Network Structure Mining: Locating and isolating core members in covert terrorist networks

MUHAMMAD AKRAM SHAIKH, WANG JIAXIN
State Key Laboratory of Intelligent Technology and Systems
Tsinghua National Laboratory for Information Science and Technology
Department of Computer Science And Technology, Tsinghua University, Beijing 100084, China.
akram296@yahoo.com, wjx@mail.tsinghua.edu.cn

Abstract: Knowing patterns of relationship in covert (illegal) networks is very useful for law enforcement agencies and intelligence analysts to investigate collaborations among criminals. Previous studies in network analysis have mostly dealt with overt (legal) networks with transparent structures. Unlike conventional data mining that extracts patterns based on individual data objects, network structure mining is especially suitable for mining a large volume of association data to discover hidden structural patterns in criminal networks. Covert networks share some features with conventional (real world) networks, but they are harder to identify because they mostly hide their illicit activities. After the September 11, 2001 attacks, social network analysis (SNA) has increasingly been used to study criminal networks. However, Finding out who is related to whom on a large scale in a covert network is a complex problem. In this paper we will discuss how network structure mining is applied in the domain of terrorist networks using structural (indices) measures or properties from social network analysis (SNA) and web structural mining research and proposed an algorithm for network disruption. Structural properties are determined by the graph structure of the network. These structural properties are used for locating and isolating core members by using importance ranking score and thereby analyzing the effect to remove these members in terrorist networks. The discussion is supported with a case study of Jemma Islamiah (JI) terrorist network.

Key-Words: Networks, Centrality, Dependency, Rank, Influence, and Destabilization.

1 Introduction

Covert networks such as criminal, money laundering, fraud, smuggling, drug/human trafficking, and terrorist networks often don't behave like normal social networks. They trade efficiency for secrecy. As these networks share some features with conventional networks, they are harder to identify because they mostly hide their illicit activities. Because terrorist networks often operate in a network form in which individual terrorists cooperate and collaborate with each other to carry out attacks [1], we could gain valuable knowledge about the terrorist organizations by studying various structural properties of terrorist networks. Structural properties are determined by the graph structure of the network. These structural properties are used to evaluate the relationship between entities, ranking important actors and identifying different roles. Structural measures can be computed locally (separately for each node) or globally (for an entire network or group). Such knowledge may help authorities develop efficient and effective disruptive strategies and measures.

Covert networks have hidden properties, and our information about them is necessarily incomplete, hence demanding complex methodological tools to correctly classify individuals in these networks so that the resources for isolating them will be used more efficiently.

In this paper we will discuss how network structure mining is applied using structural (indices) measures or properties from social network analysis (SNA) and web structural mining research. These structural properties are used for locating and isolating core members by using importance ranking score in terrorist networks.

The proposed approach is demonstrated by using publicly available data on terrorist networks. The rest of the paper is organized as follows: Section 2 discusses the background; Section 3 gives a brief overview about the network structure mining; Section 4 describes network disruption; Section 5

shows experiments on terrorist network data set of JI for identifying core members according to their ranking score and then discuss in detail how these methods are helpful to disrupt terrorist networks with illustrations; and section 6 concludes the paper.

2 Background

Law enforcement personnel have used social networks to analyze terrorist networks [1,3] and criminal networks [4]. The capture of Saddam Hussein was facilitated by SNA: military officials constructed a network containing Hussein's tribal and family links, allowing them to focus on individuals who had close ties to Hussein [5]. SNA, originating from social science research, is a set of analytical tools that can be used to map networks of relationships and provides an important means of assessing and promoting collaboration in strategically important groups [6]. SNA provides a set of descriptive measures and approaches for the investigation of terrorist networks. These techniques were originally designed to discover social structures in social networks [2] and are especially appropriate for studying criminal networks [7,8,9]. Specifically, in the literature the use of centrality and structural equivalence measures from SNA are used to measure the importance of each network member. Several centrality measures, such as degree, betweenness, closeness, and eigenvector, can suggest the importance of a node [2] and can identify the leaders, gatekeepers, and outliers in a network [10]. Baker and Faulkner [11] employed these measures, especially degree, to find the central individuals in a price-fixing conspiracy network in the electrical equipment industry. In addition to these measures we will discussed how the use of dependence centrality concept is useful in identifying core members and thereby isolating them in terrorist networks domain. Dependence centrality [12] represents how much a node is dependent on other nodes while communicating along geodesics to and from all other reachable nodes in the network. Recently Jialun Qin et al. [10] have also introduced web structural mining in counterterrorism domain. They have used Page Rank algorithm in order to find important nodes in terrorist networks.

