNE while Louvain was not able to detect this cluster. Both InfoMap and DNE picked up the relation between Node 1, Node 9, and Node 16. Having this relation in the output is important as we know from the ground-truth that Node 16 was the younger brother of Node 1. He was involved in training Darul Islam (DI), the Islamic group that fought for the establishment of an Islamic state in Indonesia, while his older brother was involved in sending DI recruits to the Philippines.

5.1.2. Bali bomb II

In this group, the small cluster *C2* detected by InfoMap and DNE unveiled some interesting information. Node 18 and Node 64 in *C2* both trained together as suicide bombers in Bali Bomb II in 2005 while Node 69 was suspected of making a video of the suicide bombers' last testaments and went on to become Noordin's courier and coordinator [83]. As with the previous category, Louvain did not pick up this small cluster, and while InfoMap and DNE both did, our algorithm performed better. In the case of InfoMap, it included Node 50 in this cluster, while our algorithm DNE didn't. Against the ground-truth, Node 50 was killed in the first Bali bombing in October 2002, so it should not appear as an actor in this category (Bali Bomb II in October 2005).

5.1.3. Jemaah Islamiyah group and Marriott bombing

C3 includes two principal leaders and planners of the Noordin network, Node 59 and Node 23. Most of the actors in *C3* are from the same organization JI (Jemaah Islamiyah), a transnational Southeast Asian militant Islamist terrorist organization 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 we check with the ground-truth information. For example, our algorithm excluded Node 15, the leader of Darul Islam (DI), from *C3*, which InfoMap did not. Given the DI affiliation, we know this node should not be in *C3*. This result suggests that DNE is better than InfoMap at categorizing members based on their specific characteristics and communication patterns.

5.1.4. Hiding Noordin (Jan 2005)

In this cluster *C4*, our 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. Louvain, on the other hand, miscategorized four members (Nodes 3, 5, 6, and 31) into this community (marked as *C1* in Louvain's output) where they should be in *C3*.

5.1.5. Jemaah Islamiyah (JI)

Members in the cluster *C5* are from the JI group. Except for non-

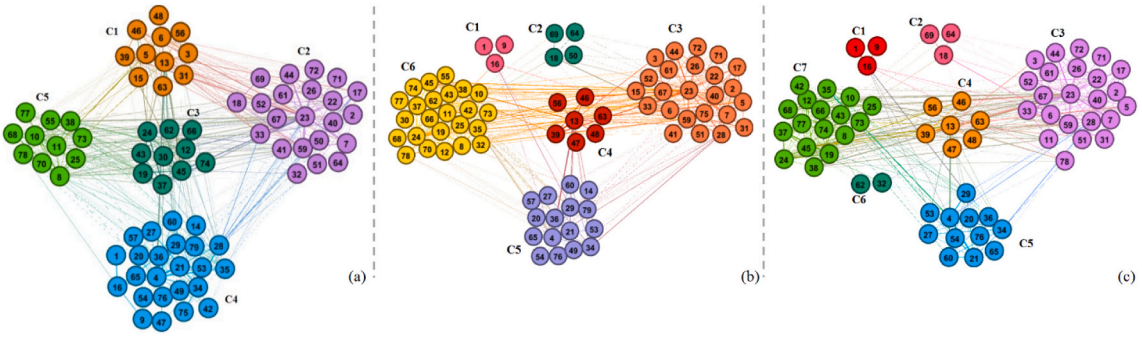

Fig. 3. Noordin Top Network Clustering. (a) Multiplex Louvain with 5 communities, *C1* to *C5* ($S_a = 127.835$). (b) Multiplex InfoMap with 6 communities, *C1* to *C6* ($S_a = 203.922$). (c) DNE with 7 non-singleton communities, *C1* to *C7* (For better resolution, singleton clusters are not included, $S_a = 242.683$).

critical members (Nodes 14, 49, 57, and 79) that are categorized as singletons in DNE, our algorithm and InfoMap produced 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*).

5.1.6. Dispose of Bali bombings leftovers

Node 62 and Node 32 in cluster *C6* (Fig. 3(c)) were two influential members of the Ring Banten group. They were responsible for finding a safe house for the the two leaders of the Noordin Top network (Nodes 59 and 23) and helped dispose of the leftover explosives from the Bali bombs. Both Louvain and InfoMap were not able to identify this cluster.

5.1.7. Embassy bombing in 2004

Cluster *C7* in Fig. 3(c) includes the actors involved in the Australian embassy bombing in September 2004. Node 45 was the field commander, Node 66 was Node 45's uncle who was the military instructor for the suicide bombers. Other members in this cluster, including Node 68, Node 73, Node77, Node 74, Node 24, and Node 43, were also trainers to the suicide bombers. Node 35 helped with recruitment, Node 38 studied bombing with Node 23, and together, they helped assemble the bomb. Our ground-truth also confirmed that Node 41 was involved in getting the detonating cord used in the bombing. Node 10, Node 12, Node 19, Node 25, and Node 37 were also found to be suicide bombers in this event. We note that *C7* in DNE is identical to *C6* in InfoMap as shown in Fig. 3(b), but our algorithm was able to exclude Node 11, who was killed in Bali Bombing I as well as nodes of lesser influence (e.g., Node 70, who was the courier) – Fig. 3(c). The corresponding Louvain community *C5*, which we are comparing *C7* to, 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 our algorithm. More importantly, our 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. Additionally, with better precision of nodes and a lower density in each community, our method will lead to better utilization of enforcement resources than ever before.

5.2. Cluster analysis on the Boko Haram network

The second dataset that we test our algorithm against is the Boko Haram terrorist network. This dataset, created by Cunningham [82] 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 due to its young cell-like structure and the lack of collective leadership. From the undirected ties, we constructed a 3-layer network: trust, communication, and knowledge sharing. The trust layer captures relationships like 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 [85] among the actors.

