Detecting Key Players in Terrorist Networks

Ala Berzinji
University of Sulaimani
Sulaimani, Iraq
Email: ala.berzinji@gmail.com

Lisa Kaati
FOI
Stockholm, Sweden
Email: lisa.kaati@foi.se

Ahmed Rezine
Linköpings University
Linköping, Sweden
email: ahmed.rezine@liu.se

***Abstract*—The interest in analyzing loosely connected and decentralized terrorist networks of global reach has grown during the past decade. Social Network Analysis (SNA) is one approach towards understanding terrorist networks since it can be used to analyze the structure of a network and to detect important persons and links.**

In this work we study decentralized terrorist networks with different types of nodes. The nodes can be either organizations, places or persons. We use a combination of different centrality measures to detect key players in such networks.

I. Introduction

Criminal and terrorist social networks can often be divided into hierarchies with actor roles varying from ordinary operatives to the finance manager and the leader. The most important roles include the leader who acts as the guide and mentor for the whole group, besides giving directions about the operations that need to be planned and carried out by the group. The finance manager deals with the execution of planned events and also manages the financing of all other operatives of the group. The finance manager is usually the node that is directly connected to most other nodes in the network. Other roles may include media manager – responsible for propaganda, claiming responsibility for terrorist events and promotion of the group and its objectives on media, military manager – responsible for arranging equipment used in terror related incidents, and operatives – responsible for carrying out the planned events.

In the post-9/11 war on terror era, terrorist organizations around the globe have evolved a decentralized strategy to carry out successful operations in the Middle East. A decentralized approach in practice puts almost the entire responsibility related to operations on the finance manager. The finance manager gives directions for carrying out various operations to other group members and provides the members with finances. Detecting the finance manager in a terrorist network is important in order to effectively counter the operations of the network.

Social network analysis (SNA) [1] is a set of powerful techniques that can be used to identify clusters, patterns and hidden structures within social networks. In this work we present an algorithm that can be used to detect the finance manager in a decentralized terrorist network. The network is represented using a subset of the categories that are present in the NATO AIntP-3 data model. The finance manager is the node in a network that is most operationally central, active and that acts as gateway in the network. The finance manager is detected using a combination of different well-known centrality measures.

Terrorist social networks are also known as dark networks. Recent studies such as [2] have explored the use of SNA methods to analyze dark networks mostly focusing on assigning roles to actors in the network. In [3] the use of centrality measures to identify key actors in criminal networks is explored and in [4] centrality measures are used to identify the group leader of the September 11th hijackers. However, none of these operates on networks with different categories of nodes.

In [5] SNA is used to determine the leader and gatekeeper role for individual nodes in addition to hierarchical clustering methods to identify subgroups within criminal networks. In [6] an algorithm that automatically detect the hidden hierarchy in terrorist networks is presented. The algorithm is based on centrality measures that are commonly used in social network analysis. Two measures of centrality: termed degree, and Eigenvector centrality are introduced as well as a dependence relation.

The Investigative Data Mining (IDM) toolkit is used for subgroup detection and terrorist intelligence analysis [7]. In the toolkit centrality measures combined with data mining techniques is used to find the hierarchy of a group and the leader of the group. However, our work is different from theirs since we consider decentralized terrorist networks, whereas their work is mostly related to networks with centralized hierarchy.

II. Preliminaries

A. Graphs and Networks

A graph G consists of a pair (V, E) where V is the set of nodes, and E the set of edges that connect the nodes. We assume in the following a graph $G = (V, E)$. Social networks are naturally modeled using graphs where nodes represent actors and edges relations between them. In the following, we often say network to mean the graph modeling it.

Edges might be undirected or directed depending on whether they reflect symmetrical or not symmetrical relations between actors.

We write $uv \in E$, for $u, v \in V$, to denote that there is an edge between nodes u and v in the graph (V, E). Most SNA techniques focus on undirected graphs since the considered relations are typically mutual and bi-directional.