3 Network Structure Mining

Network structure mining is especially suitable for mining a large volume of association data to discover hidden structural patterns in criminal networks using structural (indices) measures or properties from social network analysis (SNA) and web structural mining research.
Please, leave two blank lines between successive sections as here.

3.1 Social Network Analysis

Social network analysis (SNA) primarily focuses on applying descriptive techniques to the relationships between individuals and groups, and investigating how those relationships can be used to infer additional information about the individuals and groups [13] in a network. In SNA studies, a network is usually represented as a graph, which contains a number of nodes (network members) connected by links (relationships). Several centrality measures can be used to identify key members who play important roles in a network. Most of the centrality measures are based on shortest paths, measuring, e.g., the average distance from other vertices (nodes) or the ratio of shortest paths a vertex (node) lies on. Freeman [14] provided the basic definitions of the three most popular centrality measures: degree, betweenness, and closeness. In general, the network studied in this paper can be represented by an undirected and un-weighted graph G =(V, E), where V is the set of vertices (or nodes) and E is the set of edges (or links). Each edge connects exactly one pair of vertices, and a vertex pair can be connected by (a maximum of) one edge, i.e., multi-connection is not allowed. A terrorist network consists of V set of actors (nodes) and E relations (ties or edges) between these actors. Mathematically, a network can be represented by an adjacency matrix A, which in the simplest case is an N ×N symmetric matrix, where N is the number of vertices in the network. The adjacency matrix has elements.

$$A_{ij} = \begin{cases} 1 & \text{if i and j are connected,} \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

The matrix is symmetric since if there is an edge between *i* and *j* then clearly there is also an edge between j and i. Thus

$$A_{ij} = A_{ji} \quad (2)$$

The **degree** of a vertex in a network is the number of edges attached to it. In mathematical terms, the degree 'D_i' of a vertex *i* is [14]:

$$D_i = \sum_{j=1}^{n} A_{ij} \quad (3)$$

A network member with a high degree could be the leader or "hub" in a network.

Betweenness measures the extent to which a particular node lies between other nodes in a network [23]. The betweenness 'B_a' of a node '*a*' is defined as the number of geodesics (shortest paths between two nodes) passing through it:

$$B_a = \sum_{i}^{n} \sum_{j}^{n} g_{ij}(a) \quad (4)$$

Where $g_{ij}(a)$ indicates whether the shortest path between two other nodes *i* and *j* passes through node '*a*'. A member with high betweenness may act as a gatekeeper or "broker" in a network for smooth communication or flow of goods (e.g., money, arms).

Closeness 'C_a' is the sum of the length of geodesics between a particular node '*a*' and all the other nodes in a network. It actually measures how far away one node is from other nodes and is sometimes called farness [11,14,23]:

$$C_a = \sum_{i=1}^{n} l(i,a), \quad (5)$$

Where *l(i,a)*, is the length of the shortest path connecting nodes *i* and *a*. The most central nodes can quickly interact with all the other nodes because they are close to all the others.

Both Closeness and Betweenness centralities are global measures, where as degree centrality is termed as local measure. Note that all these measures are relative ones. These three centrality measures may produce contrary results for the same graph. It can be a case in which an actor has a low degree centrality, with a high betweenness centrality. Freeman [14] also shows that the betweenness centralities best "capture" the essence of important nodes in a graph, and generate the largest node variances, while degree centralities appear to produce the smallest node variances. In order to overcome the drawbacks of single centrality, here we used the concept of Combine Centrality Actor Ranking (CCR) as shown in equation (6) using the combination of degree, closeness and betweenness from equations (3), (4), and (5):

$$CCR = D_i + B_a + C_a \quad (6)$$

The **Eigen vector centrality** approach to order the vertices (nodes) of a graph was suggested by Bonacich [15]. His idea is based on the assumption that the value of a single vertex is determined by the values of the neighboring vertices. Network nodes can be ranked using Eigenvector Centrality calculation. Centrality is defined using the following formulas [24, 25]:

$$v_i \propto \sum_{j=N(i)} v_j \quad (7)$$

Which can be also written as:

$$v_i \propto \sum_{j=N(i)} A_{ij} v_j \quad (8)$$

We can rewrite this equation in matrix form as:

$$A\vec{v} = \lambda\vec{v} \quad (9)$$

Where *N(i)* is the number of nodes, v_i is the vector for the importance ranking, and *A* is the adjacency matrix, a table of values reflecting the adjacency of nodes, i.e. what neighboring, or adjacent, nodes are connected to other nodes of the network, and λ is the eigen value of that matrix.

