Measuring Link Importance in Terrorist Networks

Uffe Kock Wiil, Jolanta Gniadek, Nasrullah Memon
Counterterrorism Research Lab
The Maersk Mc-Kinney Moller Institute
University of Southern Denmark
Campusvej 55, 5230 Odense M, Denmark
ukwiil@mmmi.sdu.dk

***Abstract*—A terrorist network is a special kind of social network with emphasis on both secrecy and efficiency. Such networks are intentionally structured to ensure efficient communication between members without being detected. A terrorist network can be modeled as a generalized network (graph) consisting of nodes and links. Techniques from social network analysis and graph theory can be used to identify key entities in the network, which is helpful for network destabilization purposes. Research on terrorist network analysis has mainly focuses on analysis of nodes, which is in contrast to the fact that the links between the nodes provide at least as much relevant information about the network as the nodes themselves. This paper presents a novel method to analyze the importance of links in terrorist networks inspired by research on transportation networks. The link importance measure is implemented in CrimeFighter Assistant and evaluated on known terrorist networks.**

Social network analysis, terrorist network analysis, graph theory, transportation networks, CrimeFighter Assistant

I. INTRODUCTION

A terrorist network is a special kind of social network with emphasis on both secrecy and efficiency. Such networks are intentionally structured to ensure efficient communication between members without being detected [1], [2], [3].

Knowledge about the structure and organization of terrorist networks is important for both terrorism investigation and the development of effective strategies to prevent terrorist attacks. Theory from the knowledge management field plays an important role in dealing with terrorist information. Knowledge management processes, tools, and techniques can help intelligence analysts in various ways when trying to make sense of the vast amount of data being collected in relation to terrorism [4]. The collected data needs to be analyzed and visualized in order to gain a deeper understanding of the terrorist network.

A terrorist network can be modeled as a generalized network (graph) consisting of nodes and links. Nodes are entities (people, places, events, etc.) with attributes allowing relevant information to be stored about the entities. Links are relationships between the entities. Links have attributes that describe properties about the relationships.

Techniques from social network analysis (SNA) and graph theory [5] can be used to identify key nodes in the network, which is helpful for network destabilization purposes [6]. Taking out key nodes will decrease the ability of the terrorist network to function normally.

However, research on terrorist network analysis (TNA) has mainly focuses on analysis of nodes. Links are seldom first class objects with the same properties as nodes. This is in contrast to the fact that the links between the nodes provide at least as much relevant information about the network as the nodes themselves [7].

A terrorism domain model with both nodes and links as first class objects will allow additional features to be built into the terrorist network analysis and visualization tools. Hence, a possible response to the above mentioned issue is to develop new measures for terrorist network analysis focusing on links. Aiming for a better balance between analysis of nodes and analysis of links, results in additional and more precise knowledge about the terrorist network.

This paper presents a novel method to analyze the importance of links in terrorist networks inspired by research on transportation networks. The link importance measure is implemented in CrimeFighter Assistant and evaluated on known terrorist networks (the 9/11 attack and the 2002 Bali night club bombing).

The remainder of this paper is structured as follows. Section 2 describes various techniques that can be used to analyze terrorist networks. We start by looking at general techniques related to analysis of social networks and continue by looking at specific techniques that are related to analysis of terrorist networks. In Section 3, we present and evaluate our new method to analyze the importance of links in terrorist networks. Section 4 concludes the paper and discusses future work.

II. TERRORIST NETWORK ANALYSIS

This section presents techniques that are useful to analyze terrorist networks. The starting point for TNA is the existence of a network structure. Hence, much knowledge management work needs to take place prior to network analysis. Data needs to be gathered, data needs to be processed (filtered, mined, etc.) to create useful information in the form of a network structure. These prerequisite knowledge management processes are not the focus of this paper.

The network analysis phase should result in new insights (knowledge) about the network, the entities, and the relations. Also, the achieved knowledge must be visualized in a human comprehensible way to enable the intelligence analysts to make informed decisions (recommendations) about possible actions to destabilize the network.

