Retracted: Structural Analysis and Mathematical Methods for Destabilizing Terrorist Networks Using Investigative Data Mining

Nasrullah Memon and Henrik Legind Larsen

Software Intelligence Security Research Center
Department of Software, Electronics and Media Technology
Aalborg Universitet Esbjerg
Niels Bohrs Vej 8, 6700 Esbjerg Denmark
{nasrullah, legind}@cs.aaue.dk

Abstract. This paper uses measures of structural cohesion from social network analysis (SNA) literature to discuss how to destabilize terrorist networks by visualizing participation index of various terrorists in the dataset. Structural cohesion is defined as the minimum number of terrorists, who if removed from the group, would disconnect the group. We tested bottom-up measures from SNA (cliques, n-cliques, n-clans and k-plex) using dataset of 9-11 terrorist network, and found that Mohamed Atta, who was known as ring leader of the plot, participated maximum number of groups generated by the structural cohesion measures.

We discuss the results of recently introduced algorithms for constructing hierarchy of terrorist networks, so that investigators can view the structure of non-hierarchical organizations, in order to destabilize terrorist networks. Based upon the degree centrality, eigenvector centrality, and dependence centrality measures, a method is proposed to construct the hierarchical structure of complex networks. It is tested on the September 11, 2001 terrorist network constructed by Valdis Krebs. In addition we also briefly discuss various roles in the network i.e., position role index, which discovers various positions in the network, for example, leaders / brokers and followers.

1 Introduction

This paper introduces and studies the investigative data mining techniques; for example, cohesion analysis, role analysis and power analysis; and propose to construct hierarchy of non-hierarchical networks. (These analysis techniques are borrowed from social networks and graph theory.) In addition we also propose a mathematical method to find various position roles in the networks, for example, leaders, brokers and followers.

Cohesion analysis (also called structural cohesion) is often used to explain and develop sociological theories. Members of a cohesive subgroup tend to share information, have homogeneity of thought, identity, beliefs, behavior, even food habits and illnesses (Wasserman, S., Faust, K, 1994). Cohesion analysis is also believed to influence emergence of consensus among group members. Examples of cohesive sub-

X. Li, O.R. Zaiane, and Z. Li (Eds.): ADMA 2006, LNAI 4093, pp. 1037 – 1048, 2006.

groups include religious cults, terrorist cells, criminal gangs, military platoons, tribal groups and work groups etc.

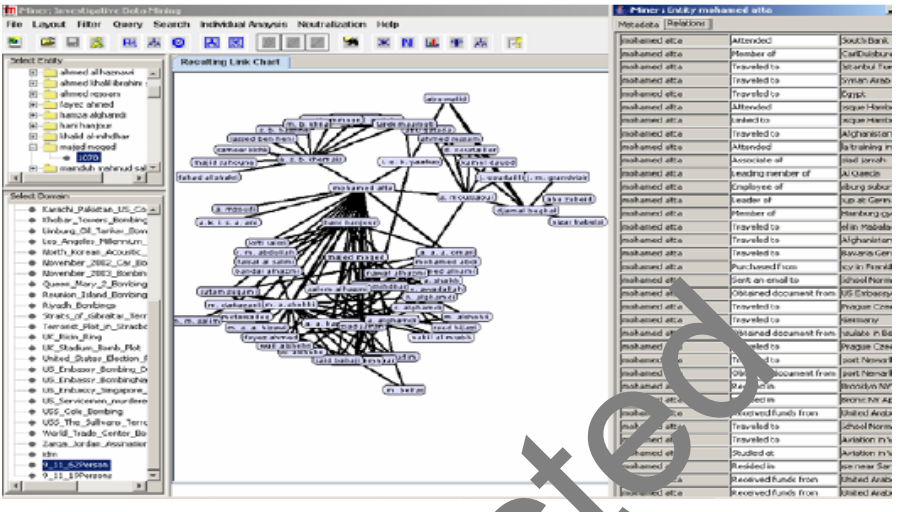

Fig. 1. The dataset of 9-11 hijackers and their affiliates. The dataset originally constructed by Valdis Krebs, but re-constructed in our investigative data mining prototype i.e. iMiner, using meta data of every terrorist.