A square matrix has as many eigenvectors and corresponding eigen values as the matrix dimensions. The so called principle eigen vector is what is needed in this calculation. The principle eigenvector is identified by searching for the highest eigen value from the calculation in equation (9). Using this equation, n (as is the dimension of the matrix) eigenvectors and eigen values are obtained. We are interested in the principle eigen vector. The principle eigenvector is the one with the highest eigenvalue. After that vector is located, it is sorted by ranking value. This way the most important nodes, i.e. nodes with highest ranking value, are found on top of the list.

The pair dependency concept in networks was first given by Freeman, L.C. [12]. Dependence centrality represents how much a node is dependent on other nodes in a network. It can be defined as "How dependent is node '*p*' to another node '*q*' while communicating along geodesics to and from all other reachable nodes in the network". Consider an undirected and un-weighted simple network representing a symmetrical relation, "communicates

with" for a set of 6 nodes as shown in Fig.1. When a pair of nodes (say, *p* and *q*) is linked by an edge so that they can communicate directly without intermediaries, they are said to be adjacent. A set of edges linking two or more nodes (*p*, *q*, *r*), such that node *p* would like to communicate with *r*, using node *q*, the dependence centrality can discover how many times node p uses node *q* to reach node *r* and how many shortest paths node *p* uses to reach node *r*. There can, of course, be more than one geodesic, linking any pair of nodes.

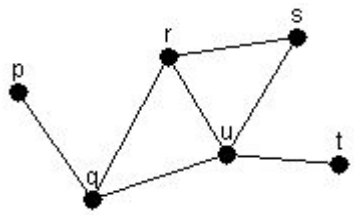

Fig.1. A Simple Network

Now let g_{pr} = the number of geodesics (shortest paths b/w two nodes) linking nodes *p* and *r*, and $g_{pr}(q)$ = the number of such geodesics that contain node *q* as a mediator between *p* and *r* then we can write:

$$b_{pr}(q) = \frac{g_{pr}(q)}{g_{pr}} \qquad (10)$$

Thus $b_{pr}(q)$ is the proportion of geodesics linking *p* and *r* that contain *q*; it is an index of the degree to which nodes *p* and *r* need *q* for the communication along the shortest path linking them together.

The dependency is thus defined as the degree to which a node, *p*, must depend upon another node, *q*, to relay its messages along geodesics to and from all other reachable nodes in the network. Thus, for a connected network having n nodes, the dependency of *p* on *q* can be written as:

$$d_{pq} = \sum_{r=1}^{n} b_{pr}(q), \qquad (p \neq q \neq r) \quad (11)$$

The dependency values of each node on every other node in the network are calculated and thus are arranged in a matrix form as shown in Table 1. Each entry in the matrix is an index of the degree to which the node designated by the row of the matrix must depend on the node designated by the column to transmit messages to and from others. Thus the resulted matrix captures the importance of each node as a mediator with respect to each other node, facilitating its communication.

Table 1. Dependency Matrix of the Simple Network

NODE LABELS	*p*	*q*	*r*	*s*	*t*	*u*	Sum/(n-1)
p	0	4	0.5	0	0	1.5	1.2
q	0	0	0.5	0	0	1.5	0.4
r	0	1	0	0	0	1	0.4
s	0	1	1	0	0	2	0.8
t	0	1	0	0	0	4	1
u	0	1	0	0	0	0	0.2
SUM/(N-1)	0	1.8	0.4	0	0	1.8	

Consider two nodes *p* and *q* in Fig.1; we want to know how much node *p* is dependent on node *q* and vice versa. It is observed from the matrix that node *p* whose dependency score with *q* is 4 (row 1 & column 2), is totally dependent on *q* to reach to all other nodes in the network, whereas node *q* whose dependency score is zero (row 2 & column 1) is not dependent on *p*, since both *p* and *q* are adjacent nodes and can reach directly.

The dependency values arranged in this form of rows and columns of a matrix are then be summed up to get the dependency rank for individual nodes as shown in Table 1. The dependency centrality can be normalized by dividing each value with *(n-1)* where *n* is the total number of nodes in the network.