A. General Social Network Analysis Techniques

Since a terrorist network is a special kind of social network, many techniques useful to analyze social networks are also applicable to TNA. SNA relies to a large extent on a mathematical model in the form of a graph and a set of algorithms that traverses the graph in various ways to analyze the network.

A graph G consists of two sets of information: a set of nodes, $N = \{n_1, n_2, \ldots, n_n\}$, and a set of links $L = \{l_1, l_2, \ldots, l_l\}$ between pairs of nodes. There are n nodes and l links. In a graph, each link is an unordered pair of distinct nodes, $l_k = \{n_i, n_j\}$.

Small graphs can provide visual information about the network, but for larger graphs it is difficult to perform analysis visually. Graph theory provides several ways to measure social networks:

- **Size** is defined as the number of nodes (n) in the network.
- **Density** is the number of links (l) in proportion to the number of links that are possible in G (if all nodes where connected to each other).
- **Nodal degree** is defined as the number of links that are incident with the node.
- A **cluster** is a part of the graph with high density of nodes and links between them.
- The **average shortest path** is the average length of the geodesic between two nodes.
- **Node degree centrality**. A node is central when it has many ties (links) to other nodes in the network. This kind of centrality is measured by the degree of the node. The higher the degree, the more central the node is.
- **Node closeness centrality** indicates that a node is central when it has easy access to other nodes in the network. This means that the average distance (calculated as the shortest path) to other nodes in the network is small.
- **Node betweenness centrality**. Usually, not all nodes are connected to each other in a network. Therefore, a path from one node to another may go through one or more intermediate nodes. Betweenness centrality is measured as the frequency of occurrence of a node on the geodesic connecting other pairs of nodes. A high frequency indicates a central node.
- **Eigenvector centrality** is like a recursive version of node degree centrality. A node is central to the extent that the node is connected to other nodes that are central. A node that is high on eigenvector centrality is connected to many nodes that are themselves connected to many nodes.

Wasserman and Faust [5] provide additional details about SNA.

B. Specific Terrorist Network Analysis Techniques

Terrorist networks are covert networks. Covertness is the major difference between terrorist and regular social networks. In terrorist network, ties between participants are usually strong, but not transparent and visible in every day routine. Relations are long-term; participation in a terrorist plot requires a high level of trust in the network. Terrorist networks are often "sleeping"; they are prepared, but remain inactive. This way they are more difficult to uncover.

As Krebs [8] noticed, a covert network must be active at times. It is during these periods of activity that they may be most vulnerable to discovery. Social networks in covert organizations tend to structure themselves towards better efficiency or robustness [9]. According to the definition of efficiency in [10], the most efficient network is a clique of the size of the network (a complete graph with density equal to 1). Yet, this structure makes the terrorist networks vulnerable to detection. If one suspect is uncovered, observation of this suspect allows investigators to determine all suspects that are connected to this suspect. Hence, the whole network would be easily disrupted. This example shows that terrorist networks cannot operate in the same way as regular social networks. Terrorists want to keep their actions (attacks are an exception) and relations hidden from the public. According to Baker and Faulkner [11], the need for secrecy is crucial to covert networks. Thus, terrorist networks have to find a balance between efficiency and secrecy.

What then determines the **secrecy** of a network? Lindelauf et al. [3] proposes a measure of secrecy which is defined by two parameters: the exposure probability and the link detection probability. The exposure probability applies to individual nodes and depends on the location in the structure. It is defined as the probability of a member of the network to be detected as a terrorist. Link detection probability represents the chance of exposure of a part of the network if a member is detected.

Considering the above measure of secrecy, the safest structure of a terrorist network would be a path graph, where all the nodes know only two neighboring nodes. Looking at this structure from an information exchange perspective, the weakness is obvious. Information has to travel a long distance from one part of the network to another and that decreases the efficiency of the network. The lower the efficiency, the worse communication and coordination in the network – to the point when launching successful operation becomes impossible.

