Influence of Key Player Detection and Removal on Efficiency and Performance of Covert Networks using Social Network Analysis

Aisha Zafar Ahmad, Anam Shahjahan
Department of Computer Engineering
National University of Sciences and Technology
Islamabad, Pakistan
aisha12@ce.ceme.edu.pk, anamshahjahan@hotmail.com

Wasi Haider Butt, Usman Qamar
Department of Computer Engineering
National University of Sciences and Technology
Islamabad, Pakistan
wasi@ce.ceme.edu.pk, usmanq@ceme.edu.pk

***Abstract*—Terrorist network is particular type of social network with prominence on efficiency and performance. In order to propose successful approaches for terrorist organizations destabilization, identification and understanding of structural properties of network is essential. This paper presents a brief survey of centrality measures from social network analysis using optimizing standards to those based on information performance, efficiency and overall performance**

Keywords— Terrorist networks; Social network analysis; centrality measures; efficiency; performance.

I. INTRODUCTION

Social network is socially organized consisting of a person, a group of person or organizations and specifies relationships such as kinship, friendship between them. Using SNA the interrelationships are normally represented as a graph, consisting of nodes that correspond to social actors and edges correspond to the ties/links [1].

The SNA technique involves detection and interpretation of behavioral patterns and hidden structures among ties and actors within social networks [2].

Terrorist network is a dynamic, versatile, vaguely delineated structure composed of number of interconnected and interrelated person, linked independently and on an aggregate level to pursue a common interest [3]. Terrorist networks are deliberately constructed to assure efficient communication among the members without being detected [4-6]. It is a particular form of social network where efficiency and information performance are most emphasized measures. To investigate terrorism and to develop effective plans for prevention of terrorist attacks, it is important to have knowledge about the organization and construction of terrorist networks. [7]

Covert networks are conceived as terrorist networks. Covertness is a major difference between a regular network and terrorist network. [7]. Covert networks are illegal networks that operate outside the boundary of law. Achievement cost of covert networks comes from other individuals, groups or societies [8], [9]. Communication content in covert networks is kept secret and the ties among the members are kept strong having high level of trust. Law enforcement departments use SNA to analyze terrorist networks [10]. For analysis of terrorist network, first the terrorist network is discovered and then detected.

A terrorist network can be viewed as a social network. As in social network we have nodes and edges, nodes corresponding to actors and links corresponding to relationships among the actors. In the similar way terrorist network consists of persons as nodes and relationships/links among the person. Relationship can be of communication, kinship, attendance/training at same school etc. So, terrorist network can be viewed as a social network.

SNA offers a set of illustrative measures that help in investigating terrorist networks. [11] SNA techniques are applicable for studying terrorist networks, as they define social structures of network. Centrality measures from SNA applied in order to measure the importance of each node in the network. Analysis of each and every node in network is performed and centrality measures for each node are calculated correspondingly.

Every terrorist organization ensures being efficient in terms of performance, coordination and communication between its members without being detected. Discovery of single or set of key players using Social network analysis centrality measures is done in literature for terrorist networks.

This research focuses on terrorist/covert networks, as terrorist/covert networks tend to perform and work efficiently without being detected. Network level measures efficiency, information performance and overall performance for the whole network are used. Terrorist networks have the property of being efficient when it comes to communication of information within network. Goal is to use node level measures and then remove set of key nodes that would result in drop of network efficiency and performance. We will prove how efficiency and performance of network can be minimized using SNA measures.

II. RELATED WORK

The very first attempt to analyze terrorist networks using essentials of SNA was done by Valdis Krebs [12] in 2002. The

study used network analysis to map 9/11 hijackers network. Krebs during his study followed conventional SNA methods in a graph. He evaluated relations/ties in the network on the basis of strength as strongest, moderate and weak ties. He used different thickness in ties between nodes to signify strength of relationship. Krebs then provided with the analysis of his research using standards of SNA, the centrality measures which evaluated the participation of each node in attacks. This was helpful for law enforcement departments in order to detect terrorist networks effectively. Krebs argued that this development traded efficiency for secrecy. Krebs in his study provided the most profound SNA of terrorist organizations to date.

