Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2019) 27: 421 – 436

doi:10.3906/elk-1806-52

Identifying criminal organizations from their social network structures

Muhammet Serkan ÇINAR[1,*], **Burkay GENÇ**[2], **Hayri SEVER**[3]
[1]Department of Computer Engineering, Faculty of Engineering, Hacettepe University, Ankara, Turkey
[2]Department of Policy and Strategy Studies, Institute of Population Studies, Hacettepe University, Ankara, Turkey
[3]Department of Computer Engineering, Faculty of Engineering, Çankaya University, Ankara, Turkey

Received: 06.06.2018 • **Accepted/Published Online:** 30.10.2018 • **Final Version:** 22.01.2019

Abstract: Identification of criminal structures within very large social networks is an essential security feat. By identifying such structures, it may be possible to track, neutralize, and terminate the corresponding criminal organizations before they act. We evaluate the effectiveness of three different methods for classifying an unknown network as terrorist, cocaine, or noncriminal. We consider three methods for the identification of network types: evaluating common social network analysis metrics, modeling with a decision tree, and network motif frequency analysis. The empirical results show that these three methods can provide significant improvements in distinguishing all three network types. We show that these methods are viable enough to be used as supporting evidence by security forces in their fight against criminal organizations operating on social networks.

Key words: Criminal networks, identification, decision tree, motif analysis, machine learning

1. Introduction

Criminal activities, especially terrorism, have been on the rise in recent decades. Most criminals today have social media accounts and chat identities, and they participate in virtual societies. Hence, the exploitation of social media and digital strategy plays a key role in terrorist networks' global dissemination of propaganda, radicalization, and recruitment [1]. Therefore, it is possible and necessary to track criminal organizations through social channels using the underlying networks structures.

The application of social network analysis (SNA) methods can be split into three fields according to criminal activities. The first one deals with terrorist networks; the second one includes street gangs, youth gangs, and delinquent groups [2]; and the last one concerns organized criminal groups [3]. There are many studies on deactivating terrorist networks [4], crime gangs, and organized criminal groups (such as illicit drug networks, dark networks, and covert networks). Studies using SNA metrics to measure network robustness and diffusion of information when structural defects exist in the network are not limited to criminal networks [5, 6]. Most of the studies on criminal networks are focused on well-known networks that are active in a specific region, such as Al Qaeda's 9/11 attack [7–9], the Islamic State in Europe or in the Middle East [1, 10], cocaine networks in US suburbs or in South Africa [9, 11], and a group trafficking heroin and cocaine in the New York City metropolitan area [12]. Generally, these studies examine node level metrics to identify the key players and network level metrics to identify the network structure in order to disrupt criminal networks.

*Correspondence: mscinar@hacettepe.edu.tr

One of the preliminary works on SNA in criminal networks was conducted by FBI special agent Roger H Davis [13]. In this work, the author demonstrated the usage of SNA methods (information flow, centrality, and density) for a real gang network. Additionally, Sparrow provided an exploratory and introductory study of SNA in criminal networks [14]. Later, Calderoni provided a detailed survey of the historical development of the usage of SNA methods in criminal investigations [3]. Recently, some literature reviews of SNA approaches in law enforcement and crime prevention were published in [15, 16].

In 2012, Shang and Yuan proposed a method called the comprehensive indicator model in order to identify suspicious persons in a conspiracy. The study also included identifying the relations between suspicious people and determining the leader [17]. The comprehensive indicator integrates the degree, betweenness, and closeness metrics after associating weights to them.

In this paper, we extend these studies by providing the most comprehensive analysis done so far. Our work is based on 16 different network metrics using data from 10 noncriminal and 14 criminal networks. Our main focus is to classify a network with respect to its criminality using only the structural data of the network. We assume zero knowledge of the individuals, except their links with the others in the network.

Our approach is outlined as follows. We first study the known noncriminal and criminal networks to compute their social network metrics by focusing on three types of networks: noncriminal, terrorist, and cocaine trading. Then we compare the computed metrics within and between types. This allows us to evaluate the metrics with respect to their ability to distinguish different types of networks. However, this evaluation considers each metric individually. In order to tackle this limitation, we construct a decision tree model, a common machine learning tool, to identify powerful combinations of metrics. Finally, we study the motif structures of each network. We conclude our work by identifying the most frequent motifs in each network type and showing that these frequencies differ significantly between different types of networks.

2. Datasets

In this section, we briefly talk about the datasets we use. We obtained terrorist networks' data from covert networks of the UCINET software package [18]. The cocaine and noncriminal networks are mostly obtained from UCINET and various other sources. We converted the collected data for each organization into undirected network structures.

Noncriminal networks are social networks that do not have any alleged criminal activities. They range from staff networks in companies to friendship networks in sports clubs and school dormitories. Noncriminal network data we used in this study are: Sawmill [18], Karate Club [19], School Dormitory (dining-table partners in a dormitory at a New York state training school), 50 Woman, Padgett (Padgett Florentine Families), Krackhardt High-Tech Managers, High Tech Employees (friendship and unionization in a high-tech firm), Thurman Office, Gagnon and Macrae Prison, and Galesburg Physicians [18]. Cocaine networks include groups conducting activities of buying or selling cocaine products. The cocaine network data we used in this study are: Cocaine Dealing [11], Operation MAMBO, Operation JUANES, Operation JAKE, and Operation ACERO. Terrorist networks include groups participating in bombings or shootings in different countries. The most famous group is Al Qaeda, which is mainly located in Afghanistan but executes terror activities in different countries. The terrorist network data we used in this study are: 9/11 Hijackers Associates, 17 November Group, Australian Embassy Bombing Operation, Bali Bombing, Christmas Eve Bombing, Jemaah Islamiyah Koschade, Madrid Train Bombing, Rhodes Bombing, and Philippines Bombing [18].

3. A comparison of networks using SNA metrics

In this section, we compare the noncriminal, cocaine, and terrorist networks to evaluate the sensitivity analysis of SNA metrics for terrorist networks. In the following subsections, we calculate each SNA metric for all the above-mentioned networks and provide empirical results and their comparison.

3.1. Transitivity

The first metric we look at is the transitivity of the network, also referred as the global clustering coefficient. This metric computes the ratio of the closed triplets to all triplets in a network, where a triplet is defined as three connected nodes and a closed triplet is simply a triangle (also known as the 3-clique).

Figure 1 shows the comparison of transitivity values of the three types of networks on the left. It is clear from the results that the transitivity values of different types of networks are quite different. While cocaine networks have low values of transitivity, imposing weak communication and connectedness between different tiers of the network, the terrorist networks have much higher transitivity values, pointing to their closed, isolated, cell-based structures.