According to the definition in [10], **efficiency** is a measure to quantify how efficiently the nodes of a network can exchange information. To calculate the efficiency of network, all the shortest path lengths between any pair of nodes in the graph must be calculated. The assumption is made that every link can be used to transfer information in the network. The efficiency is calculated in two parts: (1) the inverse of the sum of the shortest paths between any pair of nodes are calculated; (2) the result from (1) is divided by the possible number of pairs of nodes to find the average efficiency of the network.

Various measures used in TNA will be exemplified below by describing them in relation to the 9/11 hijackers and associates network presented in [8] (Figure 1).

Figure 1. The 9/11 hijackers and associates network [8].

SNA measures of the 9/11 hijackers and associates network:

- **Size**. The full 9/11 network consisted of 62 persons. The core of the network (only the hijackers) consisted of 19 persons divided into 4 groups of strongly connected members.
- **Density**. The density of the full network is very low (0.08). It shows that the network overall focused on few connections between members to ensure a high level of secrecy.
- **Nodal degree**. The average nodal degree of the full network is 4.9 which mean that detection of one member would potentially comprise 5 other members.
- **Clusters**. The core of the 9/11 network has a high density (0.585). It shows that inside the trusted core there was a focus on a high level of efficiency.
- **Average shortest path**. The diameter of the network (the longest shortest path) is 5. The average shortest path is 2.92. Thus, on average information needs to travel through 3 links to reach the target.
- **Node centralities**. When calculating the node centralities (degree, closeness, betweenness, and eigenvector), a small group of people was pointed out as central in the network. Table 1 ranks members according to the combined score of the centrality measures – only the top 10 ranked members out of 62 are listed. The scores marked in bold face are the top three scores for that measure (again out of 62).

  A closer look at the numbers in Table 1 shows that the first 4 on the list (Atta, Al-Shehhi, Hanjour, and Jarrah) each belonged to a different hijacked plane. The next 2 on the list (Moussaoui and Khemais) are central in the part of the network that connects the hijackers to the associates.

TABLE I. NODE CENTRALITIES OF 9/11 NETWORK.

Person	Degree	Closeness	Between-ness	Eigenvec-tor
Atta	**0.361**	**0.587**	**0.588**	**0.412**
Al-Shehhi	**0.295**	**0.466**	0.088	**0.399**
Hanjour	**0.213**	**0.445**	0.126	0.249
Jarrah	0.164	0.424	0.017	**0.258**
Moussaouri	0.131	0.436	**0.232**	0.084
Khemais	0.180	0.433	**0.252**	0.059
Al-Omari	0.148	0.424	0.023	0.237
Al-Shibh	0.164	0.436	0.048	0.233
Ahmed	0.131	0.407	0.026	0.201
Bahaji	0.115	0.399	0.002	0.198

The above example based on the full 9/11 network shows how traditional measures of SNA can play a role in TNA. These kinds of measures are sensitive to changes in the network. We must assume that there are missing modes and links in the network (members and ties that were not discovered in the investigation). Thus, uncovering new members and ties will change centrality measures. However, these methods still give a good measure of the importance of members in the part of the network that was detected.

According to the efficiency measure in [10], the efficiency of 9/11 network is 0.395. According to the secrecy measure in [3], the secrecy of the 9/11 network is 0.86, while the secrecy of the hijackers part of the network is lower (0.77) as this part has a higher density.

In addition to the above SNA measures, various measures related to TNA have been proposed in the literature.

Memon [12] proposed several new analysis measures and destabilization methods including:

- **Position Role Index** (PRI) is a measure aimed at making a distinction between the gatekeeper and follower roles. PRI evolved from testing efficiency of a network based on the assumption that a network without followers has a higher efficiency as followers are less connected within the structure. PRI is measured as the change of network efficiency after removal of a node. A high PRI value indicates a large loss in efficiency, if a particular node is removed.
- **Detecting hidden hierarchy**. This method aims to identify hidden hierarchical structures in horizontal networks. The method uses SNA measures and graph theory to indicate parent-child relationships of nodes in the network.
- **Subgroup detection**. A terrorist network can often be partitioned into cells (subgroups) consisting of individuals who interact closely with each other. This method uses SNA measures and graph theory to indicate clusters (subgroups) in relation to a particular node and the diameter from that node.