Role analysis can be used for finding various roles in a network. On the other hand, *power analysis* is used to discover who is powerful / influential in the network.

Some direct application areas of social networks include studying terrorist networks (Sageman, M., 2004, Berry, N. et al., 2004), which is essentially an special application of criminal network analysis that is intended to study organized crimes such as terrorism, drug trafficking and money laundering (McAndrew, D., 1999, Davis, R. H., 1981). Concepts of social network analysis provide suitable data mining tools for this purpose (Chen, H., et al., 2004).

Figure 1 shows an example of a terrorist network, which maps the links between terrorists involved in the tragic events of September 11, 2001. This graph was constructed by Valdis Krebs (Krebs, V., 2002) using the public data that were available before, but collected after the event. Even though the information mapped in this network is by no means complete, its analysis may still provide valuable insights into the structure of a terrorist organization. This graph is reconstructed in this paper, using metadata of every terrorist involved in the attacks, using our investigative data mining software prototype known as iMiner.

The remainder of the paper is organized as follows: Section 2 discusses the background; Section 3 introduces about Investigative Data Mining and Social Network Analysis techniques. The Section 4 discusses practical approaches for neutralizing terrorist networks and Section 5 concludes the paper.

2 Background

After tragic terrorist attacks by kidnapped airlines on New York and Washington in September 2001 the interest for Al Qaeda in public and media rose immediately. Experts and analysts all over the world started to offer various explanations of Al Qaeda's origins, membership recruitment, modes of operation, as well as of possible ways of its disruption. Journalists in search of hot topics took over and publicized most of the publicly available materials, often revising them further and making them even more exciting and attractive for wide audiences.

One could thus read or hear that Al Qaeda is "a net that contains independent intelligence", that it "functions as a swarm", that it "gathers from nowhere and disappears after action", that it is "an ad hoc network", "an atypical organization" (Memon N., H. L. Larsen, 2006), extremely hard to destroy, especially by traditional anti-terrorist / counterterrorist methods.

One common criticism of efforts for analyzing terrorism by focusing on tensions in defined hierarchies is to argue that the current terrorist threat is not organized with clear lines of authority. Instead they are organized as loose networks and so belong to an analytically distinct category. According to many counterterrorism analysts today, Al Qaeda has evolved from a centrally directed organization into a worldwide franchiser of terrorist attacks (Grier P., 2005). Since war in Afghanistan, which significantly degraded Osama bin Laden's command and control, Al Qaeda does appear to have become increasingly decentralized. It is now seen by many as more of a social movement than coherent organization (Wikotorowicz Q., 2001).

Al Qaeda did not decide to decentralize until 2002, following the ouster of the Taliban from Afghanistan and the arrest of a number of key Al Qaeda leaders including Abu Zubaydhah, Al Qaeda's Dean of students, Ramzi bin Al Shibh, the organizer of the Hamburg cell of 9/11 hijackers, Khalid Sheikh Mohammed, the mastermind of 9/11 and the financier of the first World Trade Center attack, and Tawfiq Attash Kallad, the master mind of the USS Cole attack.

In response these and other key losses, Al Qaeda allegedly convened a strategic summit in northern Iran in November 2002, at which the group's consultative council decided that it could no longer operate as a hierarchy, but instead would have to decentralize (Joseph Felter et. al., 2005).

There is a need for tools which construct these non-hierarchical networks into hierarchical form, so that intelligence agencies and law enforcement officers can easily understand the structure of an organization.

Our recently introduced approaches and algorithms for Investigative Data Mining in the context of counterterrorism and homeland security (Memon, N., Larsen H. L., 2006) will be particularly useful for law enforcement and intelligence agencies that need to analyze terrorist networks and prioritize their targets.

3 Investigative Data Mining

Investigative Data Mining (IDM) offers the ability to firstly map a covert cell, and to secondly measure the specific structural and interactional criteria of such a cell. This framework aims to connect the dots between individuals and "map and measure

complex, covert, human groups and organisations". The method focuses on uncovering the patterning of people's interaction, and correctly interpreting these networks assists "in predicting behaviour and decision-making within the network".