As shown in Fig. 4(c), our algorithm finds 12 non-singleton communities. For better resolution, we do not include the additional 5 resulted singleton communities in this figure. In contrast, InfoMap in Fig. 4(b) and Louvain in Fig. 4(a) with AS value of S_a= 52.242 and 46.565 respectively only discovered 11 and 9 non-singleton communities. When we compare the clusters among the three algorithms, their performance is almost identical in detecting small clusters. Where our algorithm performs better is the ability to breakdown the larger clusters that are detected by InfoMap and Louvain into smaller clusters, improving the interpretability of the results for enforcement agencies. As with the Noordin Top dataset, we discuss the outputs of each cluster against the ground-truth below.

5.2.1. Different terrorist activities

This was a single large cluster, marked as *C9* in Louvain. But it was broken into two smaller clusters, *C10* and *C1*, by InfoMap. With DNE, cluster *C9* in Louvain was discovered as three clusters *C1*, *C2*, and *C3*, which made it easier to establish a hierarchical relationship. Similarly, cluster *C8* from Louvain with 11 actors in it were split into two smaller clusters *C11* and *C12*, by our algorithm. At the same time, our 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 to undertake their investigation.

5.2.2. 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. There are limited ground-truth about this event. But, we were able to confirm that 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 [82]. We also know that both Nodes 67 and 69 were involved in the Mauritania attack. These five actors (Nodes 66–69 and 87) were in one cluster in Louvain and InfoMap while in our algorithm, the inactive actors are pruned with the active actors put into cluster *C10* (including Nodes 66, 67, and 69).

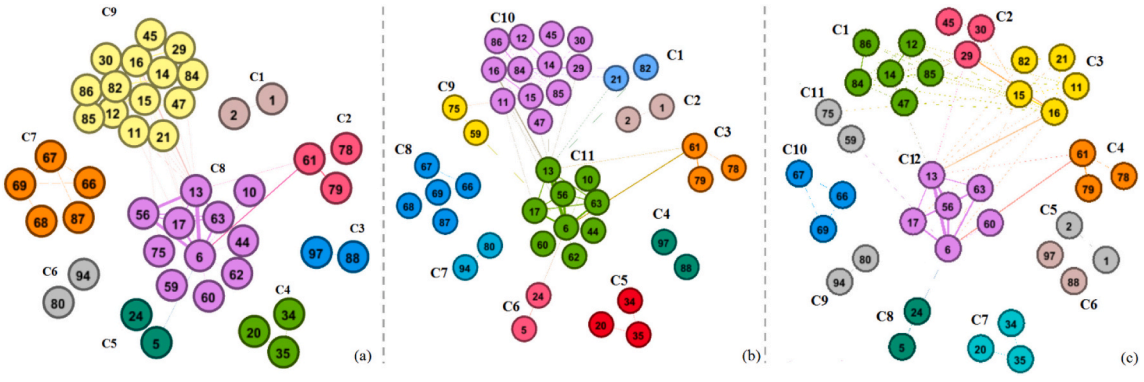

Fig. 4. Boko Haram Network Clustering. (a) Multiplex Louvain with 9 communities, *C1* to *C9* (S_a = 46.565). (b) Multiplex InfoMap with 11 communities, *C1* to *C11* (S_a = 52.242). (c) DNE with 12 non-singleton communities, *C1* to *C12* (For better resolution, singleton clusters are excluded) (S_a = 55.392).

5.3. Cluster analysis on the caviar network

The Caviar dataset was created by Morselli [28] based on an investigation that targeted a hashish and cocaine network operating in Montreal between 1994 and 1996. The principal data source came from information submitted as evidence during the trials of 22 participants in the Caviar network. It included over 1000 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 [28]. To conceal the identity of individuals, they are designated as nodes (e.g., Node 1, …, Node 110) [28]. For our experiments, we consider directed ties of each phase as a separate layer in this dark network, giving us an 11-layer multiplex network.

Fig. 5(a) shows the communities discovered by Louvain with a maximum AS value of $S_a = 990.533$. The non-singleton communities identified by InfoMap are shown in Fig. 5(b), including nine different communities with a maximum AS value of $S_a = 1114.52$. For conciseness, two singleton communities are not shown. As expected, InfoMap identifies smaller communities better than Louvain, but our algorithm again outperforms the two baselines with the higher AS value of $S_a = 3075.41$ when we compare the non-singleton communities. As seen in Fig. 5(b), the communities discovered by InfoMap are still very dense. Across the three methods, we see that our algorithm DNE is the better choice when it comes to identifying hubs and key actors in different communities. Using ground-truth information from [86], we briefly discuss the results within the five clusters in this network below.

5.3.1. Hashish trafficking

Cluster *C1* of DNE includes Node 1, the central participant targeted by law enforcement 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 (Node 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, making investigation difficult. In contrast, our algorithm significantly pruned this cluster, as shown in Fig. 5(c), retaining only the important actors.

5.3.2. 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.

5.3.3. Cocaine importations

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

5.3.4. Trafficking operations

In this cluster, our algorithm has similar results to the baseline methods except Node 107 in cluster *C2* in DNE was singled out as the link in the trafficking operations [28].

5.3.5. Legitimate importers

For this group, we see that both clusters *C5* and *C6* in Louvain were denser than the outputs of DNE in clusters *C4* and *C3*, respectively. Despite that, our algorithm proves to be capable of retaining the important nodes. Respectively, Node 101 was retained in *C4* in DNE, and Node 96 was retained in *C3* in DNE, as those 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 highlights how our use of the AS measure has helped us achieve meaningful results for our application problem. Specifically, our 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 analyze are identified) output than the baseline methods. This is further supported by our analysis in Table 4 on key actors, roles, and clusters in each of these three datasets.