These methods can be used to provide a richer and deeper understanding and insight into terrorist networks to enable better approaches to destabilize them.

Rhodes [13] proposed the use of Bayesian inference techniques to predict missing links in a covert network demonstrated through a case study of the Greek terrorist group November 17. The assumption is that during the analysis of terrorist networks it is unlikely that the intelligence analysts have an overview of the full terrorist network. Prediction of missing links can be a useful method to gain deeper understanding and conduct detailed analysis of the terrorist network.

One of a very few metrics that includes the property of links is link (edge) betweenness centrality. It measures the frequency of link occurrence on the geodesic connecting pairs of nodes [14]. Link betweenness indicates how much information flows via a particular link. The assumption is that communication flows along the shortest path. A high frequency indicates a central link. Newman [15] has proposed a variant of link betweenness centrality based on random walks instead of shortest paths.

C. *Summary*

This section has reviewed various techniques for analyzing terrorist networks. The usefulness of a number of these techniques was demonstrated through an example using the full 9/11 network as presented by Krebs [8]. The techniques primarily focus on estimating the importance of nodes of the networks. Few techniques focus on estimating the importance of links in the network. Thus, the importance of links in terrorist networks remains to a large degree an unexplored issue.

III. LINK IMPORTANCE

As mentioned, current methods of TNA assign high importance to nodes. Role analysis, centrality, and clustering measures focus on positions of nodes in the network. The goal from an intelligence analysis perspective is to come up with informed decisions regarding possible actions to destabilize the network. Carley et al. [16] proposed the following criteria to evaluate if a network has been destabilized:

- The rate of information flow through the network has been seriously reduced, possibly to zero.
- The network, as a decision making body, can no longer reach consensus, or takes much longer to do so.

Information flow in terrorist networks takes place through links and nodes. Node removal is one way to destabilize a network. However, in some cases node removal might not be the best solution. It might be better to keep the suspect under surveillance and disrupt the suspects' communication with other suspects. Therefore, it is important to determine which links are crucial to the network and how removing a particular link would influence the structure in terms of secrecy and efficiency.

A. *Secrecy and Efficiency*

According to Lindelauf et al. [3], secrecy depends on the number of links, the number of nodes, and their degree. The higher the degree of nodes, the lower the secrecy is in the network. Therefore, in order to keep a high level of secrecy in the network, connections between nodes should be sparse and there should be a low level of redundancy of connections.

Lindelauf et al. [3] has also proposed a definition of information performance which in many ways is similar to the definition of efficiency proposed in [10]. Comparing these two methods using the 9/11 network (Figure 1), results in an efficiency of 0.395 (as mentioned in the previous section) and an information performance of 0.342.

Lindelauf et al. [3] also proposed a measure of an overall performance of a network as the product between secrecy and information performance. This measure is used to assess the performance of the network in the light of the goals of terrorist network to reach a balance between secrecy and efficiency.

Looking from the links importance perspective, link removal will in most cases lead to increased secrecy (as a side effect) and to decreased efficiency (which is the goal of destabilization). However, in some cases link removal will not cause changes in network efficiency (if redundant paths of the same length exist). In this case, link removal will only result in increased secrecy (which is not the goal of destabilization).

B. Link Importance in Transportation Networks

TNA has its origin in SNA and uses related metrics. A social network can be referred to as a "pure network" because only its topology and connectivity is considered. If a network is characterized by its topology and flow characteristics (such as capacity constraints, path choice, and link cost functions) it is referred to as a flow network [17]. A flow network is a directed graph where each link has some capacity and can receive a flow – lower than its capacity. A transportation network is a flow network representing the movement of people, vehicles or goods [18].

