

A COMPARATIVE STUDY OF SOCIAL NETWORKING APPROACHES IN IDENTIFYING THE COVERT NODES

Karthika S¹ and Bose S²

1 Teaching Fellow 2 Assistant Professor
Department of Computer Science and Engineering
College of Engineering Guindy, Anna University, Chennai-600096
sk_mailid@yahoo.com
sbs@cs.annauniv.edu

ABSTRACT

This paper categories and compares various works done in the field of social networking for covert networks. It uses criminal network analysis to categorize various approaches in social engineering like dynamic network analysis, destabilizing covert networks, counter terrorism, key player, subgroup detection and homeland security. The terrorist network has been taken for study because of its network of individuals who spread from continents to continents and have an effective influence of their ideology throughout the globe. It also presents various metrics based on which the centrality of nodes in the graphs could be identified and it's illustrated based on a synthetic dataset for 9/11 attack. This paper will also discuss various open problems in this area.

KEYWORDS

Criminal Network Analysis (CNA), Social Network Analysis (SNA), Terrorist Network.

1. INTRODUCTION

The modern-day field of terrorism is experiencing tremendous growth highly motivated by the so called “net war”, a lower-intensity battle by terrorists, criminals, and extremists with a networked organizational structure [1]. The Dark Network brings to our realization that there is a set of individuals and organizations that constitute a network striving to achieve ends for governments all over the world. Such organizations are collectivity comprised of and maintained by individuals. These individuals may leave, die, or change their mindset, but still the organization can last. Remaining members can take up the roles of lost nodes, new recruits can be added and the structure can be enlarged or rearranged.

Due to the new evolving trends of security problems, a new type of intelligence is needed which is called as Social Network Analysis (SNA). The basis of social network analysis is that individual nodes are connected by complex yet understandable relationships that form networks. These networks are said to be pervasive in nature with their own law and orders framed [2]. But a drawback with SNA is that it cannot be considered as an appropriate data mining technique because it can discover the patterns from the known structure and not from hidden structure like a

terrorist network where the nodes are embedded in a large population. Hence the knowledge discovery process to isolate overt cell from covert cell uses the crime data mining technique and the hidden network is analyzed using Criminal Network Analysis (CNA).

This paper has mainly two objectives namely (i) Categorizing various approaches using CNA for studying the covert networks and providing brief details of the various types of analysis and units of analysis on which the network is understood (ii) It also elaborates on the various centrality metrics like closeness, betweenness, point, dependency etc. on the basis of a synthetic dataset of 9/11 attack using ORA tool.

The rest of the paper is structured as follows: Section 2 presents a detailed classification of various problems in criminal network analysis, Section 3 presents different centrality aspects in network mining, and Section 4 outlines the future directions of social network analysis in covert networks. Finally, Section 5 concludes the paper with a summary.

2. SOCIAL ENGINEERING APPROACHES FOR COVERT NETWORKS

In this section the paper presents the taxonomy of CNA methods for terrorist networks which is depicted in Figure 1.