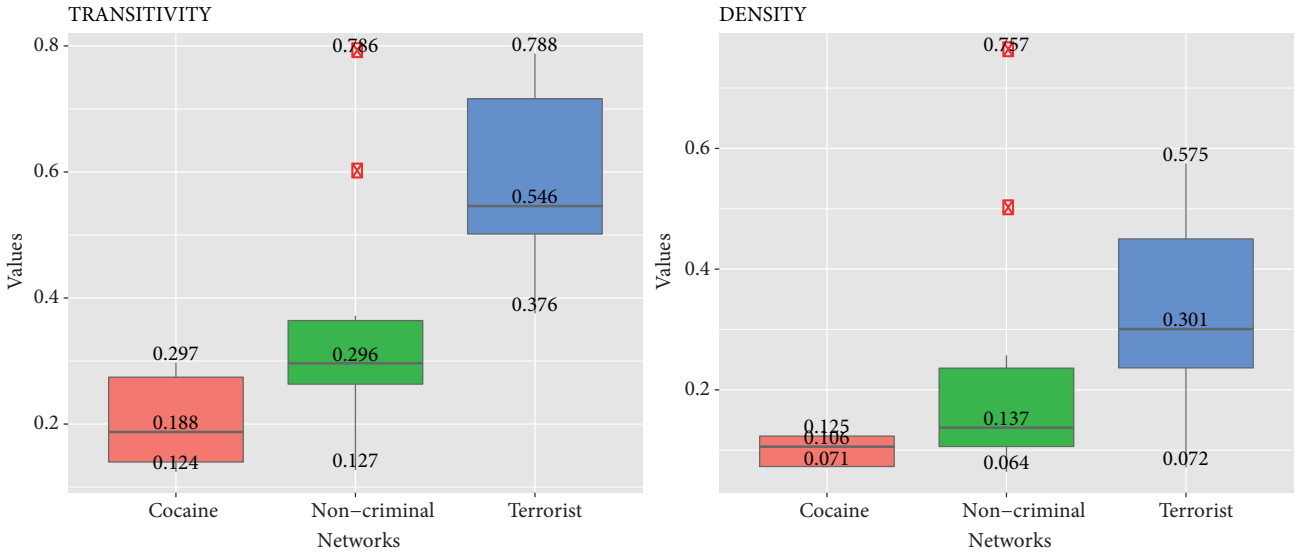


Figure 1. Box plots for transitivity and density values of examined networks. Both figures show sharp differences between network types and mark transitivity and density as important metrics.

3.2. Density

Another interesting network metric is the density of the network, which is formulated as:

$$d = \frac{2m}{n(n-1)}$$

The formula corresponds to the ratio of the existing edges to the potential edges. The density of the network is a measure of its completeness. A complete network, where any two nodes have an edge between them, has a density value of 1.0, whereas an empty network with no edges has a density value of 0.0. Considering criminal networks, low density values may trigger easier fragmentation. However, they also increase the secrecy of the network in case a member is captured by security forces.

Figure 1 provides a comparison of the densities of the three types of networks on the right. It is clear that cocaine networks tend to keep their densities as low as possible, while the densities in terrorist networks are much higher. Noncriminal networks are positioned relatively in the middle. However, they potentially have very low or very high density values.

3.3. Diameter (normalized)

Diameter is the next metric we consider. It is basically the length of the longest of all shortest paths. A low diameter value indicates a more compact network structure. A high diameter value means parts of the network are more isolated from each other. The diameter is heavily dependent on the size of the network. By adding a single node to an existing network, it is possible to increase its diameter by one. Hence, we normalize the diameter values by $n-1$, i.e. the maximum diameter value for a network with n nodes.

Figure 2 shows a comparison of the diameter values on the left. We can see from the figure that both cocaine and terrorist networks have relatively lower diameter values when compared to noncriminal networks. However, the noncriminal networks span a large range, partially overlapping with the criminal networks. This makes diameter a relatively less interesting metric with respect to density and transitivity.

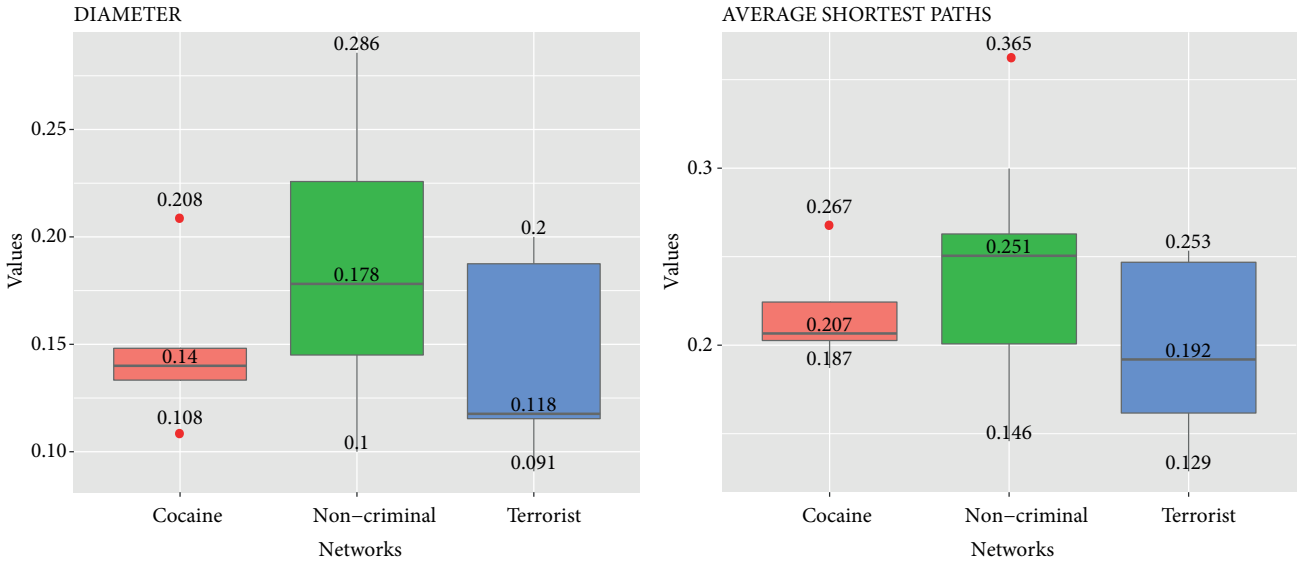


Figure 2. Box plots for diameter and average shortest path values of examined networks. Whereas diameter shows some variation between networks, ASP seems to be less descriptive.

3.4. Average shortest paths (normalized)

Next we look at the average shortest paths (ASP) metric. This metric is an average measure of how far away any two nodes in the network are. Note that, unlike diameter, the ASP is a robust metric and usually does not change significantly due to minor modifications in the network. However, the maximum possible value of ASP in a network of size n is $(n+1)/3$. Hence, it is linearly dependent on the size of the network. Therefore, we normalize all ASP values with $(n+1)/3$. i Figure 2 shows the comparison of ASP metrics on the right. The normalized ASP values of all three network types overlap each other significantly, making it very difficult to use this metric for labeling networks.