Carley et al. [13] in their study introduced current development tools in SNA. Tools comprised of network measures i.e., centrality measures and UCINET as statistical analysis program. Study also mentioned some difficulties faced in research of network destabilization, mostly difficulties were in nature of networked organization, distributed knowledge and resources and changing network structure. Carley et al asserts that difficulties can be overwhelmed by enhancing and improving current tools, one of which was expanding SNA to DNA. Their paper partially implemented the suggested improvements.

Framework for destabilization of terrorist networks has been proposed by Carley et al. [14]. Their study mentioned limitations of static SNA which are applied for identification and destabilization of covert networks. Solution proposed for this limitation was DNA, in which adding/dropping of nodes have been taken into account. Paper also defines the process of adding and dropping key entities. They also proposed strategy for destabilization of terrorist network. The study recommends that the proposed strategy is to be applied after having knowledge of entire network.

According to Carley [15] whenever a network is damaged links and nodes got missed. The remaining nodes are efficient enough to interact with each other and create an alternate way to communicate. Single isolation does affect the network performance, but it is not significant to break the network. Thus multiple isolations must be carried out in order to maximize the effect of destabilization.

In study of Jennifer [16] existing criminal network analysis tools and approaches were categorized for identification of subgroups, finding key players, discovering patterns of interaction and revealing the organizational structure.

Resseler [17] provided an overview of SNA research in counter terrorism. His study focused on several defense, academic and government activities for collection of data and terrorist network modelling.

Investigative data mining toolkit framework was introduced by Nasrullah Memon and Henrik Legind Larsen [3]. Their suggested techniques and algorithms to construct command structure of networks, have been implemented on past case studies of terrorist attacks including 9/11, Bali Bombing, WTC 1993 bombing and Khobar Tower Bombing.

For destabilization of terrorist networks two highly beneficial algorithms were proposed in 2006, by Nasrullah Memon and Henrik Legind Larsen [18]. Their study about terrorist networks turned out several possible solutions for detection of terrorist networks more efficiently. To achieve destabilization in a promising manner, hierarchy of algorithms were suggested which were based on approaches of SNA along with the measures. New centrality measure dependence centrality was introduced, which defines dependence of every node with each other nodes.

Taking case study of 9/11 Nasrullah Memon et al. [19] presented the detection of crucial parts in terrorist networks. Structural cohesion study is presented, which was used only for traditional SNA. They said structural cohesion can also be used for several other areas of applications like IDM for destabilization of terrorist networks. Structural cohesion is defined as disconnection of network after removing several nodes. Several concepts of structural cohesion are also discussed namely cliques, n-clique, n-clan and k-plex to conclude robustness, familiarity and reachability within subgroups of 9/11 networks. They also suggested a strategy for detecting critical domains in terrorist networks, removal of those nodes will result in network disruption.

Nasrullah Memon and David L. Hicks in their study of terrorist networks [20], introduced IDM technique and applied it to terrorist networks in order to detect high value of individuals. The presented approach was applied to the case study of 7/7 London Bombing.

Everton [21] proposed that before defining the strategies for disruption of social network using centrality measures form SNA in order to discover of key players, the whole topography of network must be considered for effective computation of potency of terrorist networks. The size of network, number of attacks and network resilience must be taken into account.

In order to notice the variations over time in structure and effectiveness of network, Everton [22] analyzed and constructed the Noordin's top terrorist network from 2001-2010. This study proposed that terrorist groups which are dense but decentralize are most effective and are most difficult to disrupt.

Karthika [23] examined and compared previous work done in domain of SNA for terrorist networks. Her work categorized several approaches of SNA as destabilizing terrorist networks, DNA, discovering key players and detecting subgroups etc.

III. ANALYSIS OF SNA TECHNIQUES TO DESTABLIZE TERRORIST NETWORKS

The SNA technique involves detection and interpretation of behavioral patterns and hidden structures among ties and actors within social networks [2].

