Destabilization of Terrorist Networks through Argument Driven Hypothesis Model

Dil Muhammad Akbar Hussain
Information & Security Analysis Research Centre
Department of Software Engineering & Media Technology, Aalborg University Esbjerg, Denmark
Email: akbar@aaue.dk

***Abstract*— Social network analysis has been used for quite some time to analyze and understand the behavior of nodes in the network. Theses nodes could be individuals or group of persons, events or organizations etc. Infact these nodes could be any thing importantly, these nodes propagate and obviously have attributes. In this paper a very novel and absolutely new approach to SNA is presented, for locating the important key players in the network. The system also predicts a path comprising of selected nodes which shows the vulnerability of the network and if the path along with these nodes is removed it can reduce/destabilize or even destroy the structure of the network. The paper provides comparative results for a couple of random networks with various numbers of nodes and connections. In addition to these example networks it performs a case study of the nine eleven, 62 node networks (*by Valdis E. Krebs*) to predict a path for its destabilization. This network is selected to benchmark our proposed model framework. The results obtained with various network analysis shows that it works better than other analysis measures for example based on degree, betweeness and closeness etc.**

***Index Terms*— Social Network Analysis, Terrorism, Models, Intellective simulation model.**

I. Introduction

Social Network Analysis is a mathematical method for 'connecting the dots'. SNA allows us to map and measure complex, and sometimes covert, human groups and organizations [1]. Given any network where the nodes/agents are individuals, groups, organizations etc., a number of network measures such as centrality or cut-points are used to locate critical/important nodes/agents. Social network analysis (SNA) is a multi-model multi-link problem so the challenges posed by such multi-dimensional task are enormous. Typically, models represent various processes and their organization including the interaction between processes. The standard or normal representation of a typical social network model is through a graph data structure. This type of model can be considered as an intellective simulation model, such types of models explain one particular aspect of the model abstracting other factors present in the model. The dynamics of larger social networks is so complex some time it becomes difficult to understand the various levels of interactions and dependencies just by mere representation through a graph. However, to overcome this limitation many analytical methods provide relationship dependencies, role of different nodes and their importance in the social networks. Insight visualization of any network typically focuses on the characteristics of the network structure. Many traditional social network measures and the information processing network measures can help in revealing importance and vulnerabilities of the nodes/agents in the network.

Since the start of this century many terrorism events have occurred around the globe. These events have provided a new impetus for the analysis, investigation, studying the behavior and tracking terrorist networks (individuals). In this paper a framework model for destabilizing a terrorist/covert network is presented. Networks visualization is semantically presented in the form of a graph in which the nodes represent entities and the arcs represent relationship among nodes. The framework model has two phases for the analysis process, in the first phase a tentative weighting index is determined for each node which basically indicate the potential of that node for example in terms of its importance. In the second phase argument driven multiple hypotheses are evaluated to adjust the weighting index to represent its true potential. For example if an individual is 20 years old he/she can pose more threat than a person of 50 years old even if all other parameters are exactly the same. A number of similar kinds of argument driven hypotheses are generated for selected attributes and the weighting index value obtained in the first phase is then tuned to an optimum value during this phase. Once nodes true potentials are determined the novel technique developed here predicts and highlights the most important/valuable path comprising of high weighting index value nodes. The system selects only 25 % nodes of the network in the analysis for path illumination, however this value can be changed depending upon network size. The experimental value of 25 % determined with our analysis shows that for a network of 100 nodes or less it is a reasonable choice. Based on the 25 % selected nodes if the predicted path is removed it can potentially make the network impotent, fragmented or destabilize. Each node in the network is characterized by 18 different attributes. The nodes distinctiveness classification is a challenging task. Typically, social network analysis identifies the following characteristics:

- Important individual, event, place or group.
- Dependency of individual nodes.
- Leader-Follower identification.
- Bonding between nodes.

- Vulnerabilities identification.
- Key players in the network.
- Potential threat from the network.
- Efficiency of overall network.

Kathleen Carley has provided the following key characteristics [2].

- An individual or group that if given new information can propagate it rapidly.
- An individual or group that has relatively more power and can be a possible source of trouble, potential dissidents, or potential innovators.
- An individual or group where movement to a competing group or organization would ensure that the competing unit would learn all the core or critical information in the original group or organization (inevitable disclosure).
- An individual, group, or resource that provides redundancy in the network.

Application of existing tools on the complex socio-technical systems like SNA is very demanding to winkle out the required information. Most of the measures and tools work best when the data is complete; i.e., when the information is inclusive about the interaction among the nodes. However, the difficulty is that large scale distributed, covert and terrorist networks typically have considerable missing data. Normally, a sampled snapshot data is available, some of the links may be intentionally hidden (hence missing data may not be randomly distributed). Also data is collected from multiple sources and at different time scales and granularity. In addition inclusive and correct information may be prohibitive because of secrecy. Obviously, there could be other difficulties but even these provide little guidance for what to expect when analysing these complex socio-technical systems with the existing tools. The next two sections provide a survey of the standard centrality measures and their mathematics used in the social network analysis. These measures are important and have been used as attributes in the proposed architecture of the node in addition these are used for comparison. Actual implementation of the proposed model is explained in section 4 and finally results and analysis of various example networks are presented in section 5.