3.5. Degree centralization

Our next metric is degree centralization. The degree centralization value represents whether there are certain central nodes in the network bridging all other nodes. The most centralized network with respect to its degree is a star-like network where one node is in the center and all the remaining nodes are only connected to this central node. The degree centrality of a network is computed using Freeman's formula as follows:

$$C_D = \frac{\sum_{i=1}^{n} [C_D(v*) - C_D(v_i)]}{(n-1)(n-2)}$$

Figure 3 indicates the comparison of degree centralization on the left. It is seen that the noncriminal networks have relatively lower degree centralization scores, whereas the terrorist networks span the higher end. This result is due to the more leader-dependent structures observed in terrorist and cocaine networks. However, the differences are relatively small and can be misleading. Therefore, we categorize degree centralization as a weak metric for our purposes.

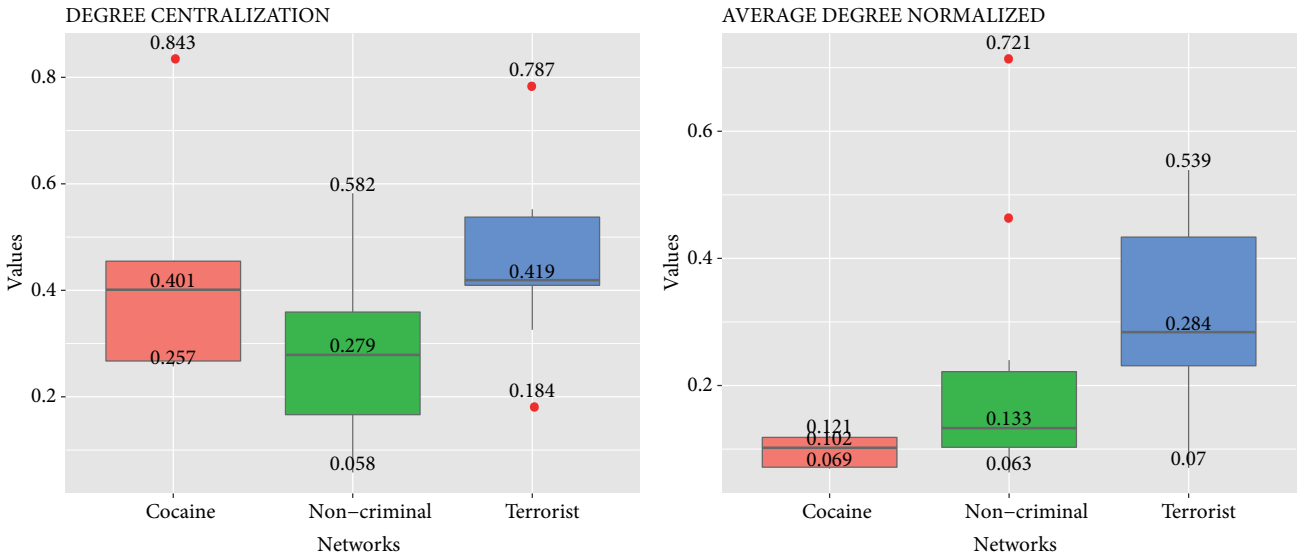


Figure 3. Box plot for degree centralization and average degree of examined networks. Average degree metric shows a sharp contrast between network types. The same cannot be said for degree centralization.

3.6. Average degree (normalized)

Our next metric is average degree, which represents the average number of connections a node has within the network. Considering that the average degree scales with the size of the network, we use a normalized measure with respect to the number of nodes in the network. Clearly, as the average degree of a network increases, the nodes become more strongly connected and alternative communication channels become more frequent. On the other hand, a low average degree is a sign of secrecy within the network, and it makes the network easier to divide into disconnected fragments when a few nodes are removed.

Figure 3 shows a comparison of average degree values. It is obvious that the three types of networks are quite different with respect to average degree. While the cocaine networks have the lowest average degree,

ensuring them more secrecy, terrorist networks have larger average degree values, a sign of cell structures and more cliquish topologies. The noncriminal networks span both ends of the spectrum. However, they are mostly positioned between the cocaine and the terrorist networks.

3.7. Maximum degree (normalized)

The next metric is the maximum degree in the network. This is actually the degree value of the node that has the maximum degree. Similar to the average degree metric, the maximum degree scales linearly with the size of the network. Hence, the values were normalized by the total number of nodes in the network.

We display our findings in Figure 4, on the left. In this figure, we can see that there is a significant difference between cocaine networks and terrorist networks. However, noncriminal networks and cocaine networks are almost identical. This indicates that, while terrorist organizations tend to form around powerful individuals, cocaine networks and legal organizations have flatter structures.

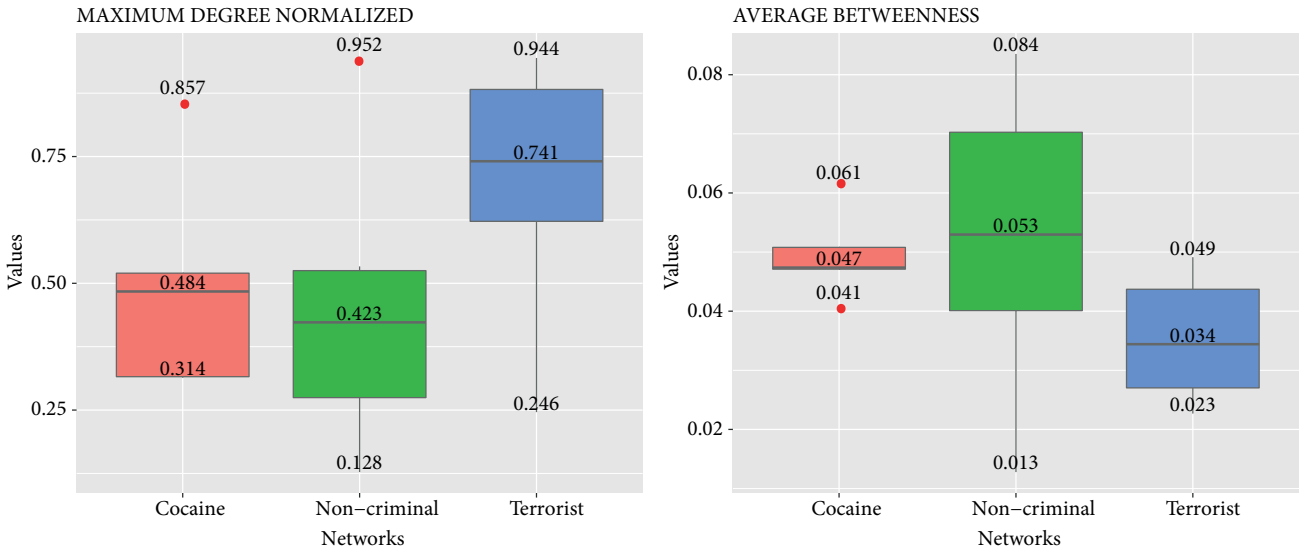


Figure 4. Box plots for maximum degree and average betweenness values of examined networks. Maximum degree is relatively higher and average betweenness is relatively lower in terrorist networks.