978-0-7695-4782-4/12 $26.00 © 2012 IEEE
DOI 10.1109/EISIC.2012.13

Unless otherwise specified, we only consider in this work techniques for undirected graphs. In other words, we consider that the pairs in the set of edges E are unordered. Also, and otherwise specified, the relations we represent with the edges are not reflexive, i.e., there are no self loops in E.

a) Basic notions and notations.: Many graph algorithms initially select a single node in V and refer to as the *ego node*. This node can be predefined or obtained either randomly or using some calculations. Given a set S, we write $|S|$ to mean the size of S. For instance, we write $|V|$ (respectively $|E|$) to mean the number of nodes (respectively of edges) in the graph. Given a node $u \in V$, all nodes connected to u in E are neighbors of u and make up its *neighborhood*, written $N_G(u)$. In other words, $N_G(u) = \{v \; s.t \; uv \in E\}$. The *degree* of a node u, written $d_G(u)$, is the number of nodes in G having an edge with the node u, i.e., $d_G(u) = |N_G(u)|$. Given two nodes u and v in V, a path between u and v is a succession of edges connecting nodes u and v. Formally, a path $\pi(u, v)$ between two nodes u and v is a sequence of edges $w_0w_1, w_1w_2, \ldots, w_{n-1}w_n$, with $w_0 = u$ and $w_n = v$. We write $w \in \pi(u, v)$ to mean that the node w participates in the path $\pi(u, v)$, and $|\pi(u, v)|$ to mean the length of the path. The length of a path is the number of occurrences of the edges participating in the path. The *geodesic distance*, written $d_G(u, v)$, is the length of a shortest path connecting the two nodes u and v if such a path exists, and is undefined otherwise. The geodesic distance between a node and each other node in the simple unweighted graphs we consider can be obtained using a breadth first traversal of the graph, i.e., iteratively exploring all neighboring nodes to those nodes that have already been searched. We use $SP_G(u, v)$ to denote the set of shortest paths between nodes u and v in the graph G.

III. Centrality

Analyzing social networks typically aims at categorizing and identifying the roles played by the participants in the network. The analysis estimates the relation of each node to the other nodes. In this context, *centrality* measures are commonly used and aim at capturing the relative importance of nodes in a network. To achieve this, the centrality of a node takes into account how other nodes in the network are related to the node through direct or indirect relations.

There are various measures of centrality to determine the importance of a node in the network by taking into account different aspects of the relations between the nodes in the network.

Centrality is one of the network properties that have been frequently used to study actors or events in terrorist social networks. The most used centrality measures in this context are degree centrality, betweenness centrality, and closeness centrality. In the following section we introduce common centrality measures and a particular closeness centrality measure, that we denote as alternative closeness.

A. Degree Centrality

Degree centrality estimates how important a node is by analyzing the number of direct relationships it has with other nodes in the network. The degree centrality of a node simply corresponds to the degree of the considered node [8]. This measure can be normalized by the number of nodes in the graph G less one (recall we exclude self loops):

$$\mathcal{C}_G^d(v) = \frac{d_G(v)}{|V| - 1}$$

In the case of a directed network, two types of degree centrality are considered: in-degree and out-degree. Whether directed or not, the idea is that the more edges a particular node participates in, the higher is its degree centrality value.

The actor with the highest degree centrality is considered to be the most strongly (or most frequently) connected node in the network. Such a node holds an advantaged position in the network in terms of connectivity with other nodes which gives it a key role to propagate information. In other words, degree centrality of an ego node is a measure of immediate influence, that is, what proportion of the nodes in the network are influenced by the ego if the latter influences its neighbors with a piece of information and none of the influenced nodes is allowed to further spread the information. The higher the proportion of nodes influenced, higher will be the degree centrality of the ego node.

Other variants of degree centrality (ex [9]) count the number of nodes related by paths of lengths less or equal to some predefined number (one for the original definition). The idea is that a node with few edges related to nodes with many edges still can have a high centrality (degree centrality). For instance, when the degree centrality is obtained with respect to maximal path lengths of two, it measures how much influence a node has if it influences its neighbors with a piece of information and the influenced nodes in turn are allowed to spread it to their neighbors, but the latter nodes are not allowed to further pass the information. A major advantage of degree centrality is its simplicity as it only takes into account the immediate neighborhood of a node when computing its centrality.

B. Betweenness Centrality

In *betweenness centrality*, higher betweenness is attributed to nodes that occur most often on the shortest paths between other nodes. Nodes that have a higher probability of being located on the shortest path between other distinct nodes have higher betweenness than other nodes. Such nodes can also be described as gateways. Nodes with high betweenness have a control over the data flowing among the different groups of nodes in the network, since such nodes often act as bridges. In criminal or terrorist networks, nodes with high betweenness usually indicate the most important or involved actors. An actor with a high degree of betweenness centrality usually holds a favored position in the network. Such a node has greater control over information propagation within the network and represents a bridge which can potentially be a single point of failure. Disconnecting such nodes can effectively disrupt communication within the network.