6. Comparison of evaluation metrics

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

6.1. Multiplex-modularity

Didier et al. [89] define the multiplex-modularity of multiplex networks as the average of modularities over various layers of the network. As expected, Table 5 shows that Louvain has higher modularity in all datasets since it results in larger sized communities. Maximizing modularity leads to fewer and denser clusters, such as the case in Louvain. As discussed, this slows down the investigation. In contrast, maximizing AS may reduce modularity, but in practice, the produced communities better match what security analysts need for faster and more accurate detection.

6.2. Surprise value and number of non-singleton clusters

In practice, enforcement agencies would want to arrest the least

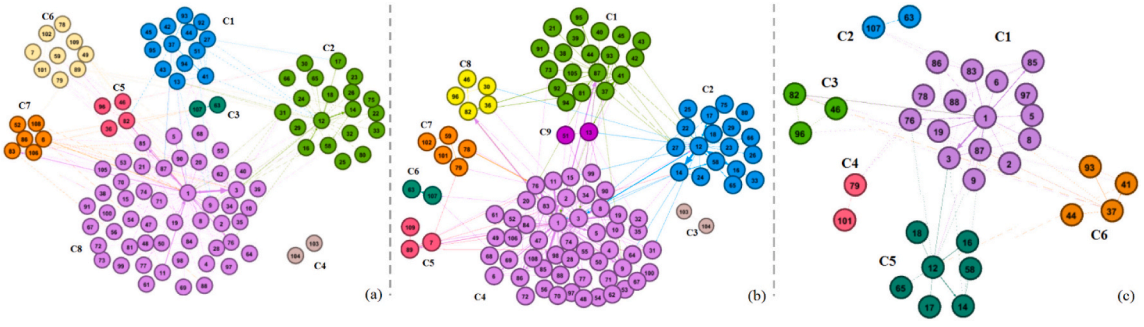

Fig. 5. Caviar Network clustering. (a) Multiplex Louvain with 8 communities, *C1* to *C8* ($S_a = 990.533$). (b) Multiplex InfoMap with 9 non-singleton communities, *C1* to *C9* ($S_a = 1114.52$). (c) DNE with 6 non-singleton communities, *C1* to *C6* (for conciseness, singleton clusters are excluded, $S_a = 3075.41$).

Table 4
Analysis of potential actors within detected clusters based on the centrality measures and their role for further disruption (Cluster IDs are according to DNE) [87,88].

Dataset	Top 10 Actors				Detected Clusters	Disruption Analysis
Noordin Top Network	**Degree**	**Hub**	**Betweenness**	**Closeness**		
	Node 23 {C3} (0.610)	**Node 23 {C3}** (0.310)	**Node 23 {C3}** (0.168)	**Node 23 {C3}** (0.681)	Developing Darul Islam (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 destabilize the network or even cause it to fall apart [33].
	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 evade being detected 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)	Jemaah Islamiyah (JI) Group and Marriott Bombing	Actors involved in community C3 are of high importance: they play a brokerage role (high betweenness centrality), hold high potentially advantageous positions within the network (high-degree and hub centrality) [87], and are close to other members (high closeness centrality) through both direct and indirect paths [88]. The arrest of these individuals could destabilise or even dismantle the network.
	Node 5 {C3} (0.377)	**Node 5 {C3}** (0.198)	**Node 28 {C3}** (0.072)	**Node 28 {C3}** (0.579)	Hiding Noordin (Jan 2005)	Node13 of cluster C4 has high betweenness centrality and high closeness centrality and was a conduit in the flow of information.
	Node 4 {C5} (0.325)	**Node 38 {C7}** (0.194)	**Node 13 {C4}** (0.072)	**Node 5 {C3}** (0.570)	Jemaah Islamiyah (JI)	In cluster C5, Node 4 acts as a connection point (high betweenness centrality).
	Node 28 {C3} (0.312)	**Node 8 {C7}** (0.185)	**Node 5 {C3}** (0.069)	**Node 13 {C4}** (0.566)	Dispose of Bali bombings leftovers	Members of C6 are not among those with high centrality values. Arresting them would have minimum impact on disintegrating the network.
	Node 45 {C7} (0.312)	**Node 45 {C7}** (0.184)	**Node 24 {C7}** (0.054)	**Node 35 {C7}** (0.562)	Embassy bombing in 2004	Members of this cluster (marked as C7) have high brokerage role. Having high degree and hub centralities put them among the high positioned actors. Disrupting this cluster could potentially destabilize the network.
	Node 35 {C7} (0.299)	**Node 10 {C7}** (0.182)	**Node 16 {C1}** (0.052)	**Node 4 {C5}** (0.558)		
	Node 8 {C7} (0.299)	**Node 35 {C7}** (0.182)	**Node 35 {C7}** (0.041)	**Node 73 {C7}** (0.558)		
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 analyze. This break down 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 with brokerage roles (high betweenness); their arrest is needed to disintegrate 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 also are 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**	Hashish Trafficking	Cluster C1 of DNE includes potentially 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 1 {C1} (0.355)	**Node 1 {C1}** (0.486)	**Node 1 {C1}** (0.649)	**Node 1 {C1}** (0.397)	**Node 107 {C2}** (1)		
	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 high position 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 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)	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 also Node 96 has a high degree centrality, acting as a potentially key member within this cluster, as verified by its role in several important operations.
	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)		
	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)			

Table 5
Community metrics over different datasets using three clustering 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

number of actors for disrupting a network. As such, maximizing AS to overcome the resolution limit (see Section 3.3.4) helps to move insignificant actors into singleton clusters, leading to lower density non-singleton communities that are easier to interpret by analysts. While this means 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 shown in Fig. 6, our algorithm managed to achieve the highest AS on our test data.