3.8. Average betweenness

Next we examine average betweenness. Betweenness of a node is an indicator of its importance in the shortest communication paths in the network. A low betweenness value indicates that the node is not at the center of information flow and is a peripheral node, whereas a node with high betweenness lies on many communication channels.

Figure 4 shows a comparison of the average betweenness values on the right. We can say that the terrorist networks generally have the lowest average betweenness values, hinting at their cell structures as well as alternative communication channels between the cells. The cocaine networks have relatively higher average betweenness values, representing communication flow in a few predetermined channels, as expected from these networks. The noncriminal networks span a large range and unfortunately make it difficult to use this metric for labeling criminal networks.

3.9. Maximum betweenness

Next we consider the maximum betweenness value for each network. This represents the betweenness of the "most between" node in the network. In other words, it is an indication of how the leaders of the network are positioned within the network.

Figure 5 gives a comparison of the maximum betweenness values on the left. We can observe that the values are quite different between cocaine and terrorist networks, with cocaine networks having relatively higher values. This proves that in cocaine networks the communication flow is more centralized, whereas in terrorist networks information may spread in multiple ways.

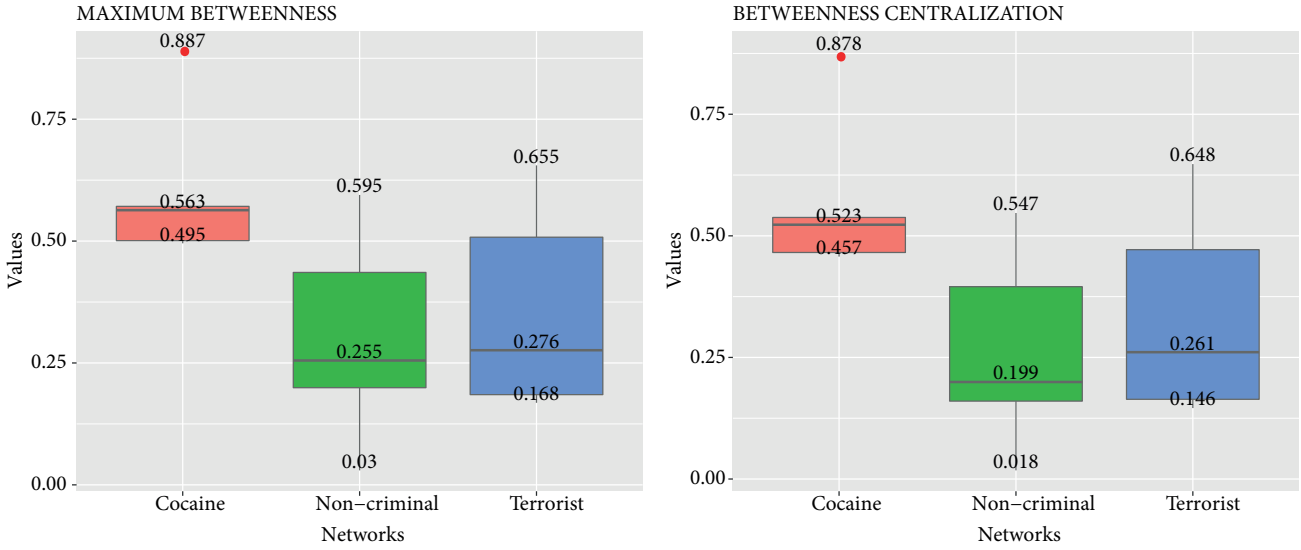


Figure 5. Box plot for maximum betweenness and betweenness centralization values of examined networks. Both tend to be higher in cocaine networks.

3.10. Betweenness centrality of network

Another metric we consider is the network-wide betweenness centrality. In order to compute this value, first the betweenness value of each node is subtracted from the maximum betweenness value. Then, the differences are summed up as follows:

$$B(G) = \sum_{i=1}^{n} (B_{max}(G) - B(v_i))$$

Additionally, the sum is normalized with $n-1$, which corresponds to the maximum possible betweenness value a network of this size can possibly have.

Figure 5 shows the results for betweenness centrality on the right. The box plots are positioned similarly to the maximum betweenness metric. Hence, it is difficult to make any distinctions between noncriminal and terrorist networks.

3.11. Average closeness

Closeness is a centrality metric and it represents how close a node is to the remaining nodes in the network. A node with high closeness value can reach most members of the network by a few links. On the other hand,

a node with low closeness is located far away from a large part of the network. First we examine the average closeness metric, which is the average of closeness values of all nodes in the network. It represents the general structure of the network. A high average closeness value indicates a compact, star-like topology, whereas a low average closeness value is an indicator of long, chain-like structures.

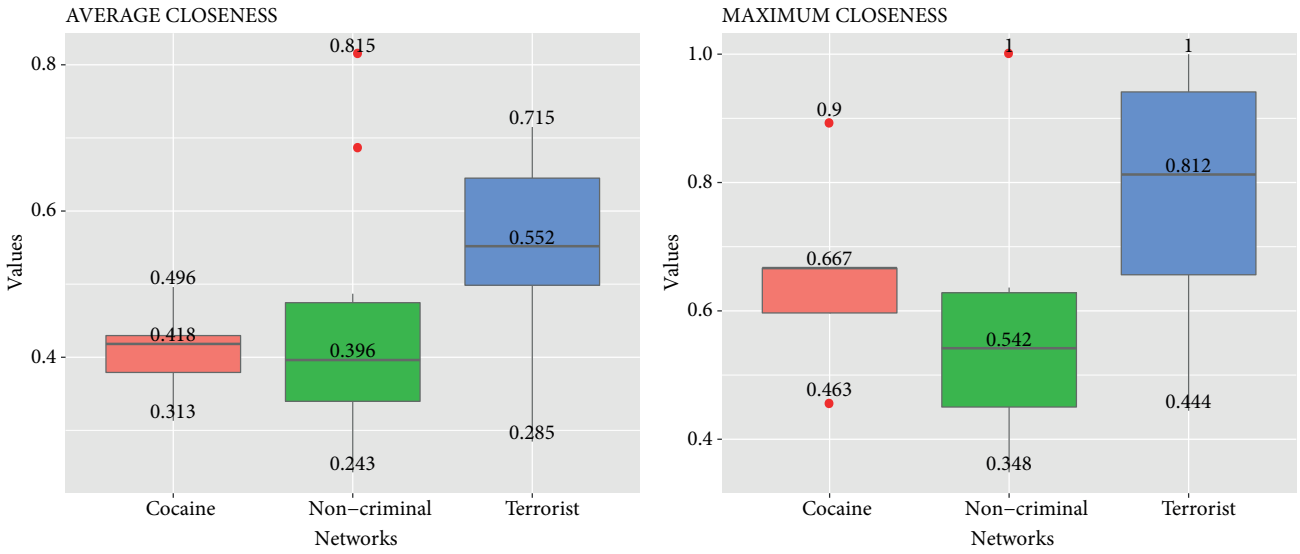


Figure 6. Box plot for average and maximum closeness values of examined networks. Terrorist networks clearly get separated from the other two.