The method also endows the analyst the ability to measure the level of covertness and efficiency of the cell 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 counter-terrorism applications to be drawn, and assists in the assessment of the most effective methods of disrupting and neutralising a terrorist cell. In short IDM "provides a useful way of structuring knowledge and framing further research. Ideally it can also enhance an analyst's predictive capability". Investigative Data Mining usually uses SNA techniques and graph theory connecting the dots in order to disconnect them.

Covert networks like terrorist networks remain mingled with socially oriented networks (like families, organizations etc.) in the real world. The buzz word for covert networks is "secrecy" and hence to discover such networks (technically, to discern distinctive patterns in the activities and communications of such dark networks) can be very tricky and often misleading due to unavailability of authentic data or in some cases availability of "doctored" data. This issue has especially blown up in the recent past and after the September 11, 2001 tragedy, it has been in the limelight so much so that it is worthwhile to take a close look at the distinguishing properties of such networks. For Example:

(1) In bright networks, actors who are highly central are typically the most important ones. On the contrary, peripheral players (or "boundary spanners" as they are typically called) may be huge resources to a terrorist group although they receive very low network centrality scores. This is because they are well positioned to be innovators, since they have access to ideas and information flowing in other clusters. Similarly, in an organization, these peripheral employees are in a position to combine different ideas and knowledge into new products and services. They may be contractors or vendors who have their own network outside of the company, making them very important resources for fresh information not available inside the company (Krebs V., 2002, Hanneman, R., 2000).

(2) The role of a "broker" (Krebs V., 2002) is a very powerful role in a social network as it ties two hitherto unconnected constituencies / groups together but of course, it is a single-point of failure. These broker type roles are often seen in terrorist networks. Such nodes are also referred to as "cutpoints" (Hanneman, R., 2000). These cutpoints may be further categorized as coordinator (The person connects people within their group), gatekeeper (The person is a buffer between their own group and outsiders. This person is known as influential in information entering the group) and representative (The person conveys information from their group to outsiders. This person is also known as influential in information sharing). We are still working on the algorithms to categorize the categories of brokers.

The main purpose of our research is to study and analyze the structure of terrorist networks in order to devise mathematical methods for destabilizing these adversaries (and to assist law enforcement and intelligence agencies), that is, minimum number of terrorists who, if removed from the network, would disconnect the network.

4 Approaches for Destabilizing Terrorist Networks

4.1 Cohesion Analysis

The aim of the detection of dense clusters is to find maximal subsets of points (with their relationships) with a high density in the cluster and relatively few relationships to other parts of the network. Graph theory gives a number of concepts and procedures that aims to detect maximal subgraphs in a graph (or network) that have a certain property and looses this property by adding another point and its relationships to the subgraph. In an undirected network, a *clique* is a maximal subgraph of at least three points in which all points are directly connected with one another. The concept clique has been generalized to *n-cliques*. In an *n-clique*, between any pair of points in the clique a path of length *n* or less exists in the graph. Such a path may go through points outside the clique, thus causing a larger distance between the points in the clique itself (or even disconnected cliques). An *n-clan* is an *n-clique* where the distance in the clique is also maximally *n*. In this paper we use bottom up approaches of cohesion analysis (cliques, n-cliques, n-clans, and k-plex) on a dataset shown in Figure1.

Modeling a cohesive subgroup mathematically has long been a subject of interest in social network analysis. One of the earliest graph models used for studying cohesive subgroups was the *clique* model (Luce, R., Perry A., 1949). A clique is a subgraph in which there is an edge between any two vertices. However, the clique approach has been criticized for its overly restrictive nature (Scott, J, 2000), Wasserman, S., Faust, K., 1994) and modeling disadvantages (Siedman, S. B., Freeman, L. C., 1992).