SNA techniques can be implemented on actors in social groups to key out actors with central roles, who are apart, or

actors who have highest degree of relations etc. Information propagation in the network can be improved or even stopped by using this information

Many studies in SNA have come out with variety of measures to analyze the communication patterns and structure of social network. Centrality is one of the most important measures. Centrality relates to position of the actor in context social network [24]. Applications of centrality in other research works are as, analyzing structure and patterns of terrorist networks, analyzing the opportunities of employment, to investigate effect of patterns in networks, etc. [25].

Centrality measures assist in identification of key person in the network. Several measures of centrality are defined which indicate importance of a node. Major centrality measures used in SNA are degree, closeness and betweenness to look at importance of a node.

A. *Node Level Measures*

Degree Centrality

Degree [26] of a node is measured as number of direct connections to a node. Node with high degree value is an important entity in the network.

Mathematically,

$$C_D(i) = \sum_{j=1}^{N} A_{ij} \tag{1}$$

In terrorist networks, degree centrality assists in identifying number of nodes who can reach directly from a particular node. It is not necessary that node with highest degree value is the leader of network.

Betweenness Centrality

Betweenness [26] of a node is measured to what extent a specific node lies between other nodes in the network. All nodes in the network are not connected directly to each other; a path from a node to another node may pass through one or more intermediate nodes within network. Betweenness centrality is measured as rate of occurrence of node on geodesic connecting other pair of nodes.

Mathematically,

$$C_B(i) = \sum_{j<k} g_{jk}(i) \Big/ g_{jk} \tag{2}$$

Where $g_{jk}(i)$ is the number of shortest paths connecting jk passing through I, and g_{jk} is total number of shortest paths

In terrorist networks, betweenness centrality assists in finding a node that contain maximum of information (broker) between two groups in the network.

Closeness Centrality

Closeness [26] of a node is measured to how quick one can reach from a node to all other nodes in the network. A node is central when it has quick and easy access to all other nodes in the network. In terrorist networks, closeness centrality assists in identifying a node that can quickly access all other nodes in the network.

Mathematically,

$$C_C(i) = \sum_{j=1}^{N} d(i,j) \tag{3}$$

In terrorist networks, closeness centrality assists in identifying a node that can quickly access all other nodes.

B. *Network Level Measures*

Efficiency

Efficiency E(G) of network is a measure [6] to quantify how efficiently exchange of information takes place between the nodes of the network.

Mathematically [6]

$$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}} \tag{4}$$

Where, N represents number of nodes in the graph. Value of E is normalized for this equation and lies between intervals of [0, 1]. The efficiency E has been calculated for many real networks.

Information Performance

Performance of network in context of information is defined by multiplicative inverse of total distance. Lindelauf et al presented a definition of information performance [27] which is close to efficiency definition proposed in [6]. In terrorist networks if information flows through number of nodes chances of interception of information are likely to be more.

Mathematically Information Performance $I(g)$, is formulized as [27]

$$I(g) = \frac{n(n-1)}{T(g)} \tag{5}$$

Where, n represents the number of nodes and $T(g)$ is the total distance.

As $T(g) \geq n(n-1)$ for any network $g \in G$ follows that $0 \leq I(g) \leq 1$.

If each node in network communicates with every node else in the network, information will move freely which will result in the best information performance that is $I(g) = 1$.

Overall Performance

Overall performance measure was proposed by Lindelauf et al. as mathematical product between information performance and secrecy [27].

Mathematically overall performance is formulized as

$$\mu(g) = I(g)S(g) \tag{6}$$

IV. Detecting and Removing Set of Key Players from Terrorist Networks

A. *Noordin Top Terrorist Network*

Communication network connecting the terrorists of Noordin's terrorist network was considered. The data was drawn from a 2006 publication of International Crises Group "Terrorism in Indonesia Noordin's Networks" [28]. The network consisted of 79 individuals, N=79. We looked at communication network of Noordin's network; communication is specified as transfer of messages among individuals or groups within the network through some sort of medium. Noordin's network was related to number of operations like Atrium Mall Bombing, Bali Bombing, Marriot Bombing, etc. Mapping of network after an event or operation is comparatively easy, where as it is much more difficult and it is a real big problem to map the terrorist/covert networks that would help in prevention of criminal activity or terrorist attacks.