In terrorist networks, links represent relations between entities; people communicate with each other and the outcome of those relations is information flow. Communication intensity can be the analogy of movement in transportation networks. Some links and nodes will be used more than others in the information flow depending on their position in the structure of a network and also on the source and destination of the information. However, unlike transportation network, the same information can travel at the same time in different parts of network. If we consider a covert network as a special case of a transportation network, where all links have infinite capacities, then measures of transportation networks can be used for TNA.

In transportation networks links are first class objects. A flow between two nodes is dependent on links and their capacity. An illustrative example can be a traffic network. Roads are pictured as links between cities; some roads are heavily used while traffic on others is light. Figure 2 shows an example involving traffic between different parts of Sweden. The thickness of links represents the density of the traffic – the thicker the link, the higher the density. Nodes presented as big circles symbolize major origins/destinations of movement. Relating this example to terrorist networks, "heavy traffic" can be understood as high level of information exchange between nodes, and nodes can be described according to centrality measures.

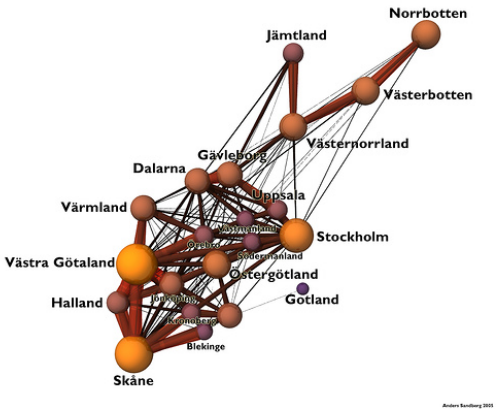

Figure 2. Example transportation network.

Based on transportation network, Jenelius et al. [19] proposed the measure of link importance. It is based on the concept of vulnerability, which in a road traffic context is defined as the susceptibility to incidents that can result in considerable reductions in network capacity during a given period. Bienenstock and Bonacich define vulnerability in the context of SNA as the loss of efficiency resulting from the elimination of nodes [20]. In transportation networks, the focus is placed on what effect the removal of a link will have on functionality. In social networks, the effect of removing a node is considered. However, removing a node from a network has the same effect as removing all the links connecting that node.

In both cases, removal of node or link leads to decrease of network functionality. Looking at Figure 2, it is clear that closing the road between Västra Götaland and Skåne would lead to bigger problems than closing the road between Stockholm and Västernorrland. Therefore the connection between the first two regions is more important than connection between the two others. Based on that assumption, the conclusion can be made that the difference between current performance and performance after link removal can be an indicator of link importance in the network.

In transportation networks, performance is considered as the sum of cost of travel from node i to node k. Based on this, a definition of link importance for transportation networks has been proposed [19] which takes three things into consideration (1) travel demand from node i to node j; (2) the generalized cost of travel from node i to node j in the initial, undamaged network; and (3) the generalized cost of travel from node i to node j when link k is closed.

C. Link Importance in Terrorist Networks

The measure of link importance in terrorist networks is inspired by transportation networks. According to Carley et al.'s [16] proposed criteria to measure network destabilization, we use overall performance (as defined by Lindelauf et al. [3]) to measure how well a terrorist network is functioning. P^0 denotes the initial performance of the network and P^k denotes the performance after removal of link k. Therefore, the performance change when removing link k can be described as:

$$\Delta P_k = P^0 - P^k \quad (1)$$

The goal of link removal in terrorist networks is to lower the performance of the network. Thus, the higher the value of performance change when removing a link, the more important is the link for the network.

The definition of link importance for transportation networks accounted travel demand between nodes as a weight for the performance change. Demand for information flow between two nodes in terrorist network can be expressed by link betweenness. The higher the value of this metrics, the more information travels via the link.

The change in link betweenness when removing link k will be used as a weight for the performance change. The weight is calculated as follows:

$$w(k) = \sum C_b(G) / (\sum C_b(G) - C_b(k)) \qquad (2)$$

Where $\sum C_b(G)$ denotes the sum of link betweenness for all links in the graph G and $C_b(k)$ denotes link betweenness for link k.