II. Network Analysis Measures

Social networks provides mapping and the social network analysis measure relationships and movement between people, groups, events, organizations or other information/knowledge processing entities. People, organization and groups are represented as nodes in the network while the links show relationships or movement between the nodes. SNA provides both visual and mathematical analysis of human relationships. This methodology could also be used by the management to perform Organizational Network Analysis [1].

1) Centrality (Degree)

To comprehend networks and their participants, we evaluate the location of participants in the network. *Degree* provides the relative importance and the location of a particular node in the network. *Degree* and similar measures indicate various roles of the nodes in a network, for example leaders, gatekeepers, role models etc [3]. A node is central if it is strategically located on the communication route joining pairs of other nodes [4][5]. Being central it can influence other nodes in the network, in other words potentially it can control the flow of information. The potential of control makes the centrality conceptual model for these nodes. The idea of centrality is not new it was first applied to human communication by Baveles in 1948 [4][6]. In this study relationship between structural centrality and influence in group processes were hypothesized. Following Baveles it was concluded that centrality is related to group efficiency in problem-solving, perception of leadership and the personal satisfaction of participants [7][8][9]. In the fifties and sixties more research was conducted on these measures and it was concluded that centrality is relevant to the way groups get organized to solve problems. The following references provide a very deep and pioneering work on these measures [10][11][12][13][14][15][16][17][18][19].

The centrality concept is not exclusive to deal with group problem tasks, it has been used in other discipline as well [20][21]. A number of centrality measures have been proposed over the past years. Most of the centrality measures are based on one of two quite different conceptual ideas and can be divided into two large classes [22]. The measures in the first class are based on the idea that the centrality of an individual in a network is related to how it is near to others. Second class of measures is based on the idea that central nodes stand between others on the path of communication [23][24][25]. A node being on the path of other nodes communication highway has the potential to control what passes through it. The simplest and most straightforward way to quantify the individual centrality is therefore the *degree* of the individual, i.e., the number of its immediate neighbors. In figure 1 a graph with seven nodes and seven edges is shown, nodes 2 and 3 are adjacent to each other, the number of nodes to which a given node is adjacent is called the *degree* of that point.

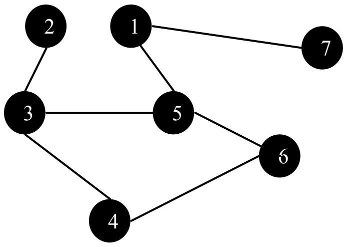

Figure 1: A Graph of 7 Nodes

Therefore, node 5 for example has a *degree* of 3. In a graph if every node is reachable from any node in the graph it is called a connected graph, which is the case in figure 1. Each path in the graph is associated with a *distance* equal to the number of edges in the path and the shortest path to reach a given pair of nodes is *geodesic* distance. For example path from node 2 to node 1 through nodes 3 and 5 is a geodesic as the other path for the same pair is also reachable through nodes 3, 4, 6 and 5 but has longer distance. Nieminen has provided a very systematic elaboration of the concept of *degree* [26]. Scott has extended the concept based on *degree* beyond immediate (first) neighbors by selecting the number of points an individual can reach at a distance two or three [27]. Similarly, Freeman produced a global measure based on the concept of *closeness* in terms of the distances among the various points [24]. The simplest notion of *closeness* is obtained by the sum of the geodesic distances from an individual to all the other points in the graph [28].

2) Betweenness

Betweenness measures to what extent a node can play the role of intermediary in the interaction between the other nodes. The most popular and simple *betweenness* measure based on geodesic path is proposed by Freeman and Anthonisse [23][25]. In many real scenarios however, communication does not travel exclusively through geodesic paths. For such situations two more *betweenness* measures are developed first based on all possible paths between couple of nodes [29] and second based on random paths [30].

3) Closeness

Another more sophisticated centrality measure *closeness* based on geodesic distance can be defined, which is the mean geodesic (i.e., shortest path) distance between a node and all other nodes reachable from it. *Closeness* can be regarded as a measure of how long it will take information to spread from a given node to other nodes in the network.