The Noordin's terrorist network comprised of 79 nodes representing the terrorists and their followers, followers interact with the terrorists directly or indirectly through 200 links among them. To individuate the set of key nodes that is, the nodes which were responsible for the key roles in the network, those nodes were deactivated in form of pairs. Deactivation is done on the basis of centrality measures. First the efficiency, information performance and overall performance of whole network are computed. On node basis centrality measure of each node is calculated. Pair of nodes with higher values of centrality is deactivated. Each time the pair of nodes is deactivated drop in efficiency, information performance and overall performance in network is noticed.

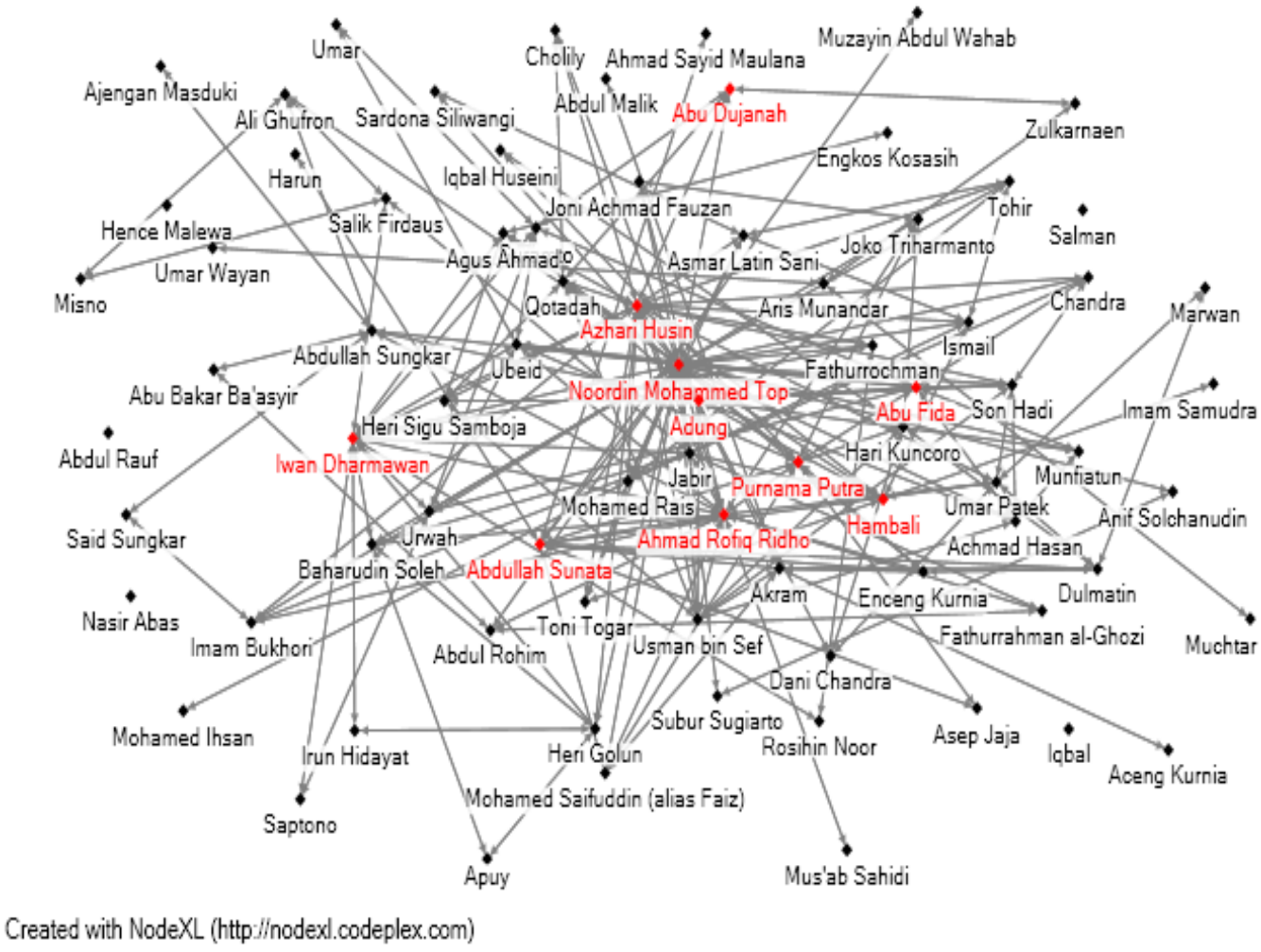

Fig. 1. *Noordin Mohammad Terrorist Network*

The results reported in the table.1 indicate that according to degree centrality Noordin Mohammad and Azhari Husin are the two key nodes/person their deactivation drops more than 23% of efficiency, 25% of information performance and 18% Overall performance of the whole network. In similar way by deactivating additional pair of nodes with key nodes causes drop in efficiency by 42%, drop in information performance by 52% and drop in overall performance by 50% of whole network.

TABLE I. EFFECT OF DEACTIVATING PAIR OF NODES IN NOORDIN MOHAMMAD TERRORIST NETWORK ACCORDING TO DEGREE CENTRALITY

Nodes Removed	C_D	E(G)	I(G)	μ(g)
-	-	0.429	0.369	0.336
Noordin Mohammad Azhari Husin	41 22	0.329	0.298	0.276
Ahmad Rofiq Ridho Iwan Dharmwan	17 13	0.304	0.238	0.222
Abdullah Sunata Purnama Putra	10 9	0.298	0.235	0.218