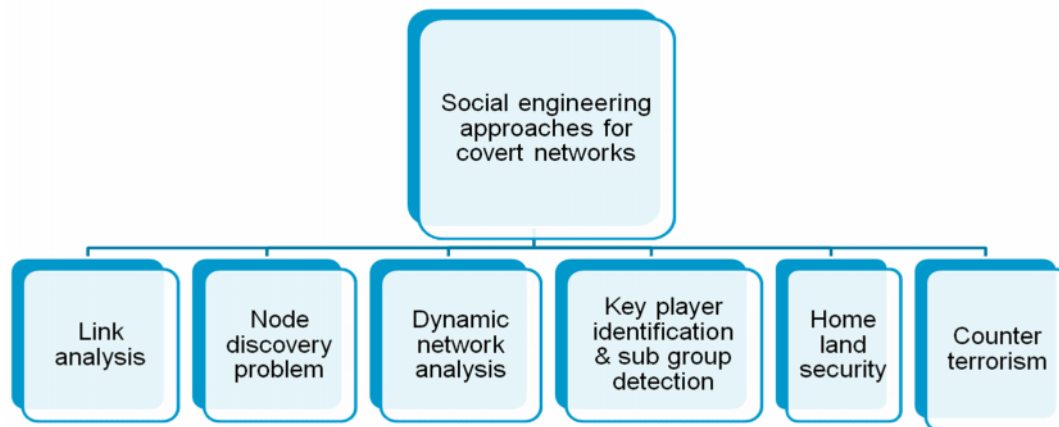


Figure 1. Taxonomy of various criminal network analysis techniques

2.1 LINK ANALYSIS

CNA requires the ability to integrate information from multiple crime incidents where the relationships between crime entities are recognized using link analysis [5].

Jennifer Schroeder, Jennifer Jie Xu, Hsinchun Chen and Michael Chau [5] establish association path linking using heuristic methods in knowledge engineering which builds up a knowledge base that results in an inference engine. This paper implements a system called as Crime Link Explorer based on a set of structured crime incidents from Tuscan police department. The system has proved that the heuristic weights helps to mirror human judgment more precisely by using the

domain knowledge of the crime investigators involved rather than the simple co-occurrence weight which just considers the incidental relations for determining the weight.

Robert D. Duval, Kyle Christensen, Arian Spahiuz [6] in their work have discussed about the problems allied to missing data and the resulting errors like node deletion, node addition, edge deletion and edge addition. The authors prefer to use the bootstrapping methodology which treats the existing network as a sample, and then obtains a resample from the network. The purpose of resample network is to reduce the size of the network and increases the density. But the problem in this methodology is that the removed link can belong to a more heavily connected nodes which reduce the total path distances to be counted, and result in decreased centrality. This method is being implemented for Jemaah Islamiyah network collected by Stuart Koschade and 9/11 hijacker network collected by Valdis Krebs [31].

Christopher C. Yang and Tobun D. Ng [7] discuss the challenges in analyzing relationships present inside the semantics of bloggers' messages because weblog social network doesn't use page ranking or indexing methods. The authors have developed a crawler called as Dark web which does link and content analysis to extract the web log sub-community. It has been experimented for terrorist network to discover the threat levels based on the activeness of interaction within the community and content development.

Jennifer Jie Xu and Hsinchun Chen [8] improve the efficiency of the existing link analysis software by providing a visual representation of a criminal network and also uses shortest path algorithm to quickly complete the analysis task. The data set is got from Phoenix police department from which the paths identified are meaningful 80% of the time and provides a perfect solution to the problem of identifying the strongest criminal associations between two or more entities.

Boongoen, T., Q. Shen, and C. Price [9] propose an unsupervised hybrid model- Connected-path to detect a false identity problem that uses link analysis and text based measures in which multiple link properties are used to refine the process of similarity estimation. Unlike the existing model which needs prior linguistic knowledge, this proposed model is language-independent and knowledge-free, and so can be easily adapted to new problem domains. For demonstrating this technique a data set has been constructed with 919 real alias pair from terrorist related web pages and news stories.

2.2 NODE DISCOVERY PROBLEM

Criminal network analysis other main objective is analyzing the covert networks to solve the node discovery problem.

Yoshiharu Maeno and Yukio Ohsawa [10] uses the clustering and ranking procedure along with the expert investigator's earlier understanding to evaluate the activeness of communication and calculates possibility of the suspicious inter-cluster relationships due to covert nodes between the clusters. It generates a latent structure if the above process is done iteratively. This technique helps to reveal the 18 hijackers of 9/11 attack and also the covert conspirators in the network.

Yoshiharu Maeno [11] present two methods to solve the node discovery problem. First method is a heuristic method in which closeness measure is determined using Jaccard's co-efficient and the other is k-medoids which is applied for classification of nodes. Along with these, the ranking algorithm is also used to recover the suspicious surveillance logs. The second method is statistical inference method that uses the maximal likelihood estimation to figure out the topology of the network, and applies an anomaly detection technique to retrieve the suspicious surveillance logs.

The author uses a computationally synthesized network and global mujahedeen organization to generate the test dataset for which the performance evaluation is done.