III. Mathematics of Centralities

Typically, centrality means *degree*, with respect to communication a node with relatively high *degree* looks important. In a social network a node that has directly connected with many other nodes actually see itself and be seen by others in the network as the indispensable source of information, for example node 5 in figure 1. This means a node with low *degree* is isolated from direct involvement, see itself and seen by others as not a stakeholder, node 7 in figure 1. A general measure of centrality based on *degree* is given $D_c(p_j)$ by [24];

$$D_C(p_j) = \sum_{i=1}^{n} d(p_i,\ p_j) \qquad (1)$$

where

$$d(p_i,\ p_j) = \begin{cases} 1\ p_i \,\&\, p_j & \textit{directly connected} \\ 0\ p_i \,\&\, p_j & \textit{not connected} \end{cases}$$

The magnitude of this equation is partly a function of the size of the network, which may be useful in determining the absolute activity of a node. On the other hand in some cases it may be desirable to have measure which is independent of the network size. For example, to compare the relative centrality points from different graphs one might need a measure from which the effect of the network size has been removed. Any node in the network can be adjacent to maximum of (n – 1) number of nodes in the graph. Therefore, maximum of $D_c(p_j)$ is the proportion of other nodes that are adjacent to p_j.

$$D'_C(p_j) = \frac{\sum_{i=1}^{n} d(p_i,\ p_j)}{(n\ -\ 1)} \qquad (2)$$

Betweenness is centrality measure of a node within a graph (network); nodes located on many shortest paths (geodesics) between other nodes have higher *betweenness* compared with others. For a graph $G = (V, E)$ with $\boldsymbol{n}$ vertices, the *betweenness* $C_B(k)$ for vertex $\boldsymbol{k}$ is:

$$C_B(k) = \sum_{i \neq j \neq k \in V} \frac{\sigma_{ij}(k)}{\sigma_{ij}} \qquad (3)$$

where σ_{ij} is the number of shortest geodesic paths from i to j, and $\sigma_{ij}\ (k)$ the number of shortest geodesic paths from i to j that pass through a vertex *k*. It could be normalized by dividing through the number of pairs of vertices not including *k*, which is (n − 1)(n − 2). Calculation of *betweenness* is quite complicated for networks when several geodesics connect a pair of nodes, which is the case in most real world networks. Also, $C_B\ (k)$ is dependent on the size of the network on which it is being calculated. Freeman [24] has provided relative centrality of any node in the network by the following relationship.

$$C'_B(k) = \frac{C_B(k)}{(n^2 - 3n + 2)/2} \qquad (4)$$

The idea is that maximum value of $C_B\ (k)$ is achieved by the central point of the *star* and is given by;

$$\frac{n^2 - 3n + 2}{2} \qquad (5)$$

Therefore, the relative *betweenness* centrality is determined by the ratio given in equation 4 and is re-written as equation 6.

$$C'_B(k) = \frac{2C_B(k)}{(n^2 - 3n + 2)} \qquad (6)$$

Yet another centrality measure which has been used in social network analysis is called c*loseness*. From retrospect c*loseness* can provide the information about nodes independence. Let us consider a set of nodes and their connections as shown in figure 2. Node 1 is directly connected with all the nodes except node 6, therefore to reach node 6 it must use node 3. Actually, it means that node 1 only needs one relayed base to communicate with every node in the network. However, node 2 or 4 needs node 1 three times and node 3 once to communicate with every one in the network. Therefore, it can be stated that node 1 is closer to all other nodes in the network. It has greater centrality of being independent of others.

The simplest mathematics for c*loseness* centrality is provided by [28], which is determined by summing the geodesics from a point of interest to all other points in the network and taking its inverse. *Closeness* grows as the distance between node ***j*** and other nodes ***(i….n)*** increases. The *Closeness* $\mathbf{C_C}$ is given by;

$$C_C(j) = \left[\sum_{i=1}^{n} d(i,\ j)\right]^{-1} \qquad (7)$$

Where *d* is the geodesic distance between respective nodes, for all those nodes which are not connected the geodesic distance is infinity. The above expression is dependent on the size (number of nodes) of the network and it is appropriate to have an expression which is independent of this limitation.

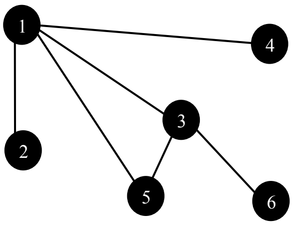

Figure 2: Sample Graph for *Closeness*

Beauchamp [31] suggested that relative *Closeness* (point centrality) for a node is given by;

$$C_C(j)' = \frac{n-1}{\sum_{i=1}^{n} d(i,\ j)} \qquad (8)$$

IV. IMPLEMENTATION

In the implementation of the system, the structure of each node in the network has been characterized by the following 18 attributes. The node structure is extendable to include more attributes however in the present study it is believed that the considered attributes cover most aspects of a node. As it is stated earlier these attributes actually constitute the framework for the evaluation of a weighting index for each node to determine the potential of its importance in the network. It should also be noted that each attribute could have multiple levels of description that could be seen later in the tables where such attributes are described in detail. The attributes are:

1) Name
2) Religion
3) Age
4) Status (Married, Unmarried etc)
5) Nationality
6) Education
7) Criminal History
8) Converted (Religion Change)
9) Known affiliation
10) Job (Kind)
11) Activity (which is making him/her suspect)
12) Ability to Recruit
13) Communication Frequency level
14) Social Image
15) *Degree* Score
16) *Betweenness* Score
17) *Closeness* Score
18) Known Associates

There are two main phases for the analysis of the network. During the first phase, the weighting index corresponding to each node is determined based on the attribute values. The weighting index gives an empirical value, higher value indicate the importance of the node and vice versa. In the second phase argument driven multiple hypotheses are generated and executed to correct or tune the real value of the weighting index hence, reflecting its actual potential. Each attribute is constructed as a table, for example see table 1 for *name attribute*. Typically, each *name* is like a signature having unique structure like fingerprint providing an individuals location, ethnicity, race etc., although terrorists may be using cover or stolen identity names. For each possibility a score is attached to provide its level of threat (table 1). The color background in the table is provided to make a correspondence between possibilities and the individual score. It should be noted here that the names of the countries are shown as A, B, C…. to avoid any mis-understanding meaning not to offend any individual if he/she belongs to these specific countries. In the implementation actual names of the countries are used.