Figure 6 shows the box plot comparison of average closeness values on the left. We observe that terrorist networks have significantly higher average closeness values, hinting at their cell structures and short communication paths between leaders and operational members. On the other hand, cocaine networks have lower average closeness values, resulting in communication flowing through the network via chains of connections. Although terrorist networks have significantly higher values, the values of the noncriminal and cocaine networks mostly overlap, making it difficult to distinguish between them.

3.12. Maximum closeness

In order to compute the maximum closeness metric, we search for the node with the maximum closeness value. A high value corresponds to individuals that can reach the whole network by using very few links. A low value is an indicator of a flatter network, where no individual is more central than the others. Maximum closeness is formally expressed as:

$$C_{\max}(G) = max\{C(v_i)|i = 1..n\}$$

Figure 6 summarizes the results for the maximum closeness values of the three network types on the right. It is seen that, unlike the average closeness values, the maximum closeness allows us to distinguish between the networks. While terrorist networks have the highest values, noncriminal networks have the lowest. This indicates that terrorist networks are built around important leading figures, whereas noncriminal networks have mostly flatter structures, where individuals are more equal. Cocaine networks are positioned between the two, hinting at mixed structures.

3.13. Closeness centrality of network

Next we consider the overall closeness centrality value of the network, computed in a similar way to the computation of betweenness centrality:

$$C(G) = \sum_{i=1}^{n} (C_{max}(G) - C(v_i))$$

The resulting value is normalized by the maximum closeness centrality value that a network of this size may have.

Figure 7 demonstrates the results of our analysis on the network centrality on the left. We observe a similar pattern to the one observed for the maximum closeness metric. However, this time the cocaine networks are mostly overlapping with the terrorist networks, whereas the noncriminal networks are further separated from the other two. In other words, this is a good metric for making a distinction between noncriminal and criminal networks.

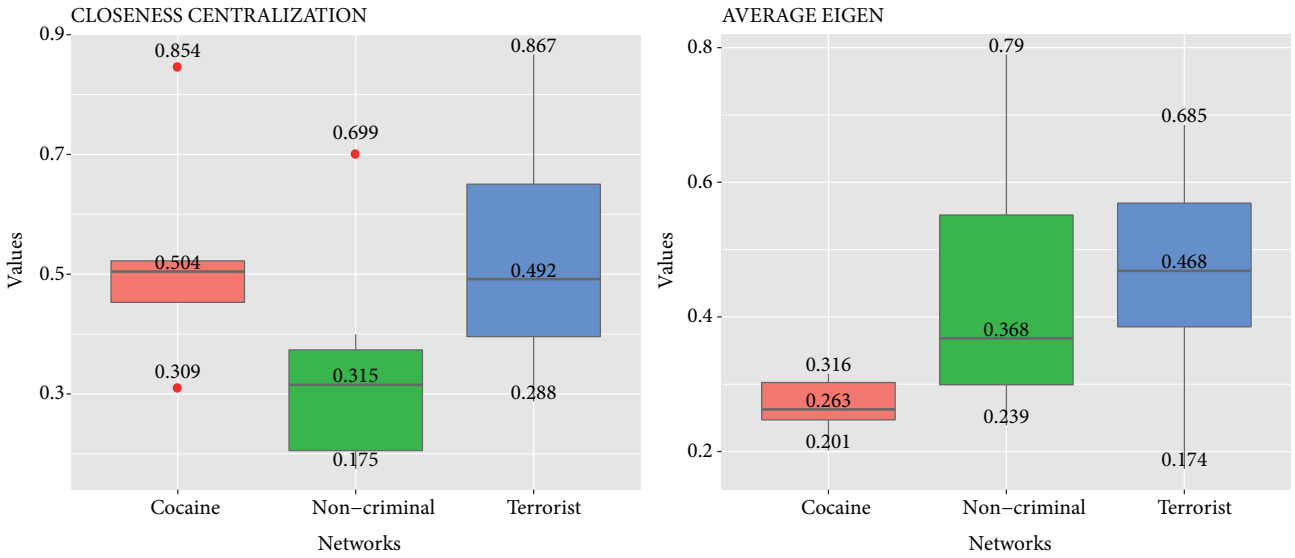


Figure 7. Box plot for closeness and average eigenvector centrality values of examined networks. Both criminal network types have high closeness centralization; however, only cocaine networks get separated by average eigenvector centrality.

3.14. Average eigenvector centrality

Our next metric is the average eigenvector centrality. Eigenvector centrality became especially popular after Google invented the well-known PageRank algorithm based on the eigenvector values of the nodes of a network. The eigencentrality of a node is the weighted average of eigencentralities of its neighbors. Therefore, it is a good representation of the relative importance of a node with respect to both the quantity and quality of the connections it makes.

The average eigenvector centrality is the average over all nodes of the network. Figure 7 demonstrates our results on the right. Although cocaine networks have very low average eigencentrality values, both noncriminal and terrorist networks span similar higher values.

3.15. Maximum eigenvector centrality

We observe that the maximum eigenvector centrality values for all graphs are 1.0 due to the nature of the computation. Hence, we omit them in further analysis.

3.16. Eigenvector centrality of network

The eigenvector centrality of the whole network is computed similarly to the closeness and the betweenness centralities. Formally it is calculated by:

$$E(G) = \sum_{i=1}^{n} (E_{max}(G) - E(v_i))$$

The sum is normalized with the maximum possible value available for a network of the same size.

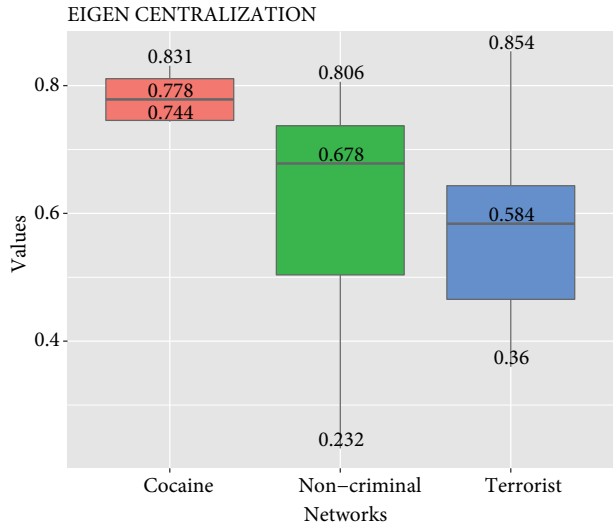


Figure 8. Box plot for eigenvalue centralization of examined networks. Terrorist networks have higher values.