In Table 1, it is observed that the lowest sum of values in a row (such as node *u*) points out that the nodes that are most difficult to be deactivated, as its communications are least damaged with the capture of other nodes. These nodes are least dependent on others and are termed as most important nodes. Their communications are uniformly distributed. Whereas the highest sum of values in a row (such as node *p*) pointing to those nodes that can be easily deactivated. These nodes are mostly dependent on others and are termed as less important.

However the lowest sum of values (such as nodes *p*, *s*, and *t*) in a column tells us that minimum communication takes place through these nodes. The capture of these nodes will be of least damage for a network. Whereas the largest sum of values (such as node *u* and *q*) in a column points out the

nodes whose capture would be highly disruptive to the network.
Table 2, shows the betweeness values of the simple network as shown in Fig. 1.
One can observed in Table 2 that nodes *p, s, t* have betweeness score zero, as these nodes least participated between the communication paths. One can only know that the remaining nodes in the network are least dependent on these nodes for the communication process. While if we look on the dependence matrix as shown in Table 1, one can guess how much p, s, t is dependent on other nodes and how much other nodes are dependent on these nodes.

Table 2. Betweeness Score of the simple network of six nodes

Node Id	Betweeness	Node Id	Betweeness
p	0	*s*	0
q	0.4	*t*	0
r	0.1	*u*	0.5

3.2 Web Structural Analysis

The PageRank algorithm, which was developed by [16], was originally designed for directed and unweighted graphs to calculate the importance of Web pages based on the Web link structure and is used in the commercial search engine Google [16] to rank the search results. However, it can also be used to determine the importance of social actors in a proper social network where links imply similar "recommendation" or "endorsement" relationships as the hyperlinks in Web graph. In a co-authorship network, a link between authors implies the mutual endorsement relationship between them and the PageRank algorithm can be used to rank the authors based their importance in this co-authorship network. In the co-authorship analysis study conducted by Liu et al. [17], PageRank was used as one of the author ranking criteria along with other traditional SNA centrality measures.
The PageRank algorithm is computed by weighting each incoming-link to a page proportionally to the quality of the page containing that incoming-link [18]. The quality of these referring pages is also determined by PageRank. Formally let $G = (V, E)$ be a directed graph with the set of vertices V and a set of edges E, where E is a subset of VxV. For a given V_i, let $In(V_i)$ be the set of vertices that point to it, and let $Out(V_i)$ be the set of edges going out of vertex V_i. The PageRank score of vertex V_i is:

$$PageRank(V_i) = (1-d) \times d \sum_{j \in In(V_i)} \frac{PageRank(V_j)}{|Out(V_j)|} \quad (12)$$

Where d is a damping factor that can be set between 0 and 1, and usually set at 0.85 [16].

Covert networks can be represented as graphs, in which actors are defined as vertices, and relations between actors are defined as edges. The graph can be constructed as an undirected and unweighted graph. For the case of undirected graph, in equation (12), we consider out degree of the vertex is equal to in degree of the vertex. Thus the modified PageRank algorithm for undirected graph, known as ImpRank is given by the formula:

$$ImpRank(V_i) = (1-d) \times d \sum_{V_j \in C(V_i)} \frac{ImpRank(V_j)}{|k(V_j)|} \quad \text{Where } i = 1, ..., N \quad (13)$$

$C(V_i)$ is the set of edges connecting with V_j, and $k(V_j)$ is the degree of vertex V_j. We also consider damping factor equal to 0.85 for ImpRank calculations.

4 Network Disruption

Disruption techniques traditionally aim at neutralizing members of terrorist networks either through capture or death. These nodes are known as the 'critical' nodes within a network [22]. The removal or isolation of these nodes ensures maximum damage to the network's ability to adapt, performance, and ability to communicate. In network analysis, node changes are the standard approach to network destabilization [4]. Kathleen Carley et al. proposed three indicators of network disruption [19]:
– The rate of information flow through the network has been minimized (perhaps to zero).
– The network, as a decision making body, cannot reach on a joint consensus.
– The ability of the network to accomplish tasks is totally impaired.

4.1 Algorithm for Network Disruption

The algorithm for network disruption is as follows:

Input: A connected network/graph

Output: A disconnected network/graph

1. Compute the Node Importance Score of every node in a network except isolates

using different measures (CCR, EVC, Node Dependency, and ImpRank)

2. Rank the nodes in decreasing order of their node importance scores

3. Remove nodes and their associated links having high importance score

5 Experiments

In this section, the network structure mining concept is demonstrated using the information from open source data (GSJ global salafi jihad terrorist network) collected by Marc Sageman [20]. A subset of 50 members, who were identified as members of the Jemaah Islamiah (JI) terrorist network is used here as a case study.