Now from table 1 first possibility means the *name* is in the database the individual is known to be a terrorist. This means the individual is known to the agencies and pose more threat compared with some one unknown, therefore given a higher score. However, one can argue that an individual who is not on the radar could be more lethal. The answer for this argument could be both yes or no but remember this score is actually not the final value.

Table 1: Name Attribute

Attribute Name	Possibilities		Score
Name	In Database		7
	From known countries where terrorists or terrorists cell exist	A	6
		B	5
		C	4
		D	3
		E	2
	From rest of the world		1

The second possibility is that the *name* belongs to a specific country and is not in the database. Therefore, a score specific to that country is selected (which is based on the threat level posed by the respective country). However, in such cases where the *name* belongs to more than one country the highest value of the score among them is selected. Table 1 is showing 5 different scores for this possibility but actually there are more countries *name* and the respective threat scores. Finally, if both possibilities are false a low or minimum score is attached. Following tables 2 and 3 show two more attributes with corresponding possibilities of threat scores. The tables for the rest of the attributes are not shown to avoid repetition, although each one is different however, there structures are similar.

Finally, after retrieving each attribute from the database with corresponding threat score the initial empirical value of the weighting index is calculated and attached to the node. Now the second phase starts with argument driven hypotheses execution, let us explain it through an example given in figure 3. From the figure it can be seen that this particular node has a weighting index value of 23. Now the *first argument* is that: the individual is un-married, age is also in the range that he/she may be more likely to be emotional/radicalized. Therefore, threat score corresponding to age and status is not true. *Second argument,* individual is un-married and education is a *chemistry* graduate, so threat scores corresponding to education and status are not true. It is more likely that the individual has a potential to construct a very sinister thing based on his/her knowledge and age (emotional, radicalized, groomed etc). Therefore, the weighting index value 23 for this node is not reflecting what he/she is capable of, so it has to be increased by a certain level determined by the argument evaluation process. Similarly, more argument based hypotheses are executed by looking at selected individual attributes to obtain an optimum value.

Table 2: Education Attribute

Attribute Name	Possibilities		Score
Education	Graduate/ Post Graduate	Chemistry	6
		Physics	5
		Nuclear	6
		Computer Science	5
		.	.
		.	.
		Humanities	4
	College		4
	School		3
	Religious School		4
	Skilled		3

Table 3: Age Attribute

Attribute Name	Possibilities	Score
Age	15 – 25	3
	25⁺ – 40	2
	40⁺ -	1

The hypothesis evaluation is computationally demanding as one can see due to the amount of permutations for various comparative reasoning. After all the nodes are dealt and the tuned (optimum) weighting index is determined for each node the prediction of path cycle starts. Now from a realistic point of view one need to eliminate couple of key player nodes to disrupt the network structure. Therefore, in our study 25% nodes from the network are selected to highlight the important/valuable path. These nodes if removed from the network could lead to weaken/destabilize if not fully nonfunctional network. When ever 25 % value is a fraction it is rounded to the next integer value. However, during the highlighting process the system may increase the number of nodes from 25% value to keep the continuity of the route. Practically it is not possible to kill or capture all the members of a terrorist network so we have selected a rudimentary (brute force selection) value of 25%, which can be increased or decreased depending upon the size of the network.

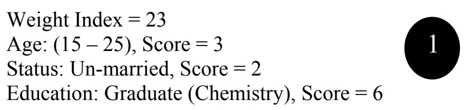
Weight Index = 23
Age: (15 – 25), Score = 3
Status: Un-married, Score = 2
Education: Graduate (Chemistry), Score = 6
1

Figure 3: Second Phase

V. Results and Conclusion

In this study 3 networks with different number of nodes are selected, first two are called random as the system selected the node attributes randomly through the network generator engine of *TANetworkTool* (Terrorist Analysis Network Tool), third one is the known 9-11 hijackers network. At present we have a database with *names, nationalities, religion, education and Job/work* mostly known so far from open sources database like trackingthethreat.com etc. The network generator engine of *TANetworkTool* takes the *nationality, name, known affiliation* from the above mentioned database. Afterwards, other attributes for example *age* (16 – 35), *married status*, *links (connectivity) with other nodes* etc., are randomly selected from a normal distribution.