Figure 8 shows the comparison for this metric. This time, cocaine networks have the highest average, whereas terrorist networks have the lowest. We can say that cocaine networks are nicely separated from the other two. However, noncriminal and terrorist networks span similar ranges.

3.17. Metric importance ranking

In the previous sections we have analyzed all the metrics individually. However, we did not mention clearly which metric is more important in describing the differences between criminal and noncriminal networks. For this purpose, we ran the metric data through the decision tree and the random forest algorithms to obtain variable importance measures they generated. We used R language libraries to compute four different variable importance measures: one from the `rpart` package, one from the `caret` package, and two from the `randomforest` package (based on mean decrease in accuracy and mean decrease in node impurity). Once we have the four normalized measures, we calculate their average to obtain a final importance measure for each SNA metric. The results are provided in the Table.

Table. Metric importance values.

Metric	Value	Metric	Value
Transitivity	0.90	Maximum degree normalized	0.27
Eigencentralization	0.74	Maximum closeness	0.25
Betweenness centralization	0.56	Diameter	0.22
Maximum betweenness	0.54	Degree centralization	0.21
Density	0.52	Average betweenness	0.19
Average degree normalized	0.46	Average eigen	0.18
Closeness centralization	0.40	Average shortest paths	0.13
Average closeness	0.39	Maximum eigen	0.00

It can be seen that transitivity appears to be the most distinguishing metric among the three network types. Eigencentralization follows it, which is in turn followed by betweenness centralization, maximum betweenness, and density.

One important thing to note here is that these values represent the individual description power of each metric. However, it is possible that when combined in various ways, two or more weak metrics together may become more powerful than a much more descriptive metric. To pursue this idea further, we develop a decision tree in the next section, which uses combinations of these metrics to determine rules that best differentiate between the classes of the target variable.

4. Classifying networks via a decision tree model

Previously, we analyzed three different types of networks using 16 different network metrics. We observed that some metrics are more useful than others when labeling a network with one of these three types. Although each of these metrics can separately be used for classifying an unknown network, it is obvious that the classes assigned by them are not always the same for a network. Moreover, some of these metrics do not provide clean distinctions and do not reveal much information.

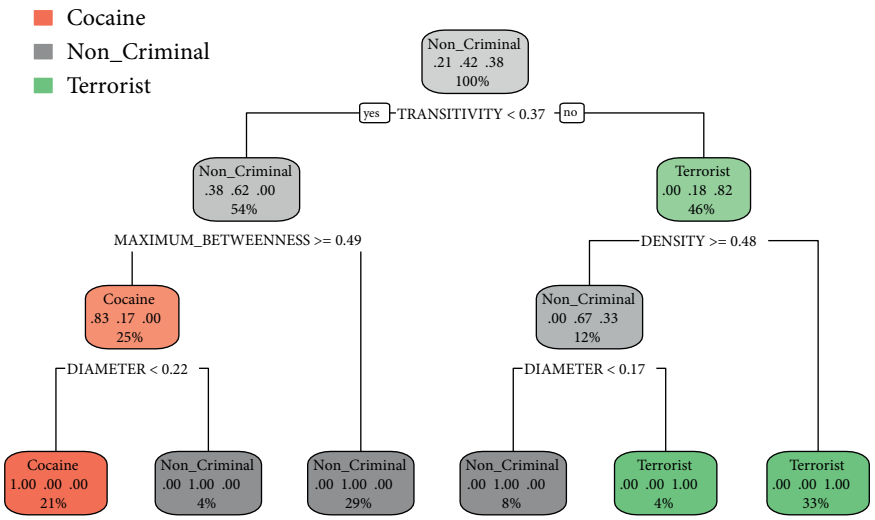
In this section, we employ a machine learning algorithm to train a model that can use these 16 metrics to classify an unknown network. Namely, we employ the `CART` algorithm to create a decision tree based on the 16 values we computed for each network. We use the R language implementation of `CART` that can be found within the `rpart` library.

Figure 9 shows the decision tree we obtained by running the `CART` algorithm on our data. The algorithm nicely groups all three types of networks into their own branches on the tree. The cocaine networks are represented by single leaf nodes, described by transitivity, maximum betweenness, and diameter. In our training dataset, there are 5 cocaine networks and they are uniquely identified in this node.

There are three noncriminal network nodes on the tree. They are described by different combinations of transitivity, maximum betweenness, diameter, and density. These three nodes exclusively cover all noncriminal networks in the training dataset.

Finally, the terrorist networks are defined in two nodes, described by combinations of transitivity, density, and diameter.

The CART algorithm works with 10-fold cross-validation. The complexity parameter (CP) values, relative errors (relerr), cross-validation errors (xerror) (also known as over-fitting), and cross-validation standard deviations (xstd) are given in Figure 9 on the right. The numbers in this table show that the relative error is down to 0, but cross-validation error is not increasing. This is a sign that the tree is not overfitting the data.



CP	relerr	xerror	xstd
0.50000	1.0000	1.1429	0.1650
0.28571	0.5000	0.7857	0.1744
0.07143	0.2143	0.7143	0.1725
0.07143	0.0000	0.6429	0.1694

Figure 9. The decision tree on the left and the corresponding CP table on the right. The decision tree provides a nice classification model with very low relative error values.

The proposed decision tree allows us to do a few things. First of all, it combines all metrics to produce one profound way to determine whether a given network is a cocaine network, a terrorist network, or a noncriminal one. One can easily use this decision tree model to classify an unknown network, such as the ones obtained from call detail records (CDRs), mobile messaging applications, or any other social network platforms. Additionally, it shows the most descriptive characteristics of the examined networks.

5. Motif analysis of network groups

Finally, we look into the criminal networks from a completely different perspective: motifs. Motifs are small subnetworks of size 3 or 4 used to uncover complex networks' structural design principles [20]. Normally, motifs are used with directed graphs. In directed graphs, we have 13 motifs of size 3 and 199 motifs of size 4. In undirected graphs, certain directed motifs correspond to a single undirected motif. Hence, in undirected graphs we have only 2 motifs of size 3, and 6 motifs of size 4, as shown in Figure 10.

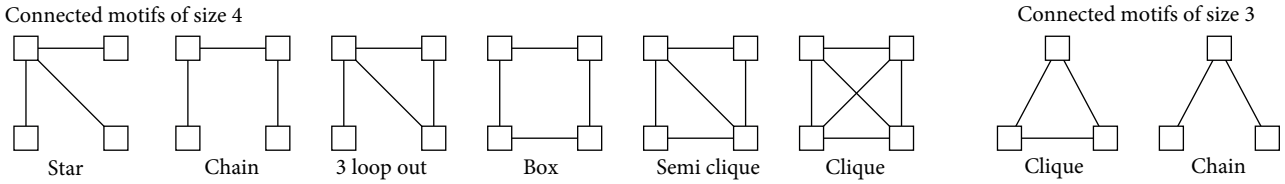


Figure 10. Motifs of size 3 and 4 in undirected networks.