Alternative approaches were suggested that essentially relaxed the definition of cliques. Clique models idealize three important structural properties that are expected of a cohesive subgroup, namely, *familiarity* (each vertex has many neighbors and only a few strangers in the group), *reachability* (a low diameter, facilitating fast communication between the group members) and *robustness* (high connectivity, making it difficult to destroy the group by removing members).

Different models relax different aspects of a cohesive subgroup. Luce R. introduced a distance based model called *n-clique* (Luce, R., 1950). This model was also studied along with a variant called *n-clan* by Mokken (Mokken, R., 1979).

However, their originally proposed definitions required some modifications to be more meaningful mathematically.

Table 1. Statistics from the results

	Groups	Groups, max. size	Groups, min. size
clique	41	6	3
n-clique	38	23	5
n-clan	22	23	5
k-plex	493	7	3

These drawbacks are pointed out and the models are appropriately redefined in (Balasundaram, B. et al, 2005). All these models emphasize the need for high reachability inside a cohesive subgroup and have their own merits and demerits as models of cohesiveness. In this paper we also discuss on a degree based model and called *k-plex* (Wasserman, S. et al, 2004). This model relaxes familiarity within a cohesive subgroup and implicitly provides reachability and robustness.

In this paper we discuss the use of the four concepts: cliques, n-cliques, n-clans, and k-plex. The dataset, which describes the network from Figure 1, has been applied to each of the four concepts. The statistics from the results are listed in Table 1.

Each node represents a specific person from the dataset, so the number of nodes should be the same for all concepts. Each concept generated different number of groups: for example, *n-clan* concept generates 22 groups while the *k-plex* concept generates 493 groups. The *n-clique* generates 38 groups and the *clique* concept generates 41 groups. For each of the concepts the maximum size and minimum size of a group has also been collected and shown in Table 1.

The statistics indicates that even with relative small dataset a huge number of groups could be generated. The groups generated are analyzed, in order to identify the best candidate nodes for destabilizing the specific network.

Figure 2 shows to how many groups each member is participated, using respectively clique, n-clique, n-clan and k-plex. As we can see some of the members are participated to many groups while other members are participated in few groups. We say that a member being participated to many groups, compared to the total number of groups, has a *high participation index*, while a member participated in a few groups, compared to the total number of groups has a *low participation index*. Participation index is defined as participation of a particular member of in different groups generated by the various concepts of structural cohesion / cohesion analysis.

For example we take a look at a member Mohamed Atta (node 33) in the matrix generated using the k-plex concept, has participated in 230 groups and the total number of groups is 493. This gives a participation index equal to 230/493, approximately 0.467.

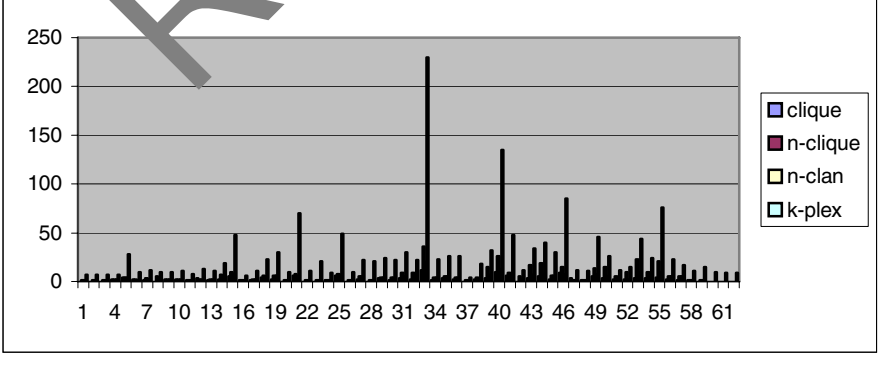

Fig. 2. The participation of the members of the 9-11 terrorists network in various groups using the concepts Clique, n-clique, n-clan and k-plex

Table 2. Participation index

	Member 33	Member 37	Member 55
clique	0.293	0.000	0.098
n-clique	0.947	0.026	0.553
n-clan	0.909	0.045	0.455
k-plex	0.467	0.008	0.152

If the participation index is closer to 1, it means that that member has participated in most of the groups, and if the participation index is closer to 0, it means that the member's participation is negligible.