5.1 Description of JI Data Set

Jemaah Islamiah (JI) is a terrorist group based in Southeast Asia. The attack by JI on a nightclub in Bali in 2002 brought the group to the world's attention. The JI data used in this demonstration is a subset of 50 terrorists as shown in Fig.2, which is drawn using NetDraw [21]. The data also captures all known relationships and interactions between terrorists. However for this study the network is constructed using relations include discipleship, worship, familial, relative, friend, and acquaintance networks. The isolates in this network are not considered and only the connected part of the network is considered in this study. The names of JI members are shown by numbered index in Table 3.

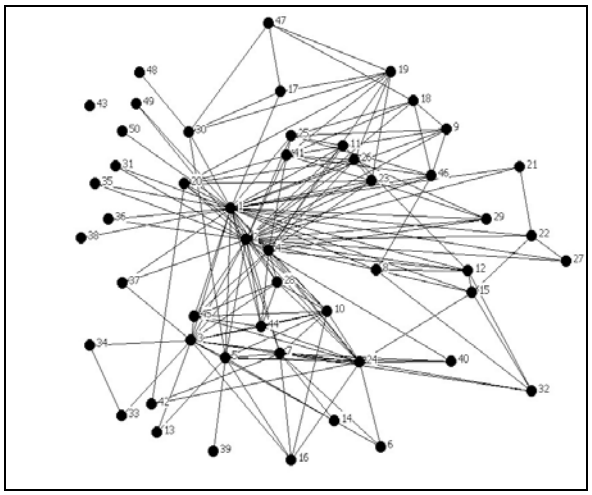

Fig.2. The terrorist network of Jemmah Islamiah (JI) members

Table 3. JI names by numbered index

NODE ID	NAME	NODE ID	NAME
1	Baasyir	26	Top
2	Sungkar	27	Idris
3	Hambali	28	Mustofa
4	Mukhlas	29	WanMin
5	Iqbal	30	Maidin
6	Faruq	31	Sani
7	Syawal	32	Dulmatin
8	Ghozi	33	Farik
9	Samudra	34	Lillie
10	Jabir	35	Yunos2
11	Amrozi	36	Naharudin
12	Imron	37	Gungun
13	Sufaat	38	Marzuki
14	Dwikarna	39	Kastari
15	Mobarok	40	Hafidh
16	Yunos	41	Abbas
17	Mistooki	42	Setiono
18	Faiz	43	BinHir
19	Hasyim	44	Rusdan
20	Sulaeman	45	Mustaqim
21	Hussein	46	Muhajir
22	Ayub	47	Fathi
23	Azahari	48	Khalim
24	Zulkarnaen	49	Roche
25	Ghoni	50	Thomas

5.2 Centrality Measures from SNA

As discussed in section 3.1, here we apply these measures on the Jemmah Islamia network as shown in Fig.2, in order to find out the most important nodes and rank them in decreasing order of their importance score. CCR and EVC scores are shown in Fig.3 and Fig.4 respectively, in which nodes are ranked according to decreasing order of their importance scores. If we analyze the data summarized in Fig.3 and Fig.4 resprctively, we conclude that node id 1 & 2 (Baasyir & Sungkar) may be the top leader of the network based on high CCR and EVC scores.

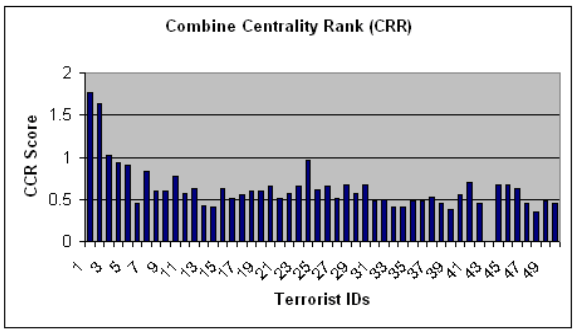

Fig.3. Combine Centrality Rank Score

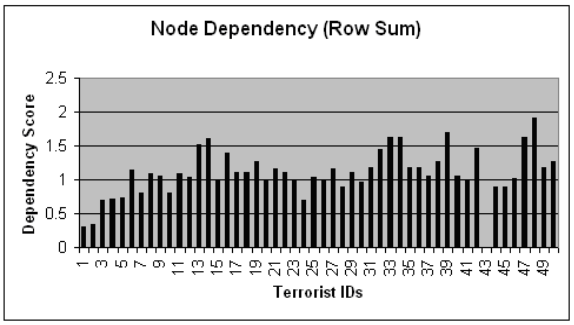

Fig.5. Dependency Rank Score (Row Sum)