1) Random Network 1

The first network consists of 20 nodes as shown in figure 4. The *TANetworkTool* after the analysis that is, computation of tentative weighting index score for each node and finally calculating the optimum weighting index score has predicted a path for 25 % nodes of the network. The path consists of 5 nodes *Mustafa Ahmed al-Hisawi, Essoussi Laaroussi, Abu Qatada, Hani Hanjour and Mamoun Darkazanli* shown by the dotted line on figure 4. When the nodes along the path are removed one can see the damage caused through our method in figure 5. The system has clearly broken the structure of the network by removing key player nodes *Abu Qatada* and *Hani Hanjour*. *Abu Qatada* is very important node in terms of its placement in the network as its *Betweenness* and *Closeness* score is higher than any other node in the network. Figure 6 shows all the centrality measure score along with optimum weighting index and the names of five nodes which system has predicted for path illumination. It can also be seen that the system has predicted some of the nodes not having a larger value of *Degree*, *Betweenness* or *Closeness* centrality. The reason being attributes data is generated randomly so it is not necessary that nodes having larger value for any of these centrality measures will also have other attributes larger. For simplicity if we consider *Degree* based centrality measure for example to select 5 nodes (25 %) to be removed from the network then *Abu Qatada, Mohammad Bensakhria, Zacarias Moussaoui, Abu Walid and Hani Hanjour* are selected straight away. Now if we remove these nodes the destruction is almost similar or may be even better than compared to our method. Typically, in SNA node having larger *Degree* centrality is believed to be a central/key player node, however, some time terrorist networks may camouflage/disguise/conceal their connectivity. Therefore, our method has the potential to perform better even if the connectivity is not apparently transparent. Reason being the system depends on collective attributes rather than only one centrality attribute like *Degree, Betweenness* or *Closeness.*

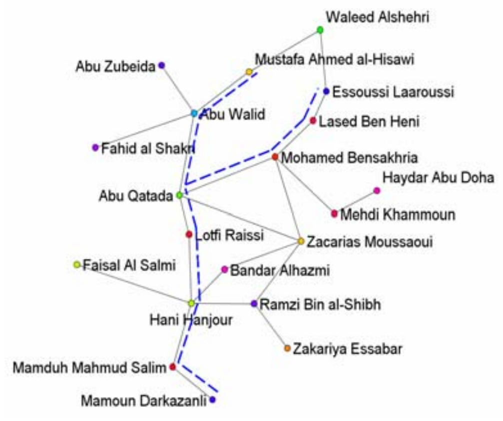

Figure 4: Network of 20 Nodes

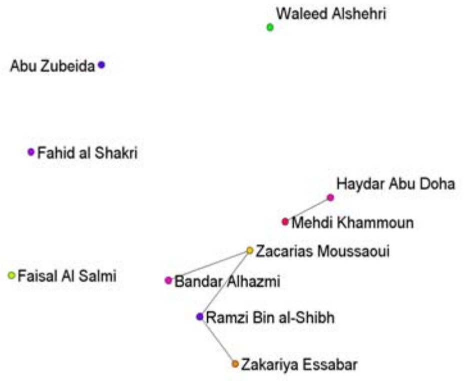

Figure 5: Network Structure after 5 nodes removed

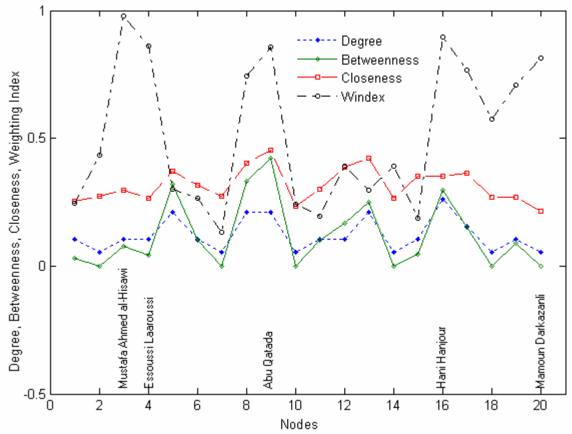

Figure 6: Centrality Measures & Weighting Index

2) Random Network 2

The second network considered for analysis consists of 30 nodes as shown in figure 7. By looking at the network we could see that *Abu Zubeida, Fayez Ahmed* and *Majed Moqed* are the key player nodes because of their placement in the network structure. Figure 8 shows all the centrality measures along with optimum weighting index for the whole network. However, the names of only those nodes are shown which system has predicted for path illumination. The path is shown by a dotted line on figure 7. Now if we remove the nodes along the path as shown in figure 9, one could clearly see the destruction suffered by the network. Although it has not selected nodes like *Abu Zubeida* and *Fayez Ahmed* which have the highest centrality measures in the network. But still the system has been able to remove (predict) nodes in such a way to make the network de-fragmented or may be even non functional.