Adung Abu Fida	9 8	0.250	0.180	0.168

Removed pair of nodes are listed in first column, degree of the removed nodes is listed in second column, original network efficiency is E(G) is 0.429, drop in efficiency deactivating pair of nodes is reported in third column, information performance of original network is 0.369, drop in information performance is reported in fourth column, overall performance of network is 0.336 and drop in overall performance of network is reported in last column.

Graphically the drop in efficiency, information performance and overall performance can be viewed in fig.2.

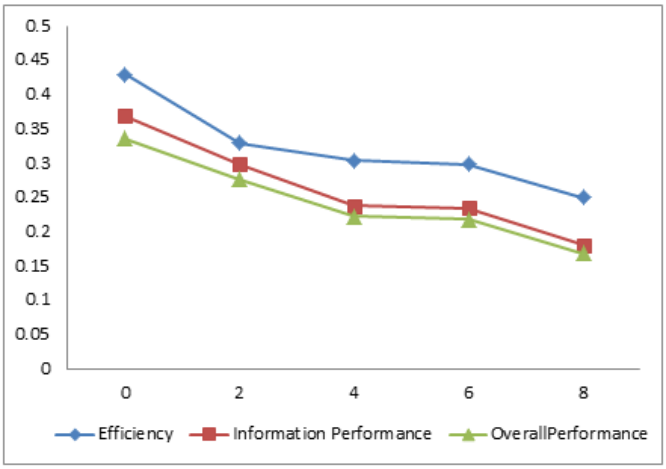

Fig. 2. *Graph representing drop in efficiency, information performance and overall performance removing set of nodes according to degree centrality.*

According to betweenness centrality when four pairs of key nodes were deactivated drop in efficiency by 32%, drop in information performance by 40% and drop in overall performance by 39% was noticed. Nodes along with their names and values of betweennes centrality are listed below in table.2.

TABLE II. EFFECT OF DEACTIVATING PAIR OF NODES IN NOORDIN MOHAMMAD TERRORIST NETWORK ACCORDING TO BETWEENNESS CENTRALITY

Nodes Removed	C_D	E(G)	I(G)	μ(g)
-		0.429	0.369	0.336
Noordin Mohammad Abu Dujanah	1452.54 285.611	0.402	0.347	0.317
Ahmad Rofiq Ridho Azhari husin	737.146 693.197	0.334	0.269	0.243
Adung Hambali	559.041 467.124	0.324	0.260	0.237
Iwan Dharmawm Purnama Putra	523.089 403.363	0.298	0.223	0.205

Graphically the drop in efficiency, information performance and overall performance according to betweenness centrality can be viewed in fig.3.