6.3. Significance

Significance [90] is a recently introduced objective function to evaluate community structure quality similar to Surprise [17]. It shows how 'real' a detected community structure is and that the results are not because of chance [90]. Surprise describes how likely it is to observe internal links in communities. Significance, on the other hand, 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

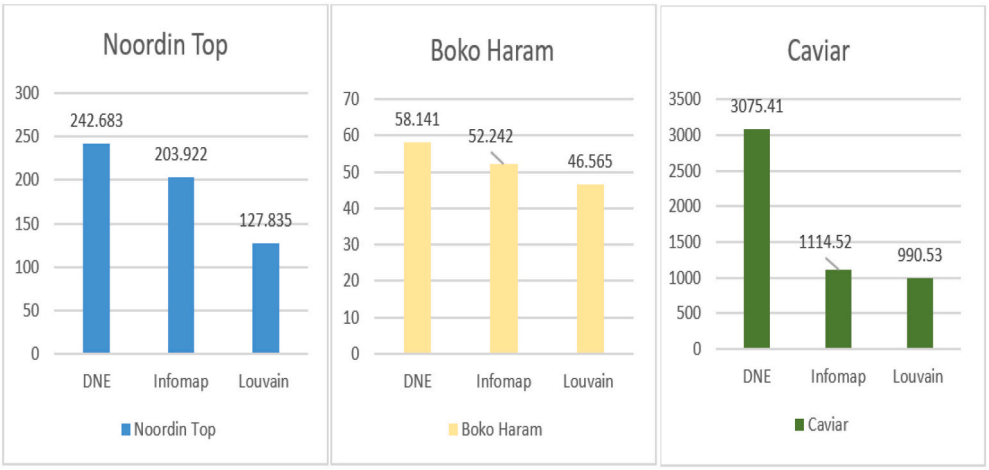

Fig. 6. Comparison of AS in different community detection methods over different datasets.

will be more discriminative than AS [90]. In our experiments, our method has the highest Significance score suggesting criminals are not clustered by chance but by their close communication within the network.

6.4. Performance

We define the performance of a cluster as the number of "correctly interpreted pairs of nodes" in a graph [91,92]. It reflects how well-connected the actors within a cluster are [91,92] 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, but, they may have few connections with actors in other clusters [91,92]. Therefore, a higher Performance value suggests that criminals within a cluster may not survive disruption within a cluster from enforcement agents as they won't be able to transfer their covert activities to another community in the network [93]. As shown in Table 5, DNE has the highest performance across all the three datasets we tested.

6.5. Internal density

This measure gives a reflection of the internal structure within a community [94,95] so that we can identify the parts of dark networks that are highly interconnected. An increase in the internal connectivity of a community reduces the possibility of using neighboring external nodes to bridge any internal disruption. With our algorithm, the detected clusters will yield a higher total weighted internal density [95], as shown in Table 5. Since our algorithm DNE prunes less important actors from the clusters, disrupting every community can potentially ensure the failure of the entire network.

6.6. Conductance

We define conductance of a set of vertices S as $\frac{c_s}{2m_s+c_s}$ [96], where $c_s = |(u,v) \in E : u \in S, v/\in S|$ is the number of edges with one end in the set and the other end outside; and $m_s = |(u,v) \in E : u \in S, v \in S|$ is the number of edges in S. A higher conductance in a cluster means 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. Sets of nodes that have fewer connections to the rest of the graph make good communities. This agreement is because such communities reduce the possibility of using neighboring nodes within other clusters to bridge an internal disruption attempt by law enforcement [93]. In the Noordin Top and Caviar datasets, our approach has the highest conductance score, while in the Boko Haram data, Louvain achieves the highest conductance score (Table 5). In the Boko Haram network, our 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 tradeoff may be acceptable since several smaller clusters are less challenging to analyze than a few large dense clusters.

6.7. Scalability

Fig. 7 depicts 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 to about 20, where any further increase does not seem to lead to further speedup. We attribute this to the

Fig. 7. Scalability: different number of walkers and various walk-lengths.

settings of our server that has a configuration of 8GB RAM and a 2.40 GHz CPU with 32 cores. We believe our programming environment prohibits a new walker thread from commencing until an existing walker thread completes its task once every CPU core has a walker thread running.

7. Conclusion

In this paper, we developed a community detection algorithm, called DNE, to find "small" and "good" communities in dark multi-layer networks. On account of the premise that criminals hide in network hubs, our design involved the use of random walkers to move towards nodes with higher hub centrality scores. We also use minwise hashing to speed up the Jaccard correlation calculations to hasten the hierarchical agglomerative clustering procedure. Our clustering procedure is also unique as it builds clusters to maximize AS instead of modularity, which helps to identify 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 our proposed approach outperforms two state-of-the-art techniques. Specifically, we achieve this 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.

The **practical implication** of our work here is increased interpretability. For enforcement agencies, staying ahead and on-top of covert networks to disrupt their criminal activities is crucial to maintaining public safety. Early detection and disruption are vital. No matter how much resources an agency has, the resource is always limited and constrained by the window of opportunity the agency can have before a disastrous event occurs. As such, algorithms that can analyze large networks and be able to detect covert communities and their activities will always be sought after to augment the security analysts to run their investigation quickly and with confidence. To achieve this, algorithms for this use-case must be *precise* (i.e., crucial actors, relations, and events should be in the output) and *concise* (i.e., "small" and low-density communities that are easy to analyze should be identified).