This weight will give higher importance to links with higher link betweenness, yet it will still keep performance change as the major factor of link importance. Based on the presented factors, the importance of link k is measure as follows:

$$LI(k) = \Delta P_k * w(k) \qquad (3)$$

The algorithm for calculating link importance consists of the following steps:

1. **Efficiency**. The sum of the shortest paths connecting each pair of nodes is computed. Based on this the efficiency (information performance) of the network is calculated according to the definition by Lindelauf et al. [3].
2. **Secrecy**. The sum of the square degrees of nodes is computed. Based on this and the number of links and nodes, the secrecy of the network is calculated according to the definition by Lindelauf et al. [3].
3. **Performance**. The overall performance of the network is computed as the product of secrecy and efficiency according to the definition by Lindelauf et al. [3].
4. **Weight**. The weight measure for link importance is computed for each link according to equation (2) above.
5. **Link importance**. The link importance for each link is computed according to equation (3) above.

Calculation of link importance results in positive and negative values. A positive value for a link means that after its removal, the performance of the network will decrease (the increase in secrecy will be lower than the decrease in efficiency of the network). A negative value for a link means that the increase of secrecy is higher than the decrease of efficiency – hence the performance of the network is increased.

The link importance measure helps intelligence analysts to understand which links are important for communication in covert networks and how their removal will influence the rest of the network. Naturally, links with high importance should be taken under consideration on order to destabilize the network.

D. Scenario 1: Link Importance in a Small Network

We use a part of the 9/11 terrorist network (Figure 3) as an example to illustrate how link importance works.

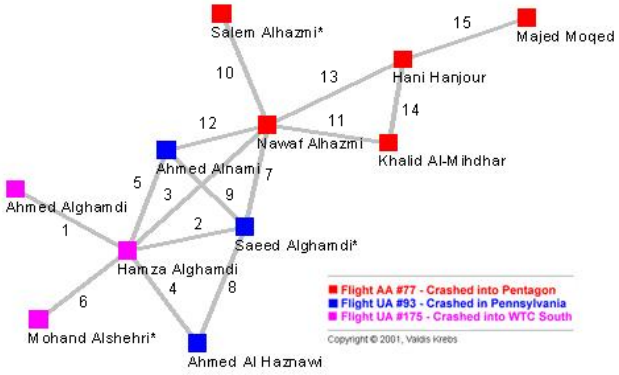

Figure 3. Part of 9/11 network.

The importance of the individual links in the network is shown in Table 2.

TABLE II. LINK IMPORTANCE IN PART OF 9/11 NETWORK.

Link	Link importance	Secrecy	Efficiency
13	0,027759679	0,6060606	0,42307693
3	0,018798648	0,6200466	0,42635658
11	0,009842231	0,6013986	0,45081967
14	0,001790676	0,5874126	0,47413793
12	0,000169219	0,6060606	0,46218488
7	-0,002133225	0,6107226	0,46218488
4	-0,002570151	0,6013986	0,47008547
8	-0,002997429	0,5920746	0,47826087
5	-0,004772992	0,6060606	0,47008547
9	-0,005190209	0,5967366	0,47826087
2	-0,007002236	0,6107226	0,47008547
10	-0,088121056	0,5967366	0,6043956
1	-0,092513749	0,5967366	0,6111111
6	-0,092513749	0,5967366	0,6111111
15	-0,106107757	0,58275056	0,64705884

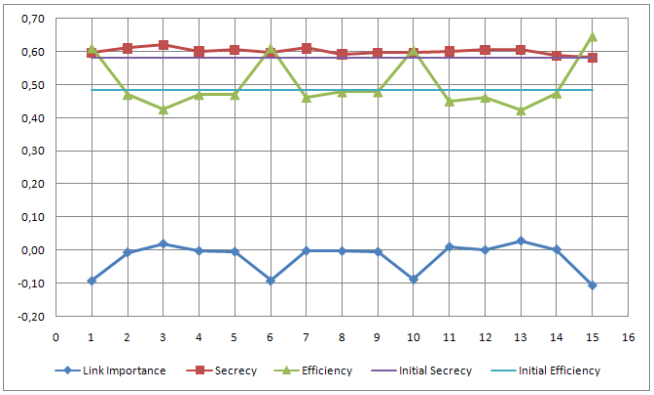

Figure 4. Link importance measures.