Original definitions of betweenness centrality ([10]) for an ego node v compute all shortest (geodesic) paths among

all pairs of nodes in the network. More specifically, the set $\{\pi(s,t)\ s.t\ |\pi(s,t)| = d_G(s,t)\}$ is computed for each pair of nodes $s,t \in V$ different from v. Then, the number of times the ego node v was found on these shortest paths, i.e., the size of the set $\{\pi(s,t)\ s.t\ v \in \pi(s,t)$ and $|\pi(s,t)| = d_G(s,t)\}$ is counted. Betweenness $\mathcal{C}_G^b(v)$ is then calculated as follows:

$$\Sigma_{s,t \in V \setminus \{v\}} \frac{|\{\pi(s,t)\ s.t\ v \in \pi(s,t) \text{ and } |\pi(s,t)| = d_G(s,t)\}|}{|\{\pi(s,t)\ s.t\ |\pi(s,t)| = d_G(s,t)\}|}$$

Calculating all geodesic paths between all pairs is costly. Instead of using geodesic paths, as in the original definition, different alternatives have been considered. One alternative [11] is to only consider, when computing betweenness centrality for an ego node, the network resulting from the nodes directly related to it together with the edges among them. Other alternatives involve statistical sampling in order to randomly select paths between two random nodes in the network and then to count the number of times the ego node appears on the randomly selected path.

C. Closeness Centrality

Closeness centrality of a node in a network is another variant for measuring the centrality of a node. It is a measure of how close a node is to all other nodes in the network (directly or indirectly). Closeness centrality measures how quickly a node can access information through other nodes in the network. A node with a high closeness centrality has a short path to other nodes in the network, and can reach them (i.e. propagate information to them) quickly. Such a node has high visibility as to what is happening in the network, and that is because information in the network may usually flow through nodes with high closeness centrality.

Typically [12], closeness centrality is measured using the geodesic distance (shortest path). The node with the highest closeness centrality is the one with the smallest distance to all other nodes in the network. One way to take into account the distance of a node v in a graph $G(V,E)$ to all other nodes is to sum the distances between v and each of the other nodes:

$$\Sigma_{u \in V \setminus \{v\}} d_G(v,u)$$

Where $d_G(v,u)$ is the geodesic distance between the nodes v and u. Closeness centrality is then defined as the inverse of the average of this sum:

$$\mathcal{C}_G^c(v) = \frac{|V| - 1}{\Sigma_{u \in V \setminus \{v\}} d_G(v,u)}$$

Measuring closeness centrality for all nodes boils down to a breadth first search of the entire network for every node.

As a result, closeness centrality does not scale as well as degree centrality. Nevertheless, the obtained result takes into account the network as a whole, instead of limiting to a local, and possibly misleading fraction.

In [13], [14] an alternative defintion of closeness centrality is presented. The idea is to sum, when computing closeness centrality for a node v, for each node u different from v, the result of applying a strictly decreasing positive function α to the distance $d_G(u,v)$ between nodes u and v, formally:

$$\Sigma_{u \in V \setminus \{v\}} \alpha\left(d_G(v,u)\right)$$

For example, when $\alpha : x \mapsto x^{-1}$ we get the definition in [13], and when $\alpha : x \mapsto 2^{-x}$ we get the one in [14]. Unlike the original definition of closeness, this definition is well suited for disconnected graphs when $\alpha(x)$ takes 0 for infinite x. In the rest of this paper, we say alternative closeness centrality to mean the closeness centrality obtained by using the function $\alpha : x \mapsto x^{-1}$, and write:

$$\mathcal{C}_G^{ca}(v) = \Sigma_{u \in V \setminus \{v\}} \left(d_G(v,u)\right)^{-1}$$

IV. Terrorist Networks

A terrorist network consists of a group of people that are members of or somehow related to a terrorist organization. After 9-11 the structure of terrorist networks changed. The structure of the networks became more decentralized and the geography of the network became more global [15]. By analyzing terrorist networks related to well-known terrorist attacks such as: 9/11 [16], the London bombings [17], Detroit Christmas in 2009 [18], the Times Square event in 2010 [19], and the planned attack in Sulaimanyah 2011 [20] we can observe that all these terrorist networks are global. The members of the networks did not stay in one place since they needed military training, finances, and indoctrination.