Considering this aim, we took an approach in the design of our algorithm that focused on optimizing the AS over what current methods do with modularity. The **research implication** of what we proposed to do here begins with the use of a different set of measures. This idea has been motivated by our use-case and the heuristics that we include from research findings elsewhere that aim to deliver a solution that aligns with the needs of our stakeholders, i.e., the law enforcement. As our results have shown, the use of AS over modularity has led to better results for the networks we are considering. As such, we believe future works in community detection of other network types should include understanding drawn from other areas of research that could be turned into heuristics that help design suitable measures to achieve the kind of community detection desired.

Secondly, our proposed algorithm has managed to bring together different components from existing methods in a way that achieve multiplex navigation in covert multi-layered networks. What our work has shown is a way towards a whole that is greater than the sum of its parts, rather than a singular focus on novelty for the sake of being different. As such, some readers may feel familiarity with the individual components discussed in this paper. But it should be pointed out that the contributions of our work lie in the way we have brought these together for our specific problem.

In terms of future work, although we have tested the proposed algorithm in a MapReduce setting to deal with large networks, all datasets used in our experiments are relatively small criminal networks so, our computations are currently done in-memory. With very large criminal networks, we may run into the limitation of fitting the network in the memory of computing nodes executing the MAP process. One way to overcome this difficulty in the future would be to partition the large network into sub-graphs for each computing node to proceed with the MAP process of that particular sub-graph.

Credit author statement

Corresponding Author (Tahereh Pourhabibi)

- Methodology development (proposing the main idea and algorithm)
- Resources (provision of study materials and experimental datasets)
- Investigation (experimental experiences)
- Writing the original draft

Co- Authors (Kok-Leong Ong, Booi Kam, Yee Ling Boo)

- Methodology validation and reliability analysis (validating the methodology)
- Writing review on the original draft and edition
- Supervision

References

[1] B.H. Erickson, Secret societies and social structure, Soc. Forces 60 (1) (1981) 188–210.
[2] P. Duijn, Detecting and Disrupting Criminal Networks; A Data-Driven Approach, Faculty of Science, University of Amsterdam, 2017.
[3] S.D. Warnke, Partial Information Community Detection in a Multilayer Network, Naval Postgradu-ate School, 2016.
[4] J. Hosseinkhani, S. Chuprat, H. Taherdoost, Discovering criminal networks by web structure min-ing, in: ICCCT 2012, IEEE Press, 2012, pp. 1074–1079.
[5] N. Crossley, G. Edwards, E. Harries, R. Stevenson, Covert social movement networks and the se-crecy-efficiency trade off: the case of the UK suffragettes (1906–1914), Soc. Networks 34 (4) (2012) 634–644.
[6] C. Broccatelli, Going beyond Secrecy: Methodological Advances for Two-Mode Temporal Criminal Networks with Social Network Analysis, University of Manchester, 2017.
[7] J.J. Xu, H. Chen, Fighting organized crimes: using shortest-path algorithms to identify associa-tions in criminal networks, Decis. Support. Syst. 38 (3) (2004) 473–487.
[8] T. Pourhabibi, Y.L. Boo, K.L. Ong, B. Kam, X. Zhang, Behavioral analysis of users for spammer detection in a multiplex social network, in: AUSDM 2018, Springer Singapore, 2019, pp. 228–240.
[9] A. Saxena, R. Gera, B. Miller, D. Chakraborty, Discovering and leveraging communities in dark multi-layered networks for network disruption, in: ASONAM 2018, IEEE Press, 2018, pp. 1152–1159.
[10] F. Troncoso, R. Weber, A novel approach to detect associations in criminal networks, Decis. Support. Syst. 128 (2020) 113159.
[11] L.G.S. Jeub, M.W. Mahoney, P.J. Mucha, M.A. Porter, A local perspective on community struc-ture in multilayer networks, Netw. Sci. 5 (2) (2017) 144–163.
[12] Z. Kuncheva, G. Montana, Community detection in multiplex networks using locally adaptive random walks, in: ASONAM 2015, ACM, 2015, pp. 1308–1315.
[13] D. Cunningham, S. Everton, G. Wilson, C. Padilla, D. Zimmerman, Brokers and key players in the internationalization of the FARC, Stud. Confl. Terror. 36 (6) (2013) 477–502.
[14] M. Sageman, Understanding Terror Networks, University of Pennsylvania Press, United States, 2004.
[15] N. Alon, C. Avin, M. Koucky, G. Kozma, Z. Lotker, M.R. Tuttle, Many random walks are faster than one, in: Proceedings of SPAA 2008, ACM, 2008, pp. 119–128.
[16] P. Magalingam, S. Davis, A. Rao, Using shortest path to discover criminal community, Digit. Investig. 15 (2015) 1–17.
[17] V.A. Traag, R. Aldecoa, J.C. Delvenne, Detecting communities using asymptotical surprise, Phys. Rev. E 92 (2) (2015), 022816.
[18] H. Cherifi, G. Palla, B.K. Szymanski, X. Lu, On community structure in complex networks: challenges and opportunities, Appl. Netw. Sci. 4 (1) (2019) 117.
[19] J. Xiang, Y. Zhang, J.-M. Li, H.-J. Li, M. Li, Identifying multi-scale communities in networks by asymptotic surprise, J. Stat. Mech. Theory Exp. 2019 (3) (2019), 033403.
[20] S. Fortunato, M. Barthelemy, Resolution limit in community detection, in: Proceedings of Natl Acad Sci 2007, National Academy of Sciences, 2007, pp. 36–41.
[21] H. Hassani, X. Huang, E. Silva, M. Ghodsi, A review of data mining applications in crime, Stat. Anal. Data Min. 9 (3) (2016) 139–154.
[22] U. Thongsatapornwatana, A survey of data mining techniques for analyzing crime patterns, in: Proceedings of ACDT 2016, IEEE Press, 2016, pp. 123–128.
[23] S. Qayyum, S. Hafsa, H. Dar, A survey of data mining techniques for crime detection, Univ. Sindh J. Inf. Commun. Technol. (USJICT) 2 (1) (2018) 1–6.
[24] J.S. McIllwain, Organized crime: a social network approach, Crime Law Soc. Chang. 32 (4) (1999) 301–323.
[25] K. Faust, G. Tita, Social networks and crime: pitfalls and promises for advancing the field, Annu. Rev. Criminol. 2 (2019) 99–122.
[26] G. Bichler, A. Malm, T. Cooper, Drug supply networks: a systematic review of the organization-al structure of illicit drug trade, Crime Sci. 6 (1) (2017) 2.