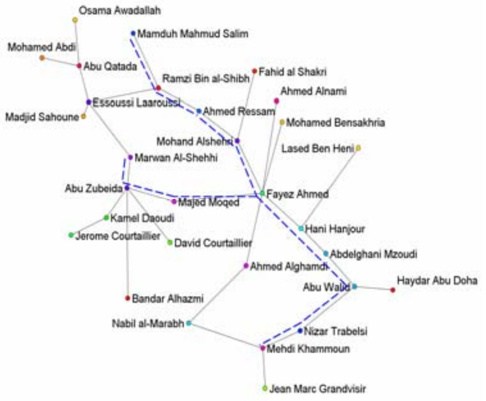

Figure 7: Network with 30 Nodes

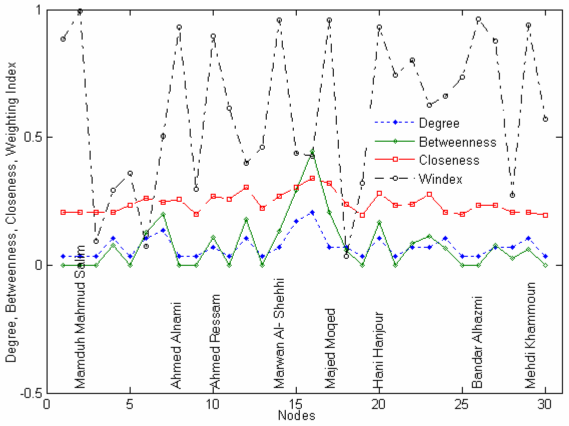

Figure 8: Centrality Measures & Weighting Index

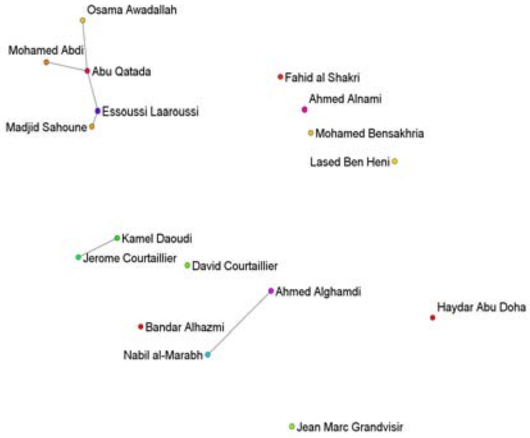

Figure 9: Network Structure after 8 nodes removed

1) 9-11 Hijackers Network

To conclude our analysis we selected the famous 62 nodes network of 9-11 hijackers and collaborators as shown in figure 10 *by Valdis E. Krebs* [1]. Therefore, this time there is no random connectivity and no random attribute selection. All the data attributes are real as obtained from the open sources. We can see that *Mohammed Atta, Marwan Al Shehhi, Fayez Ahmed, Wail Alshehri, Nawaf Alhazmi, Saeed Alghamdi, Ziad Jarrah, Zacarias Moussaoui* and *Ramzi Bin al Shibh* are the key player/important nodes of this network because of their centrality measure scores. The dotted line on figure 10 shows the path our system has predicted. Now if we remove these nodes indicated through our optimum weighting index score shown in figure 11 one could see the damage suffered by the network in figure 12.

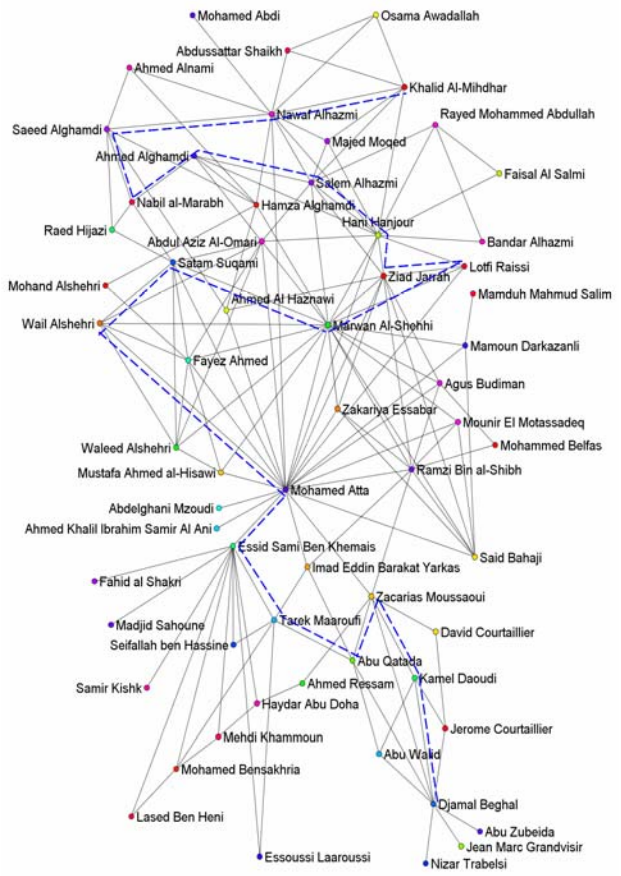

Figure 10: 9-11 Hijackers and Collaborators

It can be seen from figure 12 that it has broken the network in such a way that it would have been very difficult to be operational with such fragmented network structure. It should also be noted that all those single nodes which became un-connected after path removal are also been omitted from the figure to see the fragmented graph more clearly. Most of the 19 hijackers are either illuminated by our predicted path or left in a segment which could not pose an immediate threat. The reason of selecting this known network is that almost all attributes are known and these are used as benchmark to verify that our argument driven hypothesis model works transparently for a given network. In this study firstly simulated random data generation technique is used for the verification of the proposed SNA architecture model. Secondly, a known network data of 9 – 11 hijackers and their collaborators is used to benchmark our process of hypotheses evaluation. It shows that our method has enumerated all the important/key-players of this network.