Nasrullah Memon and Henrik Legind Larsen [4] have developed a prototype called *iMiner* that incorporates several advanced techniques like automatically detecting cells from a network, identifying various roles in a network using newly developed dependence centrality along with the existing ones like degree centrality and eigenvector centrality which also develops a hierarchy of terrorist network, provides facilities for retrieval of information and its presentation in a graph form, enable small sub graphs to be retrieved and add them to the repositories and may also assist law enforcement about the effect on the network after capturing or killing a terrorist in a network.

Matthew J. Dombroski and Kathleen M. Carley [12] discuss about how the terrorist network structure of 9/11 is estimated, determine the “what if” scenarios to destabilize a network and predict its evolution over time using a tool called NETEST. This tool uses the multiagent technology with hierarchical Bayesian inference models that helps to generate a network structure with information that are accurate and it also includes the biased net models to examine and capture the biases that may exist in a specific network or set of networks.

Christopher E. Hutchins and Marge Benham-Hutchins [13] in this paper show how SNA tools like ORA & Automap process the information and reduce the time taken for investigation by studying the person-to-person relationship and means for the criminal network in a dynamic environment. The author conducts the study on three networks which uses the data sets from HIDTASIS, analyzing phone calls based on drug investigation and multimodal network of agents, resources, locations, events and roles.

Matthew Dombroski, Paul Fischbeck and Kathleen M. Carley [14] discuss the possibilities of using the inherent structures observed in social networks to make predictions of networks using limited and missing information. The model is based on empirical network data exhibiting the structural properties of triad closure and adjacency.

S. Appavu , R. Rajaram, M. Muthupandian, G. Athiappan, K.S. Kashmeera [15] propose a decision tree based classification method to analyze the network by detecting e-mails that contain terrorism information. The proposed classification method is an incremental and user-feedback decision tree induction algorithm named Ad Infinitum which uses a supervised learning technique with a set of labeled training example that builds a classifier with which we can predict the category of an unseen incoming e-mail.

2.3 DYNAMIC NETWORK ANALYSIS

Traditional analysis approaches, such as Social Network Analysis (SNA) and link analysis are limited in their ability to handle multiplex, multimode, large scale dynamic data that are needed to characterize terrorist networks. Hence to solve this problem a modern technique called as Dynamic network analysis (DNA) is introduced which not only supports the collection, analysis and understanding of the network but also predicts the dynamic relationship and the impact of such dynamics on individual and group behavior.

Kathleen M. Carley [16] discuss about the integrated CASOS dynamic network analysis toolkit which is a collection of scalable software tools for coding, analyzing and forecasting behavior for a given relational or “network” data. These tools form a tool chain that enables analysts to move from raw texts to meta-networks for identifying the patterns in networks. This toolset contains the following tools: AutoMap is a semi-automated Network Texts Analysis (NTA) that extracts networks from texts using the distance based approach called windowing, ORA for analyzing the

extracted networks having meta-matrix data and generates report that identifies key players and can also compare two different networks, and DyNet that is built over a Construct Simulation Engine for what-if reasoning about the networks. These tools were tested by collecting thousands of open source documents about terrorism and it's being processed by Automap that constructs the database from which particular entities are studied and the resultant data are processed using ORA.

Ian A. McCulloh and Kathleen M. Carley [17] discuss about social network change detection using statistical process control chart that detects when significant changes occur in the network and from the chart the various centrality factors are calculated for several consecutive time periods. The suspected time period when a change has occurred is studied using CUSUM statistics and in depth time period is considered for understanding the degree of change.

Kathleen M. Carley [18] proposes an approach to estimate vulnerabilities and the impact of eliminating those vulnerabilities in covert networks. Key features of this work include: using detailed network data to help organizations to create a combined image using network metrics and using multiagent simulation to predict change in the already determined network view over time. Uncertainty is managed by running the model in a Monte-Carlo fashion to determine the robustness of the results and examining the result by adding and dropping nodes and edges in the underlying networks.