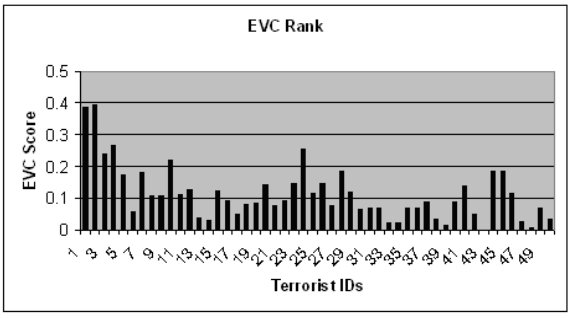

Fig.4. Eigen Vector Centrality Rank Score

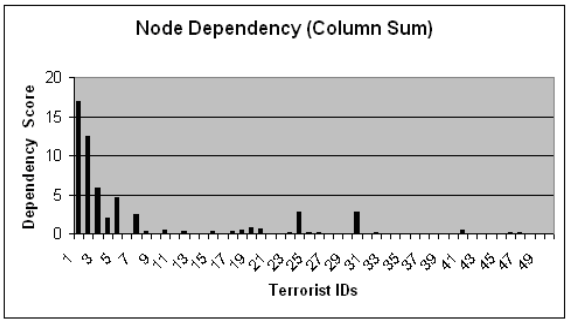

Fig.6. Dependency Rank Score (Column Sum)

As discussed earlier, dependence centrality represents how much a node is dependent on other nodes in a network [12]. Due to space constraints the dependency matrix 50X50 is not shown in this paper and only the sum of rows and columns are considered and plotted in Fig.5 and Fig.6 respectively, for the understanding of dependence centrality concept. The dependency matrix captures the importance of each node as a gatekeeper (broker or mediator) with respect to each other node, facilitating or perhaps inhibiting its communication.
The lowest sum of values in a row points out that the nodes (such as nodes 1 and 2) that are most difficult to be deactivated, as its communications are least damaged with the capture of other nodes. These nodes are least dependent on others. Its communications are uniformly distributed. Whereas the highest sum of values in a row points out nodes that can be easily deactivated (such as nodes 48,33 and 34). These nodes are mostly dependent on others.
The lowest sum of values in a column tells us that minimum communication takes place through these nodes. The capture of these nodes will be of least damage for a network. Whereas the largest sum of values in a column points out the nodes whose capture would be most disruptive the network (like nodes 1 and 2). Node 43 (BinHir) is an isolate, so we don't consider this node in the analysis.

5.3 Web Structural Analysis

As discussed above PageRank can also be used to rank the importance of terrorists within a properly constructed terrorist network. Fig.7 shows ranking of nodes according to newly developed ImpRank algorithm. The analysis of ImpRank scores of individual nodes as shown in Table 4, also suggests the highest rank of node# 1 (Baasyir) whereas node # 2 (Sungkar) comes on the second rank. These findings also confirm the real facts about the JI network leadership [20].

5.4 Network Disruption

The structural criteria outlined above allow the identification of the most important and well connected individuals within a network, through their high ranking scores. These nodes are known as the 'critical' nodes within a network. The removal or isolation of these nodes ensures maximum damage to the network's ability to adapt, performance, and ability to communicate.
After applying our proposed algorithm of network disruption as discussed in section 4 and considering metric quantities (CCR, EVC, Node Dependency, and ImpRank Scores), the individuals who are key in the JI terrorist network are identified (blue nodes) and are removed as shown in Fig.8. After removing the ten most important actors as proposed by CCR,

EVC, Dependency Rank, and ImpRank scores (nodes #1,2,3,4,5,7,12,20,24,46), which is only 20% of the total nodes the shape of the disconnected terrorist network is shown in Fig.9. This suggests that how just identifying and isolating few nodes can give a great harm to the network.