From the variation seen in the participation index we conclude that the choice of concept has an important influence on the participation index. It seems like using the concepts n-clique and n-clan results in higher participation indices, while the concepts clique and k-plex results in lower participation indices.

The three members described in the Table 2, can roughly been seen as a picture of arch types or roles in the network. In most cases a member is not 100 percent an arch type, but a combination of the three types. What type a member will match best in a specific situation will also be dependent on other factors, e.g. the phase of the operation conducted by the network.

The arch types are named brokers (gatekeeper, representative or coordinator), leaders and followers. Brokers encompass members working with logistics, communications, etc. Leaders encompass leaders at all levels, using the military terms this means officers as well as NCOs. Followers encompass the members that can be compared to the infantry in military terms.

The task of the broker is to provide supplies of weapon, money, identity card, etc. to the network. Often a broker is also preparing houses and cars for the network. The broker sometimes is the member being the secure communication between the different groups in the network. As such the broker is often related to a large number of groups in the network, since a key member in setting up the platform for the operation. Member 33 could as such be an example of a broker.

The task of the leader is, of course, to lead one or more groups in the network. As described, leaders in the network can be found at several levels, from the member leading a group to the leader running the network. Leaders tend to "hide in the crowd", and in some cases they are related to a large number of groups, in other cases they are related to only a small number of groups. As such they can be harder to find. Though in most cases the leader related to many groups, still will have a lower participation index than the broker, and the leader related to few groups will have a participation index higher than the followers. Nawaf Alhazmi (node # 55) could as such be an example of a leader.

The task of the follower is to be the executing part, or the muscles to say in a popular way. A follower is following orders from leaders has usually very limited knowledge about the overall plan. The follower is member of just a few groups since he has

no direct importance for other groups in the network, like for instance the broker. Mamduh Salem (node # 37) could as such be an example of a follower.

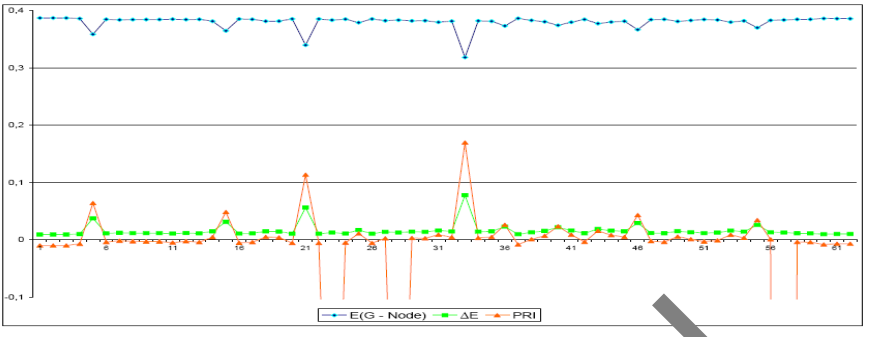

Fig. 3. The efficiency of the original network E(G) = 0.395. The removed node is shown on x-axis, the efficiency of the graph once the node is removed is shown as E(G – node); while importance of node, i.e. the drop of efficiency is shown as Δ E. The newly introduced measure position role index is shown as PRI.

4.2 Role Analysis

In role analysis we'll discover who is who in a network.

The Efficiency E(G) of a network

The network efficiency E (G) is a measure to quantify how efficiently the nodes of the network exchange information (Latora, V., et al, 2004). To define efficiency of G first we calculate the shortest path lengths $\{d_{ij}\}$ between two generic points *i* and *j*. Let us now suppose that every vertex sends information along the network, through its edges. The efficiency ε_{ij} in the communication between vertex i and j is inversely proportional to the shortest distance: $\varepsilon_{ij} = 1/d_{ij} \ \forall$ i, *j* when there is no path in the graph between i, and *j*, we get $d_{ij} = +\infty$ and consistently $\varepsilon_{ij} = 0$. N is known as the size of the network or the numbers of nodes in the graph. Consequently the average efficiency of the graph of G can be defined as (Latora, V., et al, 2004):

$$E(G) = \frac{\sum_{i \neq j \in G} \varepsilon_{ij}}{N(N-1)} = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}} \tag{1}$$

The above formula gives a value of E that can vary in the range [0, ∞], while it be more practical to normalize E in the interval of [0, 1].