2.4 KEY-PLAYER IDENTIFICATION AND SUB-GROUP DETECTION

To perform any terrorist activity there need to be some collaboration among the terrorist and these ties are framed around some nodes which act as key nodes or leaders who control and command the activity of the group. There are lots of works done to study about how the network is affected if the key nodes are removed. These networks are divided into subgroups and understanding these structures helps to disrupt terrorist network and develop effective control strategies to combat terrorism. Hence key player identification and sub-group detection are some major problem in criminal network analysis.

Stephen P. Borgatti [19] discusses about two problems in key player identification called as KPP1 and KPP2. Firstly in KPP1 the disorder in communication of the nodes if k nodes are removed has been addressed. It's being solved using graph's cohesion measure. Secondly KPP2 determines the influence of a node's tie in the network based on the maximum ties of its connection to other nodes.

Shou-de Lin and Hans Chalupsky [20] focus on finding abnormal instances in multi-relational networks (MNR) which uses unsupervised framework to model semantic profile and detects the suspicious node with the abnormal semantic profile. The authors propose a novel explanation mechanism that facilitates verification of the discovered results by generating human-understandable natural language explanations describing the unique aspects of these nodes.

Nasrullah Memon, Nicholas Harkiolakis and David L. Hicks [21] have introduced the investigative data mining technique to study terrorist networks using descriptive and predictive modeling based on centralities and applied it to the detection of high value individuals by studying the efficiency after removing some nodes, determining how many nodes are dependent on one node and if hidden hierarchy exists find the command structure. The authors have also demonstrated this newly introduced technique with a case study of 7/7 bombing plot.

Nasrullah Memon, Abdul Rasool Qureshi, Uffe Kock Wiil, David L. Hicks [22] discusses about the algorithms for subgroup detection using IDM and demonstrated them with an example of a

fictitious terrorist network. The software iMiner can detect all terrorists who are directly or indirectly connected to a specified terrorist, they can detect paths that connect two specified terrorists, they can detect connections between groups of terrorists and they can uncover connections between the root (a node) and a destination (another node in terrorist cell).

Yuval Elovici, Bracha Shapira, Mark Last, Omer Zaafrany and Menahem Friedman, Moti Schneider and Abraham Kandel [23] discuss about online tracking system called as Advanced Terrorist Detection System (ATDS) which determines the interest of a set of users based on their web access and it performs the real time monitoring of the web traffic generated by the same set of users and alerts the system if any accessed information is not relevant to the groups interest.

2.5 CNA FOR HOMELAND SECURITY

India is at the geographical center of a belt of terrorism, insurgent and separatist violence. Internally, India is faced with terrorist violence in Jammu and Kashmir, in the North East and the South. Militant organizations have links to external agencies, and these links can be surprisingly long [24]. It is necessary for the citizens and the authorities to understand the situation and learn how to face the problem using social network analysis techniques.

Aparna Basu [24] derives a linkage map of terrorist organizations in India which uses the methods of centrality and the co-occurrence of names of the terrorist organizations to determine the key players and the intensity of the links between them. The groupings affected by SNA based on textual links correctly displayed ideological and regional groupings of the terrorist organizations.

Sudhir Saxena, K. Santhanam, Aparna Basu [25] has developed in-house Terrorism Tracker (or T2) which performs systematic search for information on terrorist events from open sources. This paper addresses organization-to-organization links of terrorist organizations operating in the Indian State of Jammu & Kashmir. The SNA software package, Visone, developed in Germany, has been used with the T2 generation of “co-occurrence” pairs where organizations are cited together in an event during the period 2000 – 2003. This output was converted into an adjacency matrix to form the input to Visone for analysis and generation of linkage graphs.

2.6 COUNTER TERRORISM

Uffe Kock Wiil, Nasrullah Memon and Jolanta Gniadek [26] present the Crime Fighter toolbox for counter terrorism which performs various processes like data acquisition, knowledge management and information processing using a number of tools that are categorized as semi automatic tools which are web harvesting tool, data mining tool, data conversion tool, SNA tools, visualization tools and manual tools like knowledge base tools and structure analysis tools.