[27] P.M. Dudas, Cooperative, dynamic twitter parsing and visualization for dark network analysis, in: Network Science Workshop (NSW) 2013, IEEE Press, 2013, pp. 172–176.
[28] C. Morselli, Inside Criminal Networks, Springer-Verlag, New York, United States, 2008.
[29] C.E. Hughes, J. Chalmers, D.A. Bright, M. McFadden, Poly-drug trafficking: estimating the scale, trends and harms at the Australian border, Int. J. Drug Pol. 31 (2016) 80–89.
[30] F. Varese, The structure and the content of criminal connections: the Russian mafia in Italy, Eur. Sociol. Rev. 29 (5) (2013) 899–909.
[31] L.C. Freeman, S.P. Borgatti, D.R. White, Centrality in valued graphs: a measure of betweenness based on network flow, Soc. Networks 13 (2) (1991) 141–154.
[32] H. Chen, D. Zeng, H. Atabakhsh, W. Wyzga, J. Schroeder, Coplink: managing law enforcement data and knowledge, Commun. ACM 46 (1) (2003) 28–34.
[33] E. Ferrara, P. De Meo, S. Catanese, G. Fiumara, Detecting criminal organizations in mobile phone networks, Expert Syst. Appl. 41 (13) (2014) 5733–5750.
[34] J.J. Xu, H. Chen, Crimenet explorer: a framework for criminal network knowledge discovery, ACM Trans. Inf. Syst. 23 (2) (2005) 201–226.
[35] P. Shakarian, M. Martin, J.A. Bertetto, B. Fischl, J. Hannigan, G. Hernandez, E. Kenney, J. Lademan, D. Paulo, C. Young, Criminal social network intelligence analysis with the gang software, in: L. Gerdes (Ed.), Illuminating Dark Networks: The Study of Clandestine Groups and Organizations, Cambridge University Press, 2015, pp. 143–156.
[36] A. Rasheed, U.K. Wiil, Pevnet: a framework for visualization of criminal networks, in: ASONAM 2014, IEEE Press, 2014, pp. 876–881.
[37] M. Rosvall, C. Bergstrom, Maps of random walks on complex networks reveal community structure, in: Proceedings of Natl Acad Sci U S A. 2008, The National Academy of Sciences of the USA, 2008, pp. 1118–1123.
[38] V. Blondel, J.-L. Guillaume, R. Lambiotte, E. Lefebvre, Fast unfolding of communities in large networks, J. Stat. Mech. Theor. Exp. 2008 (2008) 1–12.
[39] M. Girvan, M. Newman, M. Girvan, M.E.J. Newman, Community structure in social and bio-logical networks, in: Proceedings of Natl Acad. Sci. USA 99, National Academy of Sciences, 2002, pp. 7821–7826.
[40] P. Pons, M. Latapy, Computing Communities in Large Networks Using Random Walks, ISCIS 2005, Springer, Berlin Heidelberg, 2005, pp. 284–293.
[41] M. Ibanez, R. Gazan, Detecting sex trafficking circuits in the U.S. through analysis of online es-cort advertisements, in: ASONAM 2016, IEEE Press, 2016, pp. 892–895.
[42] X. Shang, Y. Yuan, Social network analysis in multiple social networks data for criminal group discovery, in: Proceedings of CyberC 2012, IEEE Press, 2012, pp. 27–30.
[43] F. Ozgul, Z. Erdem, C. Bowerman, C. Atzenbeck, Comparison of feature-based criminal network detection models with k-core and n-clique, in: ASONAM 2010, IEEE Press, 2010, pp. 400–401.
[44] J. Qiu, Z. Lin, A framework for exploring organizational structure in dynamic social networks, Decis. Support. Syst. 51 (4) (2011) 760–771.
[45] R. Dreżewski, J. Sepielak, W. Filipkowski, The application of social network analysis algorithms in a system supporting money laundering detection, Inf. Sci. 295 (2015) 18–32.
[46] S. Catanese, E. Ferrara, G. Fiumara, Forensic analysis of phone call networks, Soc. Netw. Anal. Min. 3 (1) (2013) 15–33.
[47] H. Isah, D. Neagu, P. Trundle, Bipartite network model for inferring hidden ties in crime data, in: ASONAM 2015, IEEE Press, 2015, pp. 994–1001.
[48] F. Calderoni, C. Piccardi, Uncovering the structure of criminal organizations by community anal-ysis: the infinito network, in: Proceedings of SITIS 2014, IEEE Press, 2015, pp. 301–308.
[49] D.R. Schaefer, Youth co-offending networks: an investigation of social and spatial effects, Soc. Networks 34 (1) (2012) 141–149.
[50] D. Ravenda, M.M. Valencia-Silva, J.M. Argiles-Bosch, J. García-Blandón, Money laundering through the strategic management of accounting transactions, Crit. Perspect. Account. 60 (2019) 65–85.
[51] D. Anggraini, S. Madenda, E.P. Wibowo, L. Boumedjout, Network disintegration in criminal network, in: SITIS 2015, IEEE Press, 2015, pp. 192–199.
[52] F. Iqbal, B.C.M. Fung, M. Debbabi, Mining criminal networks from chat log, in: Proceedings of WI-AT 2012, IEEE Computer Society, 2012, pp. 332–337.
[53] H. Sarvari, E. Abozinadah, A. Mbaziira, D. Mccoy, Constructing and analyzing criminal networks, in: Security and Privacy Workshops (SPW) 2014, IEEE Press, 2014, pp. 84–91.
[54] F. Iqbal, B.C.M. Fung, M. Debbabi, R. Batool, A. Marrington, Wordnet-based criminal networks mining for cybercrime investigation, IEEE Access 7 (2019) 22740–22755.
[55] A. Bahulkar, B.K. Szymanski, N.O. Baycik, T.C. Sharkey, Community detection with edge aug-mentation in criminal networks, in: (Eds.), ASONAM 2018, IEEE Press, 2018, p. 1168.
[56] D. Robinson, C. Scogings, The detection of criminal groups in real-world fused data: using the graph-mining algorithm “graphextract”, Secur. Inform. 7 (1) (2018) 2.
[57] G. Oatley, T. Crick, Measuring UK crime gangs: a social network problem, Soc. Netw. Anal. Min. 5 (1) (2015) 33.
[58] D.B. Skillicorn, Q. Zheng, C. Morselli, Modeling dynamic social networks using spectral embed-ding, Soc. Netw. Anal. Min. 4 (1) (2014) 182.
[59] Y. Nadji, M. Antonakakis, R. Perdisci, W. Lee, Connected colors: Unveiling the structure of criminal networks, in: Salvatore J. Stolfo, Angelos Stavrou, Charles V. Wright (Eds.), Research in At-tacks, Intrusions, and Defenses, Springer, Berlin Heidelberg, 2013, pp. 390–410.