A. Structure of a Terrorist Social Network.

Terrorist social networks can be represented as graphs where nodes in the network represent actors or groups, and the links between the nodes demonstrate their relationship with each other. The working structure of a terrorist social network was published in 2010 by the counter terrorism agency of Iraq [21]. The report discussed operational and general working structure of terrorist groups in the region and state that the organization of modern terrorist groups is decentralized. A simplified example of such a network can be found in Figure 1. The network has leader who mostly acts as a mentor and only provides guidance on how to organize and motivate the group operatives. The actual activities are managed by the finance manager on behalf of the leader. The finance manager acts as the defacto leader of the group. In addition to the finance manager, there are other managers with limited roles such as organizing media propaganda for the group, organizing security related matters for the operatives and managing equipments for militant operations. All group members holding managerial roles are directly supervised by the finance manager. In addition to the managers, the finance manager also provides direct instructions to the operatives directly involved in militant activities.

The finance manager is the one who occupies the most central and active role in a decentralized terrorist network. The finance manager has the most contact with all other members of the group. Besides that, the finance manager is the only one having direct contact with the actual leader of the group. The

leader of the group only sets the goals for the group, and the finance manager manages to achieve those goals.

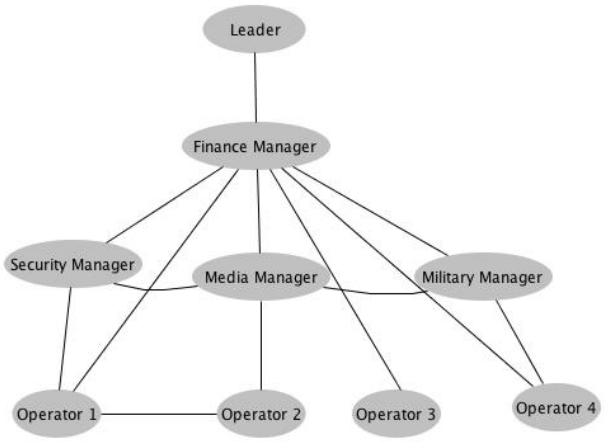

Fig. 1. A decentralized terrorist network.

B. AIntP-3 Data Model

The AIntP-3 data model is a standard that is used within NATO to facilitate the electronic and manual exchange of intelligence data between databases. The AIntP-3 data model defines several categories to capture information about concerned persons, organizations, events, places and equipments. These categories are related to each other with the help of well-defined sub-categories.

In this work we use a subset of the AIntP-3 data model to represent and structure terrorist networks. Using a well-defined standard to represent social networks and to define algorithms is crucial if the methods are to be applicable on information coming from several different sources.

There are five main categories in the data model:

- Equipment - Materials or tools used to equip investigators or investigative organizations to fulfill their roles. Such equipments or installations may be owned and/or operated by military or civilian and may exist on land, in air space, in outer space (as satellites) or under the sea.
- Organization - An organization is a grouping of individuals, with a well-defined hierarchy, aiming to achieve a common goal. Each individual in the group is assigned a role to complete individual tasks aimed towards achieving the goal. An organization can also be of criminal orientation. An organization in general may be divided into sub-organizations with their own specific hierarchy and well-defined sub-functions.
- Place - Point or area on earth or space, identifiable through a set of reference coordinates, that is occupied by an entity (unit, equipment, person or organization) or is associated with the occurrence of an incident or event.
- Biography - The description of the appearance of an individual, personal and professional attributes, personal background (family, education, career etc.) and social behavior patterns.
- Event - The description of an incident or occurrence that has some intelligence significance. An event can usually be broken down into several smaller sub-events that are in some way immediately or remotely (loosely) related.

V. Detecting Key Actors in Terrorist Networks

Finances are an important part of a terrorist operation and Levitt states in [22] that without funds no terrorist events can take place. The finance manager holds information of most of the members and the activities carried out by the network since it is not possible to carry out any terrorist related activities without material support (which requires finances). Because of the risk of being caught by security agencies, information about the leader is usually hard to obtain and therefore it is easier to identify and find information about the finance manager.