Clifford Weinstein, William Campbell, Brian Delaney, Gerald O’Leary [27] has developed the Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR) which focuses on development of automated techniques and tools for detection and tracking of dynamically-changing terrorist networks as well as recognition of capability and potential intent. The authors have also simulated the terrorist attack based on real information about past attacks and generating realistic background clutter traffic to enable experiments to estimate performance in the presence of a mix of data. They have developed a new Terror Attack Description Language (TADL) which is used as a basis for modeling and simulation of terrorist attacks.

In order to destabilize and end the terrorist organizations we need to understand the how these networks evolved, the reason behind their origin and what makes them to grow even after

removing the leading covert nodes. These are some serious is problems in criminal network analysis which have been studied.

Rebecca Goolsby [29] briefly examines how Al-Qaeda evolved from an insurgency assistance group to a terrorist network of sophistication and global reach. It argues that Al-Qaeda filled the needs of Islamist insurgencies and then developed into a complex system of networks by co-opting other groups, hijacking their agendas and transforming their ideologies. Al Qaeda thus has global aspects which in a long run can withstand any disturbances and local aspects which are more vulnerable to discovery by local authorities and disruption. They tend to lack the training, professionalism, education, capacity to ensure strict security measures and discipline within their own ranks.

Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, Gabriel Weimann [30] discuss how terrorists share their ideology and communicate with members on the “Dark Web” the reverse side of the Web used by terrorists. To improve understanding of terrorist activities from the web, the information is collected using searching, browsing and spidering. Then it is filtered based on domain and linguistic knowledge. These are then analyzed as domestic and international terrorism based on the group profile, dynamics and relationships. It’s been applied for collecting and analyzing information of 39 Jihad web sites.

The following table compares the above mentioned categories of SNA techniques by illustrating the different types of analysis which are done in each type based on their unit of analysis and presents the various measures in each.

Table 1. Comparison of various analysis in different categories of SNA for covert networks.

Classification	Type of analysis	Unit of analysis	Identification
Link analysis	Network analysis	Sample of a network	Density using centrality metrics
	Weblogs	Link and content	Weak ties
	Shortest path	Concept space and co-occurrence associations	Shortest criminal associations between two or more entities based on quality and
	Search complexity	Heuristics based on human knowledge	Multilevel search based on accuracy and
Node discovery & key player identification	Geo-graphically distributed hidden	Location based	Latent structure with time sensitive and
	Data crystallization and outlier detection	Hidden network	Collaborative activities resulting from influential nodes
	Unknown network	Adjacent dyads and triads	Structural properties of uncertain organization
	E-mails	Labeled training examples	Predicts unseen incoming e-mail
DNA and Counterterrorism	Multimodal, dynamic large scale system	Complex socio-technical data (age, birth, incomplete and missing data)	Analysis and prediction of dynamic relations
	Temporal social data	Meta-network	Predicting most significant events
	Specific network/individual level data analysis	General features of two terrorist groups	Estimates vulnerability
Home land security	Multi variant analysis	Textual links from open source data	Linkage maps of terrorist organizations
	Structured and un-structured data analysis	Person-person, organization-organization, person-organization	Co-occurrence pairs

3. NETWORK STRUCTURE MINING

Social network analysis is the identification of the “most important” actors in a social network. In this section the paper discusses a variety of measures designed to highlight the differences between important and non-important actors. These entire measures attempt to describe and measure the properties of “actor location” in a social network. All these measures are first defined

at the level of individual actor. The measures can then be aggregated over all actors to obtain a group level measure of centralization.

Prominent actors are those that are extensively involved in relationships with other actors. The centrality can be measured in both non-directional relations and directional relations. Unlike the directional relation in non-directional relation, centrality of the node does not depend on being a recipient or source. There are three predominantly used actor-level indices namely degree centrality, closeness centrality, betweenness centrality [32].