The results of link importance are depicted in Figure 4 together with efficiency, secrecy, initial efficiency (before link removal) and initial secrecy (before link removal). Removal of link number 13 results in the highest decrease of efficiency, while the increase of secrecy is insignificant. Hence, link 13 is the most importance link from a network destabilization point of view.

E. Scenario 2: Link Importance in the Full 9/11 Network

The network of 9/11 hijackers and their associates (Figure 1) is a medium sized network consisting of 62 nodes and 153 links. Figure 6 shows the results of link importance by coloring the 10 links with the highest (red) and the 10 links with the lowest importance (blue).

It is visible that the 10 most important links connect the network in a way that no node is further than two steps away from these links. These 10 links connect different segments of the network and maps out the "information backbone" of the network. The 10 links are focused around Atta, Hanjour, and Moussaoui, who were among the five the most important nodes in the network based on calculation of node centralities (as pointed out in Section 2). Therefore, it is not a surprise that the most 10 important links are primarily connecting those nodes indicating the significance of the communication between them. The most important link connects Atta to Khemais, who was the head of the Italian cell of Al-Qaeda.

It is also visible that the 10 least important links are the ones that connect peripheral nodes to the network – except for the link connecting Hanjour and Al-Shehhi. The reason for the latter is the redundancy of links in the core of the network. Hence removal of the particular link does not decrease the efficiency of the network.

F. Evaluation

The algorithm for link importance has been tested on both the 9/11 network (as shown in this paper) and on the 2002 Bali night club bombing network (as described in [21]). The algorithm is implemented in the CrimeFighter Assistant together with various other network, node, and link measures. Figure 5 shows a screenshot of the CrimeFighter Assistant when testing the 2002 Bali night club bombing network (166 nodes and 246 links).

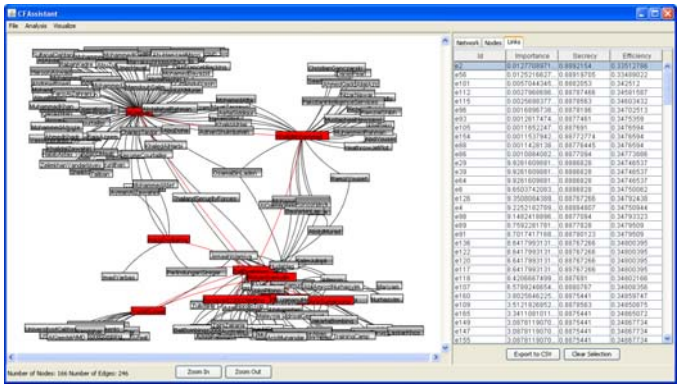

Figure 5. Screenshot of CrimeFighter Assistant.

The network visualization in the left part of CrimeFighter Assistant highlights the 10 most important nodes (according to the PRI measure) and the 10 most important links (according to the link importance measure).

In both cases (9/11 and Bali), the measure of link importance offers new insights into terrorist networks by also focusing on links and the overall network structure. The measure of link importance maps out the information backbone of a terrorist network and can (together with node measures) point to new ways to destabilize the network.

IV. CONCLUSION

This paper has proposed link importance as a new measure for destabilizing terrorist networks. The usefulness of the method was demonstrated based on analysis of the 9/11 and the 2002 Bali bombing networks. The presented work provides the following contributions:

- Description and evaluation of a novel method for measuring link importance in terrorist networks, which is inspired by research on transportation networks. It uses the measures of secrecy and efficiency proposed by Lindelauf et al. [3] together with the measure of link betweenness.
- An implementation of the proposed link importance measure in CrimeFighter Assistant, which to our knowledge also provides the first implementation of the secrecy and efficiency (information performance) measures as proposed by Lindelauf et al. [3].