The Critical Components of a network

Latora V. et al recently proposed a method to determine network critical components based on the efficiency of the network briefly discussed in the previous subsection. This method focuses on the determination of the critical nodes. The general theory and all the details can be found in Ref. (Latora, V., et al, 2004).

The main idea is to use as a measure of the centrality of a node i the drop in the network efficiency caused by deactivation of the node. The importance I ($node_i$) of the $_i$th node of the graph G is therefore:

$$I(node_i) \equiv \Delta E = E(G) - E(G - node_i), i = 1,...,N, \quad (2)$$

Where $G - node_i$ indicates the network obtained by deactivating $node_i$ in the graph G. The most important nodes, i.e. the critical nodes are the ones causing the highest ΔE.

Position Role Index (PRI)

The PRI is our newly introduced measure (Memon, N., Henrik, L. L., 2006) which highlights a clear distinction between followers and gatekeepers (It is a fact that leaders may act as gatekeepers). It depends on the basic definition of efficiency as discussed in equation (1). It is also a fact that the efficiency of a network in presence of followers is low in comparison to their absence in the network. This is because they are usually less connected nodes and their presence increases the number of low connected nodes in a network, thus decreasing its efficiency.

If we plot the values on the graph, the nodes which are plotted below x-axis are followers, whereas the nodes higher than remaining nodes with higher values on positive y axis are the gatekeepers. While the nodes which are on the x-axis usually central nodes, which can easily bear the loss of any node. The leaders tend to hide on x-axis there.

We applied this measure on the network of alleged 9-11 hijackers (Krebs, V., 2001) and results are shown in Figure 3.

It is to note that after introduction of these measures, now it is possible to find the efficiency of a network as well as if we remove a particular node, then intelligence agency can find how much efficiency of the network is affected.

The analysis shows that Mohamed Atta (node 33) was ring leader of the plot, that is, he played his role as broker in the network. But we still need to know who was influencing who in the 9-11 plot. For this we analyze the influence of the nodes using power analysis.

4.3 Power Analysis

As terrorists establish new relations or break existing relations with others, their position roles, and power may change accordingly. These node dynamics resulting from relation changes can be captured by a set of centrality measures from SNA. The centrality measures address the question, "Who is the most important or central person in the network?" There are many answers to this question, depending on what we mean by important. Perhaps the simplest of centrality measures is *degree centrality*, also called simply *degree*.

Though simple, *degree* is often a highly effective measure of the influence or importance of a node: in many social settings people with more connections tend to have more power.

A more sophisticated version of the same idea is the so-called *eigenvector centrality* (which is also known as centrality of a centrality). Where degree centrality gives a

simple count of the number of connections a vertex has, eigenvector centrality acknowledges that not all connections are equal.

To neutralize terrorist network, we have used centrality measures from SNA literature i.e. degree centrality and Eigen vector centrality.

Using undirected graph (as shown in Figure 1), we first convert it into directed graph using degree centrality and Eigenvector Centrality. For Example, if degree centrality of one node is higher than other, then simply the directed link is originated from that node and point towards other. If they are equivalent in terms of degree, the link will originate from the node with higher Eigenvector centrality. If Eigenvector centrality values for both nodes are equal, then we ignore the link.

Then we identify the parents and children pairs. For example, if we have two nodes, which are competing for being parent of a node, then we have to identify its correct parent. The correct parent will be the one which is connected with maximum neighbours. This represents the fact that the true leader, with respect to a node, which is more influential on its neighbourhood.

When we identify parents, in such a way we traverse all the nodes. Then a tree structure is obtained using dependence centrality, which we call *hierarchical chart*. For more details about algorithms used for conversion of the network (un-directed graph) to hierarchical chart as shown Figure 4, the details are available in our recently published article (Memon, N. and Henrik L. Larsen, 2006).