Table 4. ImpRank score of individual nodes in JI network

Node Id	ImpRank	Node Id	ImpRank
1	0.093	26	0.022
2	0.085	27	0.01
3	0.046	28	0.021
4	0.041	29	0.014
5	0.037	30	0.022
6	0.01	31	0.008
7	0.034	32	0.015
8	0.018	33	0.01
9	0.017	34	0.01
10	0.029	35	0.008
11	0.015	36	0.008
12	0.02	37	0.01
13	0.008	38	0.005
14	0.008	39	0.006
15	0.02	40	0.013
16	0.015	41	0.027
17	0.014	42	0.01
18	0.018	43	0.003
19	0.024	44	0.021
20	0.022	45	0.021
21	0.01	46	0.02
22	0.016	47	0.014
23	0.022	48	0.006
24	0.042	49	0.008
25	0.02	50	0.005

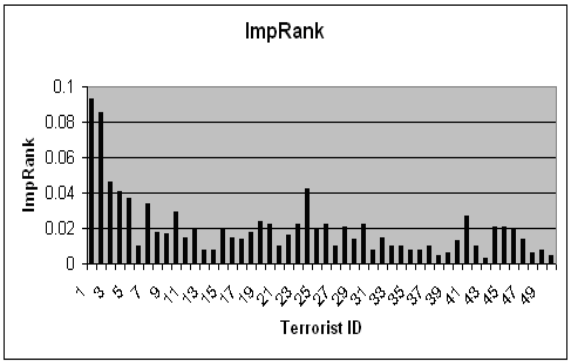

Fig.7. Ranking according ImpRank Score

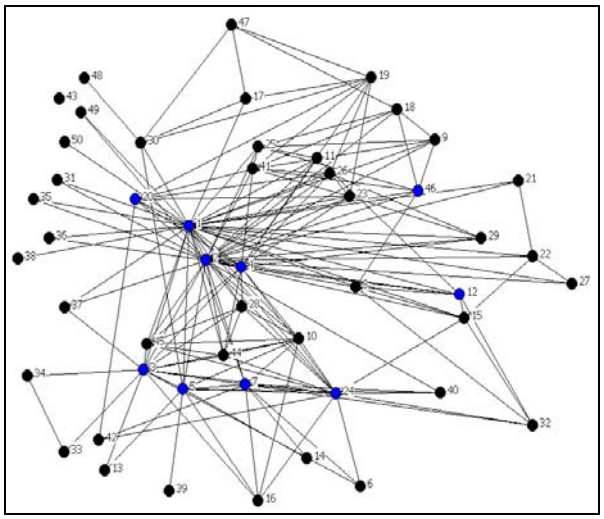

Fig.8. The terrorist network of JI showing core members (blue nodes)

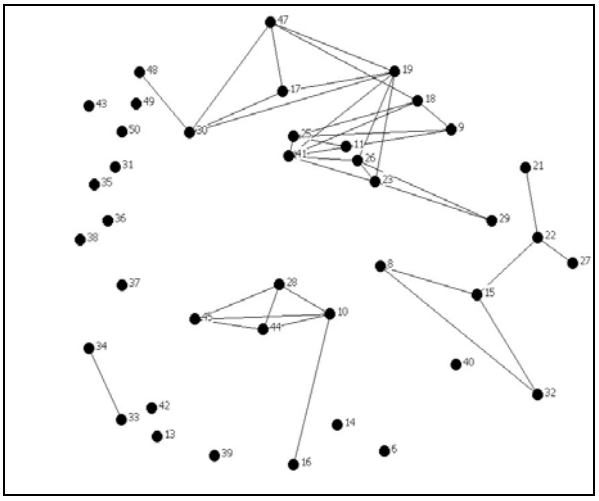

Fig.9. Network's disruption by removing core members

6 Conclusions

In this study, we have applied network structure mining in analyzing structural properties of the terrorist networks. Our goal was to locate and isolate core members using existing and newly developed techniques in order to destabilize these networks. For demonstration purpose, dataset of JI terrorist network was used as a case study. The analysis results showed that descriptive measures from SNA field are effective tools to identify key members in a terrorist network. Especially we have explained in detail the concept of dependence centrality and also proposed a new rank method CCR, and shows how this concept will help law enforcement agencies and intelligence analysts in dealing with terrorist networks. Secondly the web structural analysis such as PageRank can also be

used to rank the importance of terrorists within a properly constructed terrorist network. For this we have developed a new method ImpRank. The overall findings also confirm the real facts about the JI network leadership [20].

Our main focus of this research was to study and analyze the structure of terrorist networks in order to devise some useful methods for destabilizing these covert networks and to assist law enforcement and intelligence agencies to fight against terrorism. Moreover this research also endows the analyst, the ability to measure the level of covertness and efficiency of the network as a whole, and also the level of activity, ability to access others, and the level of control over a network each individual possesses. The measurement of these criteria allows specific counterterrorism applications to be drawn, and assists in the assessment of the most effective methods of disrupting and neutralizing a terrorist network. As has been demonstrated, by removing nodes that are of critical structural importance to the network, the information and communication flow will be significantly disrupt within the network, and likewise to reduce the decision making capability and the effectiveness of the network.