In general, the terrorist network can be represented by an undirected and un-weighted graph $G = (V, E)$, where V is the set of vertices (or nodes) and E is the set of edges. Each edge connects exactly one pair of vertices, and a vertex pair can be connected by a maximum of one edge. A terrorist network consists of V set of actors or nodes and E relations between these actors. Mathematically, a network can be represented by an adjacency matrix A , which in the simplest case is an $N \times N$ symmetric matrix, where N is the number of vertices in the network. The adjacency matrix has elements.

$$A_{ij} = 1 \text{ if } i \text{ and } j \text{ are connected and } 0 \text{ otherwise}$$

The matrix is symmetric since if there is an edge between i and j then clearly there is also an edge between j and i . Thus

$$A_{ij} = A_{ji}$$

The degree of a vertex in a network is the number of edges attached to it. In mathematical terms, the degree ' D_i ' of a vertex i is [32]:

$$D_i = \sum_{j=1}^N A_{ij}$$

A network member with a high degree could be the leader or "hub" in a network.

Betweenness measures the extent to which a particular node lies between other nodes in a network [32]. The betweenness ' B_a ' of a node ' a ' is defined as the number of geodesics (shortest paths between two nodes) passing through it:

$$B_a = \sum_{i=1}^N \sum_{j=1}^N g_{ij}(a)$$

where $g_{ij}(a)$ indicates whether the shortest path between two other nodes i and j passes through node ' a '. A member with high betweenness may act as a gatekeeper or "broker" in a network for smooth communication or flow of goods (e.g., money, arms).

Closeness ' C_a ' is the sum of the length of geodesics between a particular node ' a ' and all the other nodes in a network. It actually measures how far away one node is from other nodes and is sometimes called farness [32]:

$$C_a = \sum_{i=1}^N l(i,a)$$

where $l(i,a)$, is the length of the shortest path connecting nodes i and a . The most central nodes can quickly interact with all the other nodes because they are close to all the others. Both Closeness and Betweenness centralities are global measures, where as degree centrality is termed as local measure. These three centrality measures may produce contrary results for the same graph.

In this paper the social network of 9/11 attack in 2001[31] has been referred for generating a synthetic data set. The following graph in Figure 2. could be used to analyze different relationships not only among the 19 hijackers involved in 9/11 attack but also uses the other

covert nodes contributing for the attack and the graph maps their association to various locations where they moved in.