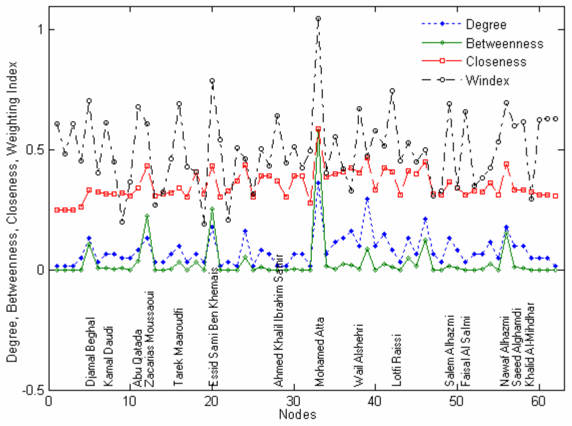

Figure 11: Centrality Measures & Weighting Index

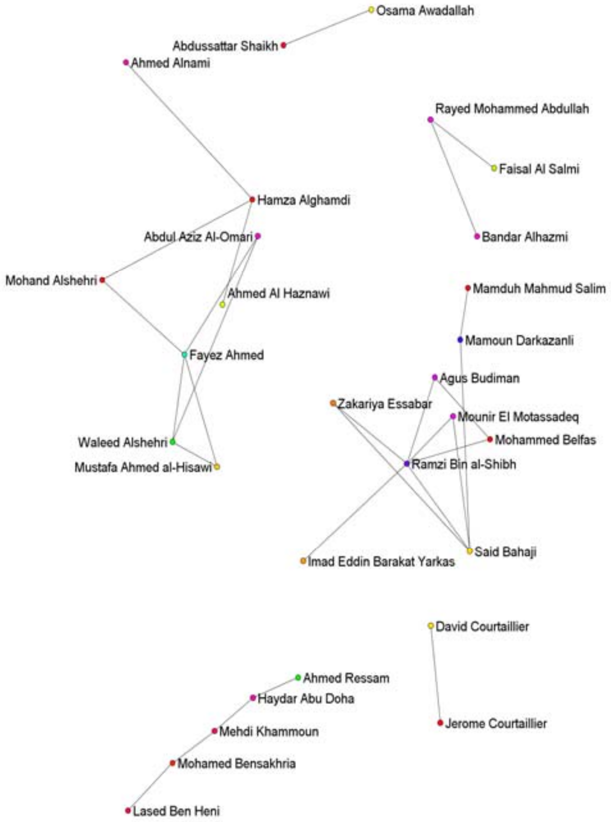

Figure 12: Network Structure after 15 nodes removed

The result for 9 – 11 hijackers/collaborators is not to prove (once again) what has already been established for that network rather it is to compliment our proposed models working capability in identifying various important nodes. Typically, to destabilize or disrupt the functionality of a terrorist/covert network one has to see if the following has been achieved;

1. Information flow has been severely affected.
2. Network is not functional as an organization.
3. Technical expertise/support is not available.

Our method has shown that even with a quarter (25 %) number of nodes selection for removal from the entire network it can achieve the upper stated goals. The reason being it is using the argument driven hypotheses that reflect real scenarios by arguing logically to evaluate threat pose by a particular node. One of the key factor in most SNA methods is that these procedures are data hungry which is also the case with the proposed method as well. However, proposed framework model has more potential to deal and predict accurately when the link/connectivity is not transparent as one would expect in modern day terrorist and covert network. The data about a network is never complete or correct and also there is fuzziness in many situations. Therefore, our analysis could produce inconsistent/improved results at different time instances as the data may be different at those discrete time intervals.

References

[1] Valdis Krebs; Connecting the Dots -- Tracking Two Identified Terrorists, 2002.

[2] Kathleen M. Carley, Ju-Sung Lee, David Krackhardt; Destabilizing Networks, Dept. of Social and Decision Sciences, Carnegie Mellon University, Pittsburgh, PA 15143, November 2001.

[3] Nasrullah Memon, Henrik Legind Larsen, **D. M. Akbar Hussain:** Constructing Hierarchy of Non-hierarchical Terrorist Networks, Study from Theory to Implementation for Analyzing and Destabilizing Terrorist Networks, Published in the proceedings of Descartes Conference on Mathematical Models in Counterterrorism, DCMMC - 2006, Washington DC, USA, September 28 – 29 2006.