[60] H. Wan, Y. Lin, Z. Wu, H. Huang, A community-based pseudolikelihood approach for relation-ship labeling in social networks, in: Dimitrios Gunopulos, Thomas Hofmann, Donato Malerba, Michalis Vazirgiannis (Eds.), Machine Learning and Knowledge Discovery in Databases, Springer, Berlin Heidelberg, 2011, pp. 491–505.
[61] T. Alzahrani, K.J. Horadam, Analysis of two crime-related networks derived from bipartite social networks, in: Proceedings of ASONAM 2014, IEEE Press, 2014, pp. 890–897.
[62] X. Wang, M. Wang, J. Han, ACCDS: A criminal community detection system based on evolving social graphs, in: Carson Woo, Jiaheng Lu, Zhanhuai Li, Tok Wang Ling, Guoliang Li, Mong Li Lee (Eds.), Advances in Conceptual Modeling, Springer International Publishing, 2018, pp. 44–48.
[63] M. De Domenico, A. Lancichinetti, A. Arenas, M. Rosvall, Identifying modular flows on multi-layer networks reveals highly overlapping organization in interconnected systems, Phys. Rev. 5 (1) (2015), 011027.
[64] M. Rosvall, A.V. Esquivel, A. Lancichinetti, J.D. West, R. Lambiotte, Memory in network flows and its effects on spreading dynamics and community detection, Nat. Commun. 5 (1) (2014) 4630.
[65] Z. Zhang, Q. Li, D. Zeng, H. Gao, User community discovery from multi-relational networks, Decis. Support. Syst. 54 (2) (2013) 870–879.
[66] C. Gaiteri, M. Chen, B. Szymanski, K. Kuzmin, J. Xie, C. Lee, T. Blanche, E. Chaibub Neto, S.-C. Huang, T. Grabowski, T. Madhyastha, V. Komashko, Identifying robust communities and multi-community nodes by combining top-down and bottom-up approaches to clustering, Sci. Rep. 5 (1) (2015) 16361.
[67] X. Li, G. Xu, M. Tang, Community detection for multi-layer social network based on local ran-dom walk, J. Vis. Commun. Image Represent. 57 (2018) 91–98.
[68] W. Liu, T. Suzumura, H. Ji, G. Hu, Finding overlapping communities in multilayer networks, PlosOne 13 (4) (2018), e0188747.
[69] R. Interdonato, A. Tagarelli, D. Ienco, A. Sallaberry, P. Poncelet, Local community detection in multilayer networks, Data Min. Knowl. Disc. 31 (5) (2017) 1444–1479.
[70] A. Solé-Ribalta, M. De Domenico, S. Gómez, A. Arenas, Random walk centrality in intercon-nected multilayer networks, Physica D 323–324 (2016) 73–79.
[71] V. Satuluri, S. Parthasarathy, Y. Ruan, Local graph sparsification for scalable clustering, in: Proceedings of SIGMOD 2011, ACM, 2011, pp. 721–732.
[72] C. Nicolini, C. Bordiera, A. Bifonea, Community detection in weighted brain connectivity net-works beyond the resolution limit, NeuroImage 146 (1) (2017) 28–39.
[73] B. Perozzi, R. Al-Rfou, S. Skiena, Deepwalk: Online learning of social representations, in: Proceedings of SIGKDD 2014, ACM, 2014, pp. 701–710.
[74] B.R. Memon, Identifying important nodes in weighted covert networks using generalized centrality measures, Proceedings of EISIC 2012, IEEE Press, pp. 131–140.
[75] S.S. Everton, Tracking, Destabilizing and Disrupting Dark Networks With Social Networks Analysis, Cambridge University Press, USA, 2008.
[76] N. Roberts, S. Everton, Monitoring and disrupting dark networks: a bias toward the center and what it costs us, in: Alexander R. Dawoody (Ed.), Eradicating Terrorism from the Middle East: Policy and Administrative Approaches, Springer International Publishing, 2016, pp. 29–42.
[77] A. Mirzal, M. Furukawa, A method for accelerating the hits algorithm, J. Adv. Comput. Intell. Intell. Inform. 14 (1) (2010) 89–98.
[78] R. Sibson, Slink: an optimally efficient algorithm for the single-link cluster method, Comput. J. 16 (1) (1973) 30–34.
[79] J.D. Ser, J.L. Lobo, E. Villar-Rodriguez, M.N. Bilbao, C. Perfecto, Community detection in graphs based on surprise maximization using firefly heuristics, in: Proceedings of CEC 2016, IEEE Press, 2016, pp. 2233–2239.
[80] R. Aldecoa, I. Marín, Surpriseme: an integrated tool for network community structure characteri-zation using surprise maximization, Bioinformatics 30 (7) (2014) 1041–1042.
[81] A. Lancichinetti, S. Fortunato, Community detection algorithms: a comparative analysis, Phys. Rev. E 80 (5) (2009), 056117.
[82] D. Cunningham, S. Everton, P. Murphy, Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis, Rowman & Littlefield, Lanham, United States, 2016.
[83] International Crisis Group, Terrorism in Indonesia : Noordin’s Networks, International Crisis Group, Jakarta, 2006, p. 35.
[84] N. Roberts, S. Everton, The Noordin Top terrorist network, in: Disrupting Dark Networks, Cam-bridge University Press, Cambridge, 2011, pp. 385–396.
[85] R. Gera, R. Miller, A. Saxena, M. MirandaLopez, S. Warnke, Three is the answer: Combining relationships to analyze multilayered terrorist networks, in: Proceedings of ASONAM 2017, IEEE Press, 2017, pp. 868–875.
[86] C. Morselli, C. Giguere, Legitimate strengths in criminal networks, Crime Law Soc. Chang. 45 (3) (2006) 185–200.
[87] D. Bright, C. Greenhill, T. Britz, A. Ritter, C. Morselli, Criminal network vulnerabilities and ad-aptations, Glob. Crime 18 (4) (2017) 424–441.
[88] S.J. Strang, Network analysis in criminal intelligence, in: Anthony J. Masys (Ed.), Networks and Network Analysis for Defence and Security, Springer International Publishing, 2014, pp. 1–26.
[89] G. Didier, A. Valdeolivas, A. Baudot, Identifying communities from multiplex biological net-works by randomized optimization of modularity, F1000Research 7 (1042) (2018) 1–33.
[90] V.A. Traag, G. Krings, P. Van Dooren, Significant scales in community structure, Sci. Rep. 3 (1) (2013) 2930.
[91] U. Brandes, M. Gaertler, D. Wagner, Experiments on Graph Clustering Algorithms, ESA 2003, Springer, Berlin Heidelberg, 2003, pp. 568–579.