The leader is the only one who can make a decision about an operation and all operations need financial resources. Usually the leaders' only relationship in the network is with the finance manager, which in turn is in direct contact with other involved (or required) actors and operatives [21]. In [23] the tracking of two identified terrorists is described. They found that the finance manager acted as a local leader, and they could track his relations and find the actual leader through him.

The terrorist network Al-Qaeda which is believed to be most strongly present in Pakistan, Iraq, Yemen, and the Magreb (Morocco to Libya) has started to become extremely decentralized in its operations, the decentralized structure of Al-Qaeda is also mentioned in [6], [24], [25].

In this work, we present a method for detecting the finance manager in a decentralized network. The finance manager is in charge of the activities of terrorist groups in different geographic locations and has to provide funding to the operatives performing those activities. For this reason the finance manager has the most relations in many different regions. We can find the node in the network with the most relations to different places with the measure of degree centrality [26]. This is due to two reasons, the finance manager has cluster relations to almost all other members of the group.

- The salary of the group members is managed by the finance manager (in case of Al-Qaeda in Iraq, all members receive at least 100 dollars every month from the finance manager [21])
- Because of the operations of the group, the finance manager supports every active operative with extra funds and therefore has close relations with them [21].

One of the problems of the terrorist groups is the procurement of funds and their secret transfer to other people in other places. After 9/11 government security organizations around the world have focused on transfers of funds when they are large in amount, and also when funds are transferred from countries with conflicts to EU or North America [27]. The finance manager of a group needs to avoid being tracked by any security agency and avoid tracking by:

- Acting as the supervisor for his organization. He organizes different projects and organizations globally and locally overseeing different businesses. This helps procure/-generate funding for various activities of his group [21].
- The finance manager has relations besides the organizations that he oversees with other groups or organizations that provide funding to his group [21].

From this we can observe that the finance manager acts as a gatekeeper between the organizations that provide funds to his organizations. Besides that he also manages the finances of his group's organizations and businesses. As a result, the finance manager is represented by a node with high betweenness centrality with local and global organizations within the network.

We are interested in developing a technique to track the finance manager in terrorist organizations that follow the modern trends of post 9/11 decentralized terrorist networks. So finding the finance manager will require employing a combination of strong centrality measurements as

- Finding the node with most relations with other nodes, using degree centrality.
- Finding the node that has the most relations with other places, using node centrality.
- Finding the node with the most closeness to all other nodes, both with the original and the alternative definitions of closeness centrality.
- Finding the node that is the gateway between all the organizations that have relations with this group using betweenness centrality.

Following these steps can help in narrowing down the focus to the key actors in the social network and detecing the finance manager.

VI. Algorithm for Discovering Finance Manager

In this section we present an algorithm designed to find the node in the network that

1) represents a person having highest degree centrality among all other persons and places,
2) is closest to all other nodes in the network, and
3) has highest betweenness centrality between the organizations.

This way we can discover the node that is operationally most central, active, gateway and controllable in the network.

The social network is represented by an undirected graph (V, E) with n vertices composed of the following subgraphs.

- (V_p, E_p) − graph representing persons as nodes and relations between them. The number of vertices is denoted n_p.
- (V_o, E_o) − graph representing organizations as nodes and the relations between them. The number of vertices is denoted n_o.
- (V_{pl}, E_{pl}) − graph representing places as nodes and the relations between them. The number of vertices is denoted n_{pl}.

The sum of all the nodes in the above subsets equals the total number of nodes in the entire graph, i.e., $n = n_p + n_o + n_{pl}$. In addition to the given edges in (V_o, E_o) , (V_{pl}, E_{pl}), there are three additional subsets of edges that are a part of the set E in (V, E). These sets of edges sets are:

- $E_{p\cdot o}$ − edges representing relations between persons and organizations.
- $E_{p\cdot pl}$ − edges representing relations between persons and places.
- $E_{o\cdot pl}$ − edges representing relations between organizations and places.

The purpose of the algorithm is to find a node in the network that represents a person that is operationally most central to the network and also closest to other nodes. The algorithm consists of the following five steps.