Studies on motifs can be grouped under two titles: motif detection and classification. Motif detection in a graph is well studied and different algorithms are developed for efficiently finding and counting motifs in large networks. Some existing studies on motif search and detection use Mfinder [21], Fanmod [22], Kavosh [23], NemoFinder [24], MODA [25], Grochow [26], and FPF [27]. Classification using motifs is also a very popular topic in the literature. Research shows that the frequency of different motifs can be used to identify the domain of a network or the type of the network within a domain [28]. Motif classification studies are especially popular in biological networks [29–32].

We use motif classification to see whether cocaine, noncriminal, and terrorist networks exhibit different frequency patterns. Since our networks are undirected and we have only two size 3 motifs for undirected networks, we focus on size 4 motifs. Figure 11 shows the average frequencies of size 4 motifs.

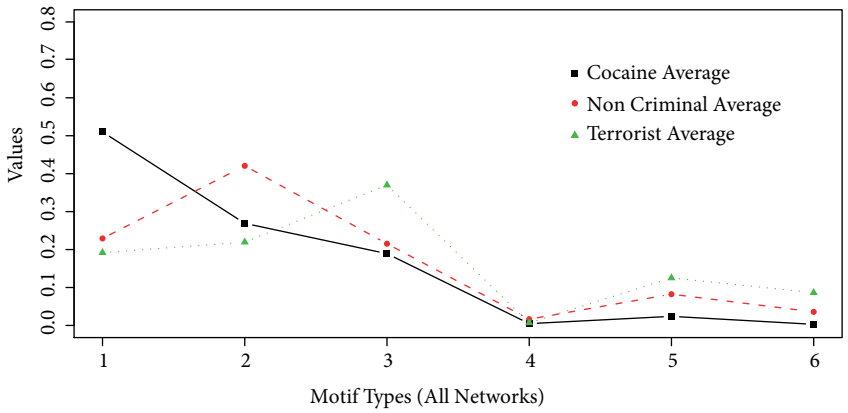


Figure 11. Averages of motif frequencies. There are significant differences between network types, especially in motifs 1, 2, and 3.

This figure clearly outlines the significant differences between the three network types. Especially for the first three motifs, we see that each motif has a different network type topping it. The first motif is mostly visible in cocaine networks, the second motif in noncriminal networks, and the third one in terrorist networks. The fourth motif is very rare in all network types. The fifth and the sixth motifs are relatively more frequent in terrorist networks and are least visible in cocaine networks. This characterization leads us to simple rules with which we can identify the type of an unknown network. Supported with analysis of individual metrics and the decision tree classification, the motif analysis may strengthen the overall classification result.

6. Testing

In this section, we provide some empirical results on actual data. The data we use for our tests are not included in the training data to avoid any bias. The datasets we use for testing are taken from Leuprecht and Hall's study [33]. More specifically, we test with the Minneapolis Recruitment Network (MRN), Australia Recruiting Network (ARN), Minneapolis Fundraising Network (MFN), and St. Louis/San Diego Fundraising Network (SDFN). The decision tree model presented in Section 4 classifies MRN and ARN as terrorist networks, SDFN as a cocaine network, and MFN as a noncriminal network. This shows us that recruitment networks tend to operate more like terrorist organizations, whereas fundraising networks, whose only aim is to provide the monetary support for operations conducted by other networks, operate more like cocaine trading networks. The reason MFN is labeled as a noncriminal network by the decision tree is its diameter value of 0.375, which is greater than 0.22.

We also tested our decision tree model using well-known social network generators: random networks (Erdös–Rényi), preferential attachment networks (Barabási–Albert), small world networks (Watts–Strogatz), and a stochastic block model. Our results indicate that networks generated with the preferential attachment model are identified as cocaine networks, whereas small world networks with small neighborhoods are identified as terrorist networks. If the neighborhood of each node is crowded, small world networks tend to become identified as noncriminal networks. Random networks and SBMs are almost always identified as noncriminal

networks. These findings are in line with the intuition: cocaine networks are constructed around a prominent leader figure and new members join the network via "recruiters", whereas terrorist networks are more distributed and less centralized, growing locally and connecting globally.

Finally, we tested the four criminal networks and four synthetic networks for their motif frequencies. In this case, the results indicate that the star motif is the most important determinant. Using star motif frequencies, ARN, MFN, and SDFN were labeled as criminal networks, similar to the labeling of cocaine trading networks, and MRN as a terrorist network. On the other hand, preferential attachment models were labeled as cocaine trading networks, random networks and SBMs as noncriminal networks, and small world networks as terrorist networks. The chain motif labels all synthetic networks as noncriminal networks and marks MFN, ARN, and SDRN as terrorist networks. MRN was wrongly labeled as a noncriminal network by the chain motif. The "3 loop out" motif marks ARN and small world networks as terrorist networks. The remaining motifs do not provide much information and are ignored.

As a conclusion, our tests show that the decision tree model and the motif frequencies can be used as a reliable decision support mechanism for identifying networks.

Note that, although the relative error of the decision tree model is very low, we do not recommend labeling any network as a criminal network solely based on this study. Any data analysis study is heavily dependent on the availability and the quality of the data. The data we used in this study are neither absolutely correct nor complete. This study aimed to outline the most important descriptive features of criminal networks and the decision tree we proposed may only be used as a final confirmation of a suspicious case.

7. Conclusions

In this paper, we compared three types of networks–noncriminal, cocaine, and terrorist–with respect to well-known social network analysis metrics in order to develop a methodology for classifying an unknown network. We first analyzed each network under each metric. We outlined significant similarities and/or differences between the analyzed networks using each metric. We then combined our results using a machine learning tool, the decision tree, to produce a successful classifier. Finally, we analyzed each network with respect to its motif frequencies. We outlined the differences between different network types.

Individual metrics, the decision tree model, and the motif patterns can work together to classify an unknown network as one of the cocaine, terror, or noncriminal networks. Our results can be employed by security forces in their operations for uncovering hidden criminal organizations from the traces they leave on social networks. Moreover, the general methodology we have applied is applicable to other scenarios that can be modeled using simple graphs. The only requirement is that the subgraph type to be identified needs to show different structural tendencies compared to an average subgraph within the same network. For example, we can extend our work with different types of crime, such as recruitment networks, fundraising networks, street gangs, and fraud networks. Our results may also be used to generate synthetic crime networks. Considering that actual criminal network data are very rare and difficult to access, being able to synthetically produce criminal networks of designated types at varying sizes could be extremely useful for criminal network research.

Our methodology may also be extended to fields other than criminal research. For example, molecular pathways within cells can be modeled as networks and it may be useful to identify different types of pathways from their network structures. As another example, citation networks may be monitored to identify frauds. Basically, our approach is applicable to any network that contains multiple types of subgraphs that differ in their structures.