Future work will further investigate, evaluate, and improve the measure of link importance. We are currently looking into how link weights can be incorporated, since not all links are equally important. We believe that incorporation of link weights will result in a more precise measure of link importance.

REFERENCES

[1] M. Baccara and H. Bar-Isaac, "Interrogation methods and terror networks," Mathematical Methods in Counterterrorism, 2009, pp. 271-290. Springer.

[2] R. Lindelauf, P. Borm, and H. Hamers, "On heterogeneous covert networks, "Mathematical Methods in Counterterrorism, 2009, pp. 215-228. Springer.

[3] R. Lindelauf, P. Borm, and H. Hamers, "The influence of secrecy on the communication structure of covert networks," Social Networks, 31 (2009), 126-137. Elsevier.

[4] U. K. Wiil, N. Memon, and J. Gniadek, "Knowledge management processes, tools and techniques for counterterrorism," Proceedings of the International Conference on Knowledge Management and Information Sharing, (Funchal, Portugal, October 2009), pp. 29-36. INSTICC Press.

[5] S. Wasserman and K. Faust, "Social network analysis: methods and applications", 1994. Cambridge University Press.

[6] N. Memon, U. K. Wiil, R. Alhajj, C. Atzenbeck, and N. Harkiolakis, "Harvesting covert networks: the case study of the iMiner database," International Journal of Networking and Virtual Organizations, 2010. Inderscience Publishers.

[7] P. A. Gloor and Y. Zhao, "Analyzing actors and their discussion topics by semantic social network analysis," Information Visualization, 2006, pp. 130-135.

[8] V. E. Krebs, “Uncloaking terrorist networks,” First Monday, 7(4-1), 2002.

[9] W. Enders and X. Su, “Rational terrorists and optimal network structure,” Journal of Conflict Resolution, 51(1):33, 2007.

[10] V. Latora and M. Marchiori, “How the science of complex networks can help developing strategies against terrorism,” Chaos, Solitons and Fractals, 20(1):69-75, 2004.

[11] W.E. Baker and R.R. Faulkner, “The social organization of conspiracy: illegal networks in the heavy electrical equipment industry,” American Sociological Review, 837-860, 1993.

[12] N. Memon, “Investigative data mining: mathematical models for analyzing, visualizing and destabilizing terrorist networks,” PhD thesis, 2007. Aalborg University, Denmark.

[13] C. J. Rhodes, “Inference approaches to constructing covert social network topologies,” Mathematical Methods in Counterterrorism, 2009, pp. 127-140. Springer.

[14] M. Girvan and M. E. J. Newman, “Community structure in social and biological networks,” Proceedings of the National Academy of Sciences, 99(12):7821-7826, 2002.

[15] M. E. J. Newman, “A measure of betweenness centrality based on random walks,” Social networks, 27(1):39-54, 2005.

[16] K. M. Carley, J. S. Lee, and D. Krackhardt, “Destabilizing networks,” Connections, 24(3):31-34, 2001.

[17] M. M. Fischer and R. Lände, “GIS and network analysis,” Handbook of transport geography and spatial systems, 5:391-408, 2004.

[18] M. G. H. Bell and Y. Iida, “Transportation network analysis,”, 1997. Wiley.

[19] E. Jenelius, T. Petersen, and L. G. Mattsson, “Importance and exposure in road network vulnerability analysis,” Transportation Research Part A, 40(7):537-560, 2006.

[20] E. J. Bienenstock and P. Bonacich, “Balancing efficiency and vulnerability in social networks,” Dynamic social network modeling and analysis: Workshop summary and papers, pp. 253-264, 2003. The National Academies Press.

[21] J. Gniadek, “Destabilizing terrorist networks through link importance analysis”, Masters Thesis, Counterterrorism Research Lab, The Maersk Mc-Kinney Moller Institute, University of Southern Denmark, 2010.

Figure 6. Link importance in the 9/11 network.