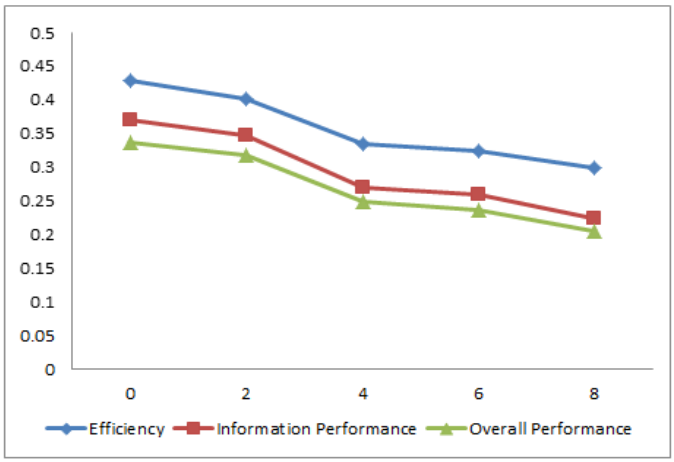

Fig. 3. *Graph representing drop in efficiency, information performance and overall performance removing set of nodes according to betweenness centrality.*

In the similar way according to closeness centrality deactivating three pair of nodes results in drop of efficiency, information performance and overall performance by by 39%, 50% and 50% of the whole network.

TABLE III. EFFECT OF DEACTIVATING PAIR OF NODES IN NOORDIN MOHAMMAD TERRORIST NETWORK ACCORDING TO CLOSENESS CENTRALITY

Nodes Removed	**C_D**	**E(G)**	**I(G)**	**μ(g)**
-		0.429	0.369	0.336
Noordin Mohammad Azhari Husin	0.009 0.007	0.329	0.298	0.336
Ahmad Rofiq Ridho Iwan Dharmwan	0.006 0.006	0.304	0.238	0.276
Adung Abu Fida	0.006 0.005	0.260	0.188	0.17

Results after removing pair of key nodes are listed in table.3.

Graphically the drop in efficiency, information performance and overall performance according to closeness centrality can be viewed in fig.4.

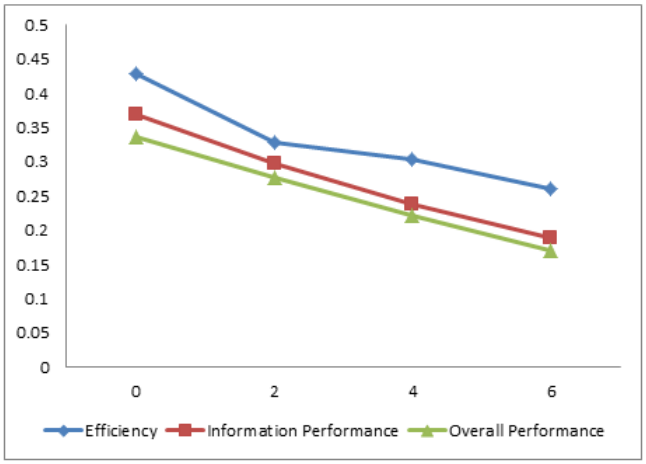

Fig. 4. *Graph representing drop in efficiency, information performance and overall performance removing set of nodes according to closeness centrality*

It was analyzed that by removing pair of nodes according to centrality measures the network efficiency, information performance and overall performance of the network was affected. As terrorist networks tend to be efficient in terms of performance and information propagation, by removal of 15% to 20% of the nodes their efficiency, information propagation and performance will be disturbed. So, having partial knowledge about terrorist networks and individuating key nodes from the network would help in disruption of terrorist network and prevention of criminal activity.

V. Conclusion

In this paper critical nodes of the network were identified whose removal causes a drop in efficiency and performance. Critical nodes are the nodes that are responsible for their efficient functions in terms of performance and efficiency. Application of the work is to find critical nodes from a communication network in order to protect from attacks, and to find the set of key nodes to target them that would result in disruption of a covert/terrorist network.