As a concluding remark, we emphasize once again that the results provided here are only for academic purposes and prone to data-based statistical errors. Hence, no individual or organization can be labeled as guilty or innocent solely based on our studies.

References

[1] Chatfield AT, Reddick CG, Brajawidagda U. Tweeting propaganda, radicalization and recruitment: Islamic State supporters multi-sided twitter networks. In: ACM 16th Annual International Conference on Digital Government Research; 27–30 May 2015; Phoenix, AZ, USA. New York, NY, USA: ACM. pp. 239-249.

[2] Carrington PJ. Crime and social network analysis. In: Scott J, Carrington PJ, editors. The SAGE Handbook of Social Network Analysis. London, UK: SAGE Publications, 2011. pp. 236-255.

[3] Calderoni F. Social network analysis of organized criminal groups. In: Bruinsma G, Weisburd D, editors. Encyclopedia of Criminology and Criminal Justice. New York, NY, USA: Springer, 2014. pp. 4972-4981.

[4] Helbing D, Brockmann D, Chadefaux T, Donnay K, Blanke U, Woolley-Meza O, Moussaid M, Johansson A, Krause J, Schutte S et al. Saving human lives: what complexity science and information systems can contribute. J Stat Phys 2015; 158: 735-781.

[5] Goodarzinick A, Niry MD, Valizadeh A, Perc M. Robustness of functional networks at criticality against structural defects. Phys Rev E 2018; 98: 022312.

[6] Jalili M, Perc M. Information cascades in complex networks. J Complex Netw 2017; 5: 665–693.

[7] Krebs V. Uncloaking terrorist networks. First Monday 2002; 7: 4.

[8] Husslage B, Borm P, Burg T, Hamers H, Lindelauf R. Ranking terrorists in networks: a sensitivity analysis of Al Qaeda's 9/11 attack. Soc Networks 2015; 42: 1-7.

[9] Morselli, C. Inside Criminal Networks. 8th ed. New York, NY, USA: Springer, 2009.

[10] Gutfraind A, Genkin M. A graph database framework for covert network analysis: an application to the Islamic State network in Europe. Soc Networks 2017; 51: 178-188.

[11] Natarajan M. Understanding the structure of a large heroin distribution network: a quantitative analysis of qualitative data. J Quant Criminol 2006; 22: 171-192.

[12] Lupsha PA. Networks versus networking: analysis of an organized crime group. In: Waldo GP, editor. Career Criminals. Beverly Hills, CA, USA: SAGE Publications, 1983. pp. 59-87.

[13] Davis RH. Social network analysis: an aid in conspiracy investigations. FBI Law Enforcement Bulletin 1981; 50: 11-19.

[14] Sparrow MK. The application of network analysis to criminal intelligence: an assessment of the prospects. Soc Networks 1991; 13: 251-274.

[15] Berlusconi G. Social network analysis and crime prevention. In: Leclerc B, Savona E, editors. Crime Prevention in the 21st Century. Cham, Switzerland: Springer, 2017. pp. 129-141.

[16] D'Orsogna MR, Perc M. Statistical physics of crime: a review. Phys Life Rev 2015; 12: 1-21.

[17] Shang X, Yuan Y. Social network analysis in multiple social networks data for criminal group discovery. In: IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC); 10–12 October 2012; Sanya, China. New York, NY, USA: IEEE. pp. 27-30.

[18] Borgatti SP, Everett MG, Freeman LC. Ucinet. In: Alhajj R, Rokne J. editors. Encyclopedia of Social Network Analysis and Mining. New York, NY, USA: Springer, 2014. pp. 2261-2267.

[19] Zachary WW. An information flow model for conflict and fission in small groups. J Anthropol Res 1977; 33: 452-473.

[20] Milo R, Shen-Orr S, Itzkovitz S, Kashtan N, Chklovskii D, Alon U. Network motifs: simple building blocks of complex networks. Science 2002; 298: 824-827.

[21] Kashtan N, Itzkovitz S, Milo R, Alon U. Efficient sampling algorithm for estimating subgraph concentrations and detecting network motifs. Bioinformatics 2004; 20: 1746-1758.

[22] Wernicke S, Rasche F. FANMOD: a tool for fast network motif detection. Bioinformatics 2006; 22: 1152-1153.

[23] Kashani ZRM, Ahrabian H, Elahi E, Nowzari-Dalini A, Ansari ES, Asadi S, Masoudi-Nejad A. Kavosh: a new algorithm for finding network motifs. BMC Bioinformatics 2009; 10: 318.

[24] Chen J, Hsu W, Lee ML, Ng SK. NeMoFinder: dissecting genome-wide protein-protein interactions with meso-scale network motifs. In: ACM 12th SIGKDD International Conference on Knowledge Discovery and Data Mining; 20–23 August 2006; Philadelphia, PA, USA. New York, NY, USA: ACM. pp. 106-115.

[25] Omidi S, Schreiber F, Masoudi-Nejad A. MODA: an efficient algorithm for network motif discovery in biological networks. Genes Genet Syst 2009; 84: 385-395.

[26] Grochow JA, Kellis M. Network motif discovery using subgraph enumeration and symmetry-breaking. In: 11th Annual International Conference on Research in Computational Molecular Biology; 21–25 April 2007; Oakland, CA, USA. Berlin, Germany: Springer. pp. 92-106.

[27] Schreiber F, Schwöbbermeyer H. Frequency concepts and pattern detection for the analysis of motifs in networks. Transactions on Computational Systems Biology III 2005; 3: 89-104

[28] Milo R, Itzkovitz S, Kashtan N, Levitt R, Shen-Orr S, Ayzenshtat I, Alon U. Superfamilies of evolved and designed networks. Science 2004. 303: 1538-1542.

[29] Xiong H, Capurso D, Sen Ś, Segal MR. Sequence-based classification using discriminatory motif feature selection. PLoS One 2011; 6: e27382.

[30] Buza K, Schmidt-Thieme L. Motif-based classification of time series with bayesian networks and svms. In: 32nd Annual Conference of the Gesellschaft für Klassifikation (GfKI 2008); 16–18 July 2008; Hamburg, Germany. Berlin, Germany: Springer. pp. 105-114.

[31] Kunik V, Solan Z, Edelman S, Ruppin E, Horn D. Motif extraction and protein classification.In: Computational Systems Bioinformatics Conference; 8–11 August 2005; Stanford, CA, USA. New York, NY, USA: IEEE. pp. 80-85.

[32] Xing EP, Karp RM. MotifPrototyper: a Bayesian profile model for motif families. P Natl Acad Sci USA 2004; 101: 10523-10528.

[33] Leuprecht C, Hall K. Why terror networks are dissimilar: how structure relates to function. In: Masys AJ, editor. Networks and Network Analysis for Defence and Security. Cham, Switzerland: Springer, 2014. pp. 83-120.