1) **Degree Centrality** is calculated for each node v_p in graph (V_p, E_p); that is,
$$\mathcal{C}^d_{(V_p,E_p)}(v_p) = \frac{d_{(V_p,E_p)}(v_p)}{n_p - 1}$$
is calculated for each v_p in the set V_p.
2) **Degree Centrality** is calculated for each v_p in V_p in the subgraph $(V_p \cup V_{pl}, E_{p\cdot pl})$; that is,
$$\mathcal{C}^d_{(V_p\cup V_{pl},E_{p\cdot pl})}(v_{pl}) = \frac{d_{(V_p\cup V_{pl},E_{p\cdot pl})}(v_{pl})}{n_{pl} - 1}$$
is calculated for each v_p in the set V_p.
3) **Closeness Centrality** is calculated for each node v_p in V_p and with respect to *a*ll nodes in (V,E)[1]; that is,
$$\mathcal{C}^c_{(V,E)}(v_p) = \frac{|V| - 1}{\Sigma_{u\in V\setminus\{v_p\}} d_{(V,E)}(v_p, u)}$$
is calculated for each v_p in V.
4) **Alternative Closeness Centrality** is calculated for each node v_p in the set V_p; that is,
$$\mathcal{C}^{ca}_{(V,E)}(v_p) = \Sigma_{u\in V\setminus\{v_p\}} \left(d_{(V,E)}(v_p, u)\right)^{-1}$$
is calculated for each node v_p in V_p.
5) **Betweenness Centrality**[2] is calculated for each node v_p in V_p and with respect to all organizations in V_o; that is, $\mathcal{C}^b_{(V_p\cup V_o,E_{p\cdot o})}(v_p)$, defined as $\Sigma_{s,t\in V_o} \frac{|\{\pi(s,t)\ s.t\ v_p\in\pi(s,t) \text{ and } |\pi(s,t)|=d_{(V_p\cup V_o,E_{p\cdot o})}(s,t)\}|}{|\{\pi(s,t)\ s.t\ |\pi(s,t)|=d_{(V_p\cup V_o,E_{p\cdot o})}(s,t)\}|}$ is calculated for each node v_p in V_p.

Once all the centrality scores have been measured as described in above items, the key actors in the social network can be identified. The nodes with high scores for most of the

[1]Measuring closeness centrality separately for organizations and places does not produce very meaningful results. We consider all nodes (including persons, organizations and places) and calculate closeness centrality for them, but for targeting purposes the most useful node is the one with the highest Closeness Centrality score and represents a person.

[2]We only consider nodes and edges between persons and organizations in this case. We do so by measuring betweenness centrality for all nodes between vertices that represent organizations. Our interest here is the node with the highest betweenness centrality score that represents a person.

centrality measures represent all the key actors in the network. The node with the highest score on all the centrality measures represents the finance manager. This is also expected since the finance manager in decentralized networks has all the properties to have largest scores on all mentioned centrality measures. The most important properties of the finance manager include - (1) most direct or 1-hop neighboring nodes, which makes it score higher on closeness centralities, and (2) most common occurrences on all shortest paths between all nodes in the network, making it score higher on betweenness centrality.

VII. Conclusions and Future work

In this work we present an algorithm that can be used to detecting the finance manager in a decentralized terrorist network. The finance manager plays a central role and is the most active actor in a terrorist network.

The networks that we consider contains different categories of nodes. The categories we use are a subset of categories that are presented in the NATO AIntP-3 data model. Detecting the finance manager is done by using a combination of different well-known centrality measures on the different categories of nodes in the network.

One direction for future work is to investigate more complex terrorist networks with different relations as well as different types of nodes. To analyze such networks properly new measures and algorithms are needed. Analyzing more complex networks may provide analysts with more information regarding the key players, structure and information flow in the network than using the traditional social networks where only persons and relations are present.

Acknowledgment

This research was financially supported by Vinnova through the Vinnmer-programme.

References

[1] S. Wasserman and K. Faust, *Social Network Analysis:Methods and Applications*. Addison-Wesley, 1994.

[2] J. Xu, D. Hu, and H. Chen, "Dynamics of Terrorist Network: Understanding the Survival Mechanisms of Global Salafi Jihad," *Jour. of Homeland Security and Emergency Management*, vol. 6, 2009.

[3] M. K. Sparrow, "The application of network analysis to criminal intelligence: An assessment of the prospects," 1991, social Networks. Esevier 13, 251-274, 3.

[4] V.E.Krebs, "Mapping networks of terrorist cells," *International Network for Social Network Analysis*, vol. 24(3), 2002.