References:

[1] Krebs, V. E., Mapping networks of terrorist cells. Connections 24(3), 2001, 43-52.

[2] McIllwain, J.S., Organized crime: A social network approach. Crime, Law & Social Change 32, 301–323.

[3] Stewart, T., Six degrees of mohamed atta, 2001, (accessed on March 10, 2007), http://money.cnn.com/magazines/business2

[4] Borgatti, S., The key player problem. In: Proceedings from National Academy of Sciences Workshop on Terrorism, Washington DC, 2002.

[5] Hougham, V., Sociological skills used in the capture of saddam Hussein, 1991, (accessed on october 6, 2007), http://www.asanet.org/footnotes/julyaugust05/fn3.html

[6] Chan, K., Liebowitz, J., The synergy of social network analysis and knowledge mapping: a case study. Int. J. Management and Decision Making 7(1), 2006, 19–35.

[7] Wasserman, S., Faust, K., Social Network Analysis: Methods and Applications, Cambridge University Press, Cambridge, 1994.

[8] McAndrew,D., The structural analysis of criminal networks. In:Canter,D.,Alison, L. (eds.) The Social Psychology of Crime: Groups, Teams, and Networks, Offender Profiling Series, III, Aldershot, Dartmouth, 1999, pp. 53–94

[9] Sparrow, M.K., The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks 13, 1991, 251–274.

[10] Qin, J., et al., Analyzing terrorist networks: A case study of the global salafi jihad network. In:Kantor,P.,Muresan,G.,Roberts,F.,Zeng,D.D., Wang,F.-Y.,Chen, H., Merkle, R.C. (eds.) ISI. LNCS, vol. 3495, 2005, pp. 287–304. Springer, Heidelberg.

[11] Baker,W.E.,Faulkner,R.R., The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. American Sociological Review 58(12), 1993, 837–860.

[12] Freeman, L.C., The gatekeeper, pair-dependency, and structural centrality. Quality and Quantity. 14, 1980, 585-592.

[13] Degenne, A. & Forse, M., Introducing Social Networks. London: Sage Publications, 1999.

[14] L. C. Freeman, Centrality in social networks: Conceptual clarification, Social Networks 1, 1999, 215-239.

[15] Bonacich, P., Factoring and weighting approaches to status scores and clique identification. Journal of Mathematical Sociology 2, 1972,113–120.

[16] Brin, S., Page, L, The Anatomy of a Large-Scale Hypertextual Web Search Engine. Computer Networks and ISDN Systems 30, 1998, 1–7.

[17] Liu, X., Bollen, J., Nelson, M. L., Van de Sompel, H., All in the Family? A Co-Authorship Analysis of JCDL Conferences (1994-2003). Proceedings of the IEEE/ACM Joint Conference on Digital Libraries 2004, Tucson, AZ

[18] Cho, J., Garcia-Molina, H., Page, L., Efficient Crawling through URL Ordering. Proceedings of the 7th International WWW Conference, Brisbane, Australia, 1998.

[19] Kathleen, C.M., Lee Ju-Sung, D.K., Destabilizing networks. Connections 24(3), 2002,79–92.

[20] Sageman, Marc, Understanding Terror Networks. University of Pennsylvania Press, 2004.

[21] Borgatti, S.P., NetDraw Ver.2.073, 2008, Computer Software, Analytic Technologies, Harvard, Home page: http://www.analytictech.com/

[22] Memon, N., Larsen, H.L., Structural Analysis and Mathematical Methods for Destabilizing

Terrorist Networks. In: Li, X., Zaïane, O.R., Li, Z. (eds.) ADMA 2006. LNCS (LNAI), vol. 4093, pp. 1037–1048. Springer, Heidelberg

[23] Jennifer J. Xu and Hsinchun Chen. "CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery", ACM Transactions on Information Systems, Vol. 23, No. 2, April 2005, Pages 201–226.

[24] M. Burgess, Analytical Network and System Administration, Wiley, 2004 ISBN 0-470-86100-2.

[25] Ilir Bytyci, Monitoring Changes in the Stability of Networks Using Eigenvector Centrality [Master Thesis], Oslo University College, 2006