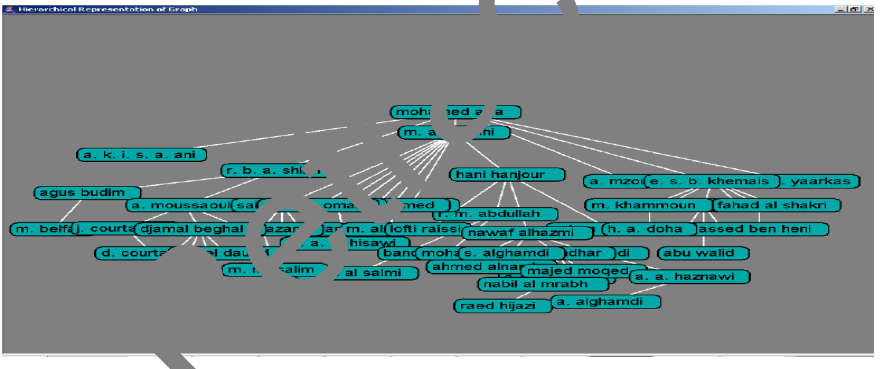

Fig. 4. The hierarchy clearly suggests that Muhammad Atta was the most powerful person (leader) of the plot. While M.A. Shehhi was assisting him, as he is below in the hierarchy. They both were found the key leaders of the plot by 9-11 commission.

Dependence centrality (Memon N. and Henrik L. L, 2006) of a node is defined as how much that node is dependent on any other node in the network. Mathematically it can be written as:

$$DC_{mn} = \sum_{m \neq p,\, p \in G} \frac{d_{mn}}{N_p} + \Omega \tag{2}$$

Where **m** is the root node which depends on **n** by $\mathbf{DC_{mn}}$ centrality and $\mathbf{N_p}$ actually is the Number of geodesic paths coming from **m** to **p** through **n**, and $\mathbf{d_{mn}}$ is geodesic

distance from ***m*** to ***n.*** The Ω is taken 1 if graph is connected and 0 in case it is disconnected. In this paper we take Ω as 1, because we consider that graph is connected. The first part of the formula tells us that:

How many times **m** uses **n** to communicate other node **p** of the network? In simple words **p** is every node of the network, to which **m** is connected through **n** (The connection represents the shortest path of node **m** to **p**, and **n** is in between). $\mathbf{N_p}$ represents the number of alternatives available to **m** to communicate to **p** and $\mathbf{d_{mn}}$ is the multiplicative inverse of geodesic distance (**1/d**).

5 Conclusion

In this paper we have discussed structural analysis and mathematical methods for destabilizing terrorist networks, which will assist law enforcement agencies in understanding the structure of terrorist networks. We presented three different approaches for destabilizing terrorist networks. The cohesion analysis of the dataset shows that Mohamed Atta participated in maximum groups generated by structural cohesion measures, which is a clear indication of working of this node as supplier/ broker / gatekeeper in the network. In reality he was also an important and found as ring leader by 9-11 commission.

The position role index measure assists in finding about who is who in a network (for example, leaders, gatekeepers and followers). This measure also proved that the role of Mohamed Atta was an important and he worked as gatekeeper. The importance of this node can be seen from Figure 3, because deactivating the node, the efficiency of the graph is drastically decreased.

The power analysis concept also proved that Mohamed Atta was the most powerful node in the network and worked as leader in the network and this node is shown as the top node in the hierarchical chart generated by the algorithms recently introduced by the authors.

The mathematical methods and algorithms discussed in the paper are implemented in the investigative data mining prototype known as iMiner. The *iMiner* demonstrates key capabilities and concepts of a terrorist network analysis tool. Using the tool investigating officials can predict overall functionality of the network along with key players. Thus counterterrorism strategy can be designed keeping in the mind that destabilization not only means disconnecting network but disconnecting those key players from the peripheries by which maximum network could be disrupted.