[4] Bavelas, A.; A mathematical model for group structures". Human Organization 7: Pages 16-30, 1948.

[5] Shaw M. E.; Group structure and the behaviour of individuals in small groups". Journal of Psychology Vol. 38, Pages 139 – 149, 1954.

[6] Bavelas, A.; Communication patterns in task oriented groups". Journal of the Acoustical Society of America Vol. 22, Pages 271-282, 1950.

[7] Leavitt Harold J.; Some effects of communication patterns on group performance. Journal of Abnormal and Social Psychology Vol. 46, Pages 38-50, 1951.

[8] Smith Sidney L.; Communication Pattern and the Adaptability of Task-oriented Groups: an Experimental Study. Cambridge, MA: Group Networks Laboratory, Research Laboratory of Electronics, Massachusetts Institute of Technology, 1950.

[9] Bavelas, A. and D. Barrett; An experimental approach to organizational communication. Personnel Vol. 27, Pages 366-371, 1951.

[10] Glanzer M. and R. Glaser; Techniques for the Study of Team Structure and Behaviour. Part II: Empirical Studies of the Effects of Structure. Technical Report, Pittsburgh, American Institute, 1957.

[11] Glanzer M. and R. Glaser; Techniques for the study of group structure and behaviour. Part II: Empirical studies of the effects of structure in small groups. Psychological Bulletin 58, Pages l - 27, 1961.

[12] Cohen A. M; Communication networks in research and training. Personnel Administration 27, Pages 18-24, 1964.

[13] Shaw M. E.; Communication networks", In L. Berkowitz (ed.), Advances in Experimental Social Psychology, Vol. VI, Pages 111 – 147, New York, Academic Press, 1964.

[14] Stephenson, K. A. and Zelen, M., 1989. Rethinking centrality: Methods and examples, Social Networks 11, Pages 1–37, 1989.

[15] Flament C.; Applications of Graph Theory to Group Structure. Englewood Cliffs, NJ, Prentice Hall, 1963.

[16] Burgess R. L.; Communication networks and behavioural consequences". Human Relations 22, Pages 137 - l59, 1968.

[17] Snadowski A.; Communication network research: an examination of controversies". Human Relations 25, Pages 283 - 306, 1972.

[18] Rogers D. L.; Socio-metric analysis of inter-organizational relations: application of theory and measurement. Rural SocioEonv 39, Pages 487 – 503, 1974.

[19] Rogers E. M. and R. Agarwala Rogers; Communication networks in organizations. Communication in Organizations, Pages 108-148, 1976, New York, Free Press.

[20] Cohn B. S. and M. Marriott; Networks and centres of integration in Indian civilization. Journal of Social Research I, Pages 1 – 9, 1958.

[21] Pitts F. R.; A graph theoretic approach to historical geography, the professional geographer 17, Pages 15 - 20, 1965.

[22] Latora V, Marchiori M.; A measure of centrality based on network efficiency, arxiv.org preprint cond-mat/0402050, 2004.

[23] Freeman Linton C.; A set of measures of centrality based on betweenness. Sociometry 40, Pages 35 - 41, 1977.

[24] Freeman Linton C.; Centrality in social networks: I. Conceptual clarification. Social Networks 1, Page 215 – 239, 1979 .

[25] Anthonisse J. M.; The rush in a graph. Amsterdam: University of Amsterdam Mathematical Centre, 1971.

[26] Nieminen J.; On centrality in a graph. Scandinavian Journal of Psychology 15, Pages 322 – 336, 1974.

[27] Scott J.; Social Networks Analysis. 2nd Edition, Sage Publications, London, 2003.

[28] Sabidussi G.; The centrality index of a graph. Psychometrika 31, Pages 581 - 603, 1966.

[29] Freeman Linton C., Stephen P. Borgatti and Douglas R. White; Centrality in valued graphs, A measure of betweenness based on network flow. Social Networks 13, Pages 141 – 154, 1991.

[30] Newman M. E. J.; A measure of betweenness centrality based on random walks, cond-mat/0309045, 2003.

[31] Beauchamp, M. A.; An improved index of centrality, Behavioral Science 10, Pages: 161 – 163, 1965.

D. M. Akbar Hussain is an Associate Professor of Computer Science and Engineering in the Software Engineering and Media Technology Department at Aalborg University Esbjerg, Denmark. His research interests are investigation of applications which are not only computationally expensive but also require large memory for storage. For example, Multiple Target Tracking, Air Traffic Control (ATC) Systems, Social Network Analysis (SNA) and Biometrics like Fingerprint matching. He has been actively doing research in these areas, especially developing algorithms to deal with data association techniques like; Track Splitting, Probabilistic Data Association Filter (PDAF) and Joint Probabilistic Data Association (JPDA). He is also involved in developing procedures, techniques, models to destabilize terrorist networks. He received his Masters degree from Punjab University, Pakistan in 1979 and PhD in Control Engineering from Sussex University, UK in 1992. Prior to his current position he has worked in the industry Lineo Inc, Canada. Dr. Akbar is a member of IEEE, IAENG and IDA.