[5] J. Xu and H. Chen, "Criminal network analysis and visualization," *Commun. Ass. for Computing Machinery*, vol. 48, pp. 100–107, 2005.

[6] N. Memon, H. Larsen, H. Legind, D. Hicks, and N. Harkiolakis, "Detecting Hidden Hierarchy in Terrorist Networks: Some Case Studies," *Springer-Verlag*, pp. 477–489, 2008, proc. of the IEEE ISI 2008 PAISI, PACCF, and SOCO int. ws on Intelligence and Security Informatics.

[7] N. Memon, D. L. Hicks, and H. L. Larsen, "How Investigative Data Mining Can Help Intelligence Agencies to Discover Dependence of Nodes in Terrorist Networks," in *Proc. of Advanced Data Mining and Applications*, 2007, pp. 430–441, Springer-Verlag.

[8] L. C. Freeman, "Centered Graphs and the Structure of Ego Networks," 1982, University of California.

[9] P. Bonacich, "Power and Centrality: A Family of Measures," *American Journal of Sociology*, vol. 92, no. 5, pp. 1170–1182, 1987.

[10] R. A. Hanneman and M. Riddle, "Introduction to social network methods," 2005, University of California. Last visited: 1 July 2011.

[11] S. Borgatti, "Centrality and network flow," *Social Networks*, vol. 27, no. 1, pp. 55–71, 2005.

[12] F. Hildorsson, "Scalable Solutions for Social Network Analysis," Master Thesis, Uppsala University, 2009.

[13] T. Opsahl, F. Agneessens, and J. Skvoretz, "Node centrality in weighted networks: Generalizing degree and shortest paths," *Social Networks*, vol. 32, no. 3, pp. 245–251, 2010.

[14] C. Dangalchev, "Residual closeness in networks," *Physica A: Statistical Mechanics and its Applications*, vol. 365, no. 2, pp. 556–564, 2006.

[15] National Commission On Terrorist Attack Upon The United States, "Final Report of the National Commission on Terrorist Attacks Upon the United States," 2004, the 9/11 Commission report executive summery by UNT libraries. Last visited: 1 July 2011. [Online]. Available: http://govinfo.library.unt.edu/911/report/911Report.pdf

[16] S. Mandal, "Financial Investigation and CounterTerrorism Case Study: 7 July 2005,London," 2005, iCPYTR, RSIS Singapore.

[17] R. Esposito and B. Ross, "Northwest Bomb Plot Planned by al Qaeda in Yemen," 2009, online article by ABC News. Last visited: 12th August 2011. [Online]. Available: http://abcnews.go.com/Blotter/al-qaeda-yemen-planned-northwest-flight-253-bomb-plot/story?id=9426085

[18] R. Rivera, "A dread revived: Terror in the trunk," 2010, online article by NYtimes. Last visited: 13th August 2011.

[19] Daily Mail Reporter, "British police given more time to question man suspected of aiding botched Stockholm suicide bomb attack," 2011, online article by dailymail. Last visited: 13th August 2011.

[20] R. Floyd, "'Safe' kurd city is shaken," 2011, online article by The Augusta Chronicle. Last visited: 12th August 2011.

[21] Anti terrorism Agency-Kurdistan Iraq, *The Geosecurity of Mosel*, 2010, PUK media.

[22] M. Levitt, "Checkbook jihad," 2011, online article by Foreign Policy. Last visited: 12th August 2011.

[23] V. Krebs, "Connecting the Dots Tracking Two Identified Terrorists," 2008, online article by Orgnet. Last visited: 12th August 2011. [Online]. Available: http://www.orgnet.com/tnet.html

[24] N. Memon, U. K. Wiil, and P. A. R. Qureshi, "Practical algorithms for subgroup detection in covert networks," *Int. Jour. of Business Intelligence and Data Mining*, vol. 5, pp. 134–155, January 2010.

[25] N. Memon, A. R. Qureshi, U. K. Wiil, and D. L. Hicks, "Novel Algorithms for Subgroup Detection in Terrorist Networks," *Availability, Reliability and Security*, vol. 0, pp. 572–577, 2009.

[26] E. Kaplan, "Tracking Down Terrorist Financing," 2006, online article by Council on Foreign Relations. Last visited: 12th August 2011.

[27] Terrorist Financing Operations Section, "Terrorist Financing," 2007, online article by FBI. Last visited: 12th August 2011.