References

[1] Scott, J.: Social Network Analysis: A Handbook, 2 edn. Sage Publications, London 2000.

[2] de Nooy, Wouter, Andrej Mrvar, and Vladimir Batagelj. 2005. *Exploratory Social Network Analysis with Pajek*, *Structural Analysis in the Social Sciences*. Cambridge, UK: Cambridge University Press.

[3] N.MemonandH.L.Larsen, "Investigative data mining toolkit: A software prototype for visualizing,analyzing and destabilizing terrorist networks," *Visualising Network Information*, 2006,pp. 14-1–14-24.

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

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

[6] 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

[7] Uffe Kock wiil, Jolanta Gniadek, Nasrullah Memon, Measuring link Importance in Terrorist Networks, Internaional Conference on Advances in Network Analysis and Mining,2010

[8] H.B. Milward, J. Raab, Int. Public Manag. J. 9, 333 (2006)

[9] R.M. Bakker, J. Raab, H. Brinton Milward, J. Policy Anal. Manag. 31, 33 (2012)

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

[11] Muhammad Akram Shaikh, Wang Jiaxin: Investigative Data Mining: Identifying Key Nodes in Terrorist Networks, Multitopic Conference, 2006. INMIC '06, pp. 201-207 IEEE IEEE (2006).

[12] V. E. Krebs, (2002), "Uncloacking Terrorist Networks". First Monday, Volume 7, 4 - 1 (2002)

[13] K. M. Carley, J. S. Lee and D. Krackhardt (2001) Destabilizing Networks.Connections, Vol 24(3), pp 31-44.

[14] K.M. Carley,J.Reminga, and N.Kamneva, "Destabilizing terrorist networks," in *Proc.NAACSOS Conference*, 2003.

[15] K. M. Carley (2003), Dynamic Network Analysis, Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, Eds. Ronald Breiger, Kathleen Carley, and Philippa Pattison, Committee on Human Factors, National Research Council, National Research Council, pp 133-145

[16] Xu, Jennifer, and Hsinchun Chen, (2005) "Criminal network analysis and visualization", Communications of the ACM, Vol. 48, No.6, pp100-107.

[17] Ressler, Steve, (2006) "Social network analysis as an approach to combat terrorism: past, present, and future research", Homeland Security Affairs, Vol. 2, No.2, pp1-10.

[18] N. Memon and H. L. Larsen, (2006), "Practical Approaches for Analysis, Visualization and Destabilizing Terrorist Networks", Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE 2006.

[19] N. Memon, K. C. Kristoffersen, D. L. Hicks, and H. L. Larsen, "Detecting critical regions in covert networks: A case study of 9/11 terrorists network," *The Second International Conference on Availability, Reliability and Security*, 2007, pp. 861-870.

[20] N. Memon and D. L. Hicks, "Detecting key players in 11-M terrorist network: A case study," Presented at Third International Conference on Availability, Reliability and Security, 2008.

[21] Everton, Sean F., (2009) "Network topography, key players and terrorist networks" Annual Conference of the Association for the Study of Economics, Religion and Culture, Washington, DC.

[22] Everton, Sean F., Cunningham and Dan, (2011) "Terrorist Network Adaptation to a Changing Environment".

[23] Karthika, S., and S. Bose, (2011) "A comparative study of social networking approaches in identifying the covert nodes", International Journal on Web Services Computing (IJWSC), Vol. 2, pp65-78.

[24] Friedkin NE (1991) Theoretical foundations for centrality measures. Am J Sociol 96(6):1478–1504

[25] Borgatti SP, Everett MG (2006) A graph-theoretic framework for classifying centrality measures. Social Networks 28(4):466–484

[26] Freeman, Linton C., (1979) "Centrality in social networks conceptual clarification", Social networks, Vol. 1, No. 3, pp215-239.

[27] 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.

[28] Roberts, Nancy and Sean F. Everton. 2011. *Roberts and Everton Terrorist Data: Noordin Top Terrorist Network (Subset)*. [Machine-readable data file]