References

1. Balasundaram, B., Butenko, S., Trukhanov, S.: Novel approaches for analyzing biological networks. *Journal of Combinatorial Optimization* 10, 23–39, 2005.
2. Berry, N., Ko, T., Moy, T., Smrcka, J., Turnley, J., Wu, B.: Emergent clique formation in terrorist recruitment. The AAAI-04 Workshop on *Agent Organizations: Theory and Practice*, July 25, 2004, San Jose, California, 2004.
3. Bonacich, P., Power and Centrality. *American Journal of Sociology* 92: 1170-1184, 1987.
4. Burt, R. S., Structural Holes, *Cambridge, MA: Harvard University Press*, 1992.

5. Burt, R. S., Structure, A General Purpose Network Analysis Program. *Reference Manual, Newyork: Columbia University*, 1990.
6. Chen, H., Chung, W., Xu, J.J., Wang, G., Qin, Y., Chau, M.: Crime data mining: A general framework and some examples. *Computer* 37(4), 50–56, 2004.
7. Davis, R.H.: Social network analysis: An aid in conspiracy investigations. *FBI Law Enforcement Bulletin* pp. 11–19, 1981.
8. Freeman, L.C.: The sociological concept of "group": An empirical test of two models. *American Journal of Sociology* 98, 152–166 ,1992.
9. Grier, P. "The New Al Qa'ida: Local Franchiser," *Christian Science Monitor* (11 July 2005). Online at: http://www.csmonitor.com/2005/0711/p01s01-woeu.html (Accessed on May 26, 2006).
10. Hanneman, R. E., Introduction to Social Network Methods. *Online Textbook Supporting Sociology 175. Riverside, CA: University of California*, 2000.
11. Joseph Felter et. al., *Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities* (West Point, N.Y.: United States Military Academy, 2006), p. 7-9.
12. Robert Windrem, "The Frightening Evolution of al-Qa'ida," *MSNBC.com,* (24 June 2005). Online at: http://msnbc.msn.com/id/8307333 (Accessed on May 26, 2006).
13. Krebs, V.: Mapping networks of terrorist cells. *Connections* 24, 45–52, 2002.
14. Latora, V., Massimo Marchiori How Science of Complex Networks can help in developing Strategy against Terrorism, *Chaos, Solitons and Fractals* 20, 69-75, 2004.
15. Luce, R., Perry, A.: A method of matrix analysis of group structure. *Psychometrika* 14, 95–116, 1949.
16. Luce, R.: Connectivity and generalized cliques in sociometric group structure. *Psychometrika* 15, 169–190, 1950.
17. McAndrew, D.: The structural analysis of criminal networks. In: D. Canter, L. Alison (eds.) The Social Psychology of Crime: Groups, Teams, and Networks, *Offender Profiling Series, III. Aldershot, Dartmouth* ,1999.
18. Memon, N., Detecting Terrorist Related Activities using Investigative Data Mining Tool, In Proceedings of Symposium 5, Data/Text Mining from Large Databases IFSR 2005, Kobe, Japan, 2005.
19. Memon, N. Henrik Legind Larsen, Practical Algorithms for Destabilizing Terrorist Networks, *Lecture Notes in Computer Science (LNCS)* 3975, ISI 2006, Eds. S. Mehrotra et al. pp. 389-400, 2006.
20. Mokken, R.: Cliques, clubs and clans. Quality and Quantity 13, 161–173, 1979.
21. Newman, M. E. J. The structure and function of complex networks, *SIAM Review* 45, 167-256, 2003.
22. Scott, J.: Social Network Analysis: A Handbook, 2 edn. *Sage Publications*, London 2000.
23. Seidman, S.B., Foster, B.L.: A graph theoretic generalization of the clique concept. *Journal of Mathematical Sociology* 6, 139–154, 1978.
24. Sageman, M.: Understanding Terrorist Networks. *University of Pennsylvania Press*, 2004.
25. Wasserman, S., Faust, K.: Social Network Analysis. *Cambridge University Press*.1994.
26. Wiktorowicz, Q. "The New Global Threat: Transnational Salafis and Jihad," *Middle East Policy* 8, no. 4 (2001: 18-38)