[92] M. Gaertler, Clustering, in: Ulrik Brandes, Thomas Erlebach (Eds.), Network Analysis: Methodo-Logical Foundations, Springer, Berlin Heidelberg, 2005, pp. 178–215.
[93] G. Galvan, J. Agarwal, Community detection in action: identification of critical elements in infra-structure networks, J. Infrastruct. Syst. 24 (2018), 04017046.
[94] Y. Song, S. Bressan, Fast community detection, in: DEXA 2013, Springer, Berlin Heidelberg, 2013, pp. 404–418.
[95] G. Liu, L. Wong, H.N. Chua, Complex discovery from weighted ppi networks, Bioinformatics 25 (15) (2009) 1891–1897.
[96] H. Almeida, D. Guedes, W. Meira, M.J. Zaki, Is there a best quality metric for graph clusters?, in: ECML PKDD 2011 Springer, Berlin Heidelberg, 2011, pp. 44–59.

Tahereh Pourhabibi is a PhD candidate in the School of Accounting, Information Systems and Supply Chain, RMIT University, Melbourne, Australia. She received her Master of Science in Artificial Intelligence from Al-Zahra University, Tehran, Iran. Her research interests include machine learning, data mining, anomaly detection, and their application in suspicious activity detection and fraud detection.

Kok-Leong Ong is an Associate Professor at the Centre for Data Analytics and Cognition, La Trobe University. He received his Ph.D. in 2004 and B. A. Sc. (Hons) in 1999 from the Nanyang Technological University, Singapore. His research interest includes data mining and analytics, and machine learning and AI, and his works have been supported by over $1.46m of grants to-date. He has published over 80 peer-reviewed papers and has served in over 60 Program Committees..

Booi Kam is a Professor in the School of Accounting, Information Systems and Supply Chains, RMIT University. His current research interests are in areas of strategic digital supply chain operations and supply chain relationships. A recipient of an Emerald Literati Network Awards for Excellence, Booi is regularly invited by universities in China, England, France, Korea, and Taiwan to give public lectures and teach into their degree programs. Booi holds a Ph.D. from the University of California at Los Angeles. He co-authors Consumer Logistics, a book by Edward Elgar Publishing.

Yee Ling Boo received her PhD in Information Technology from Monash University Australia. She is currently a senior lecturer in the School of Accounting, Information Systems and Supply Chain, RMIT University, Melbourne, Australia. Her research interests include Data Mining, Brain Inspired Computing, Cognitive Analytics and their applications in business, education and health. Before the pursuit of her PhD. degree, she was a software engineer in Malaysia. Her research works have appeared in reputable journals and conferences.