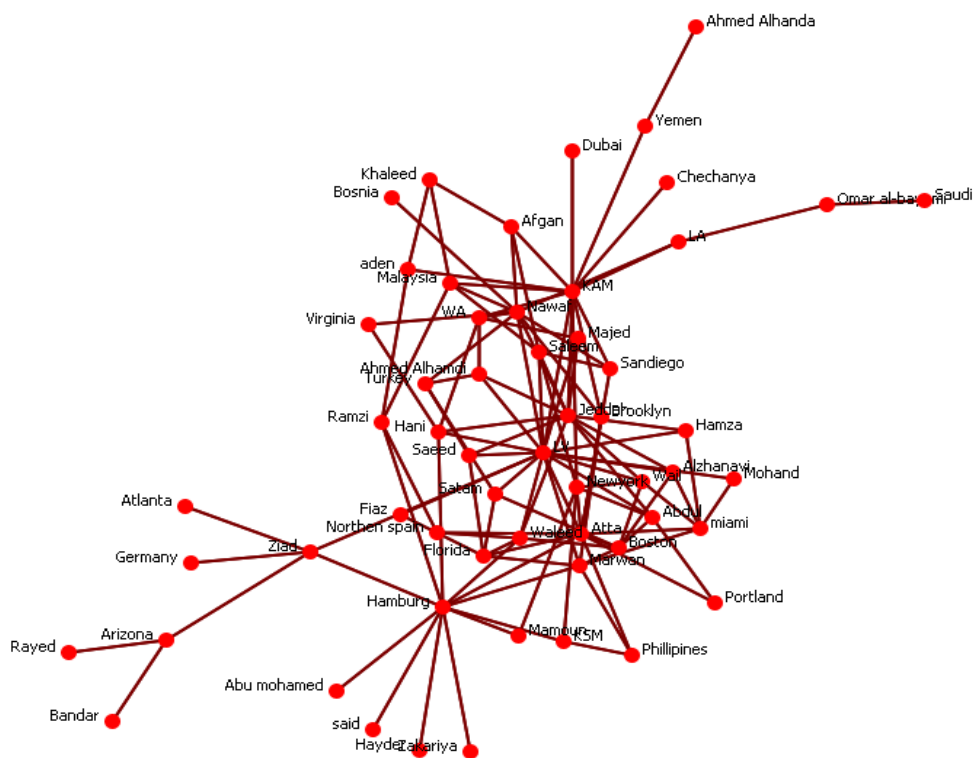


Figure 2. A graph depicting different relationships between the hijackers, conspirators and various locations in 9/11 attack.

For the network in Figure 2. the actor level indices are calculated using the above discussed three centrality measures which are shown in Figure 3. and the following table illustrates the maximum value node in each category.

Table 2. Top source node with highest centrality measures in 9/11 terrorist network.

Centrality Measures	Source Node	Maximum Value
Degree	Khalid Al-Mihdhar(KAM)	13
Betweenness	Khalid Al-Mihdhar(KAM)	392.35
Closeness	Rayed, Bandar	300

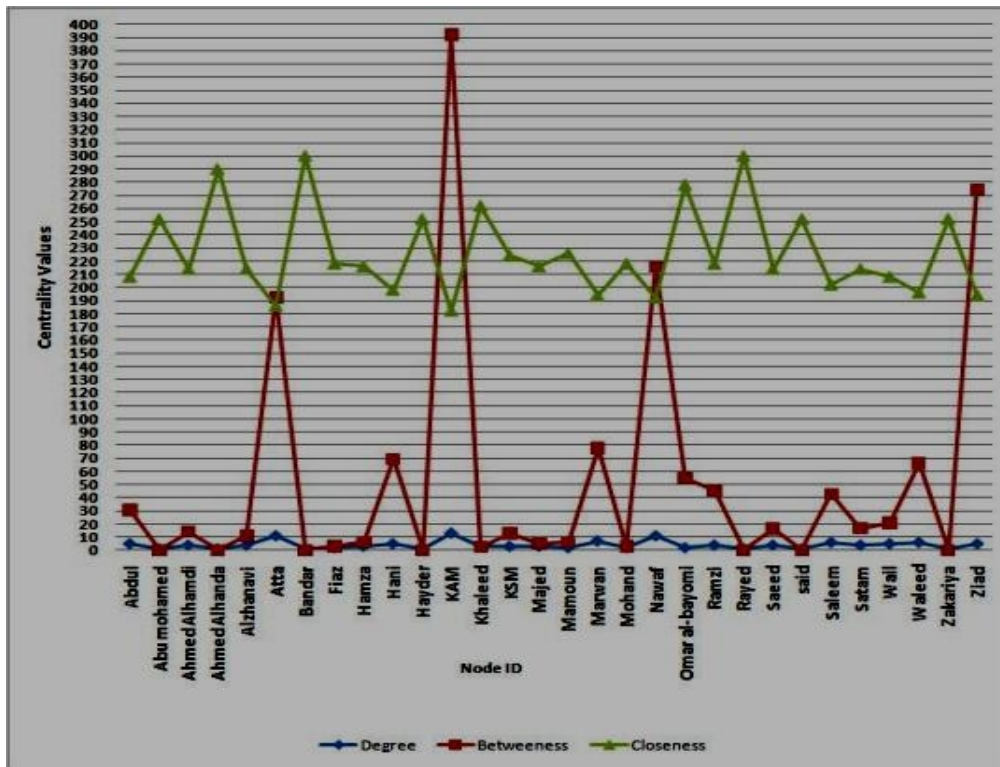


Figure 3. A graph showing the three centrality measures degree, betweenness and closeness for all the hijackers and associates involved in 9/11 attack.

The key entities for the above given network of 57 nodes is calculated based on Agent by Agent matrix and density of the network is computed as 0.07581. Figure 4 represents the key players of the above discussed network shown in figure 2 (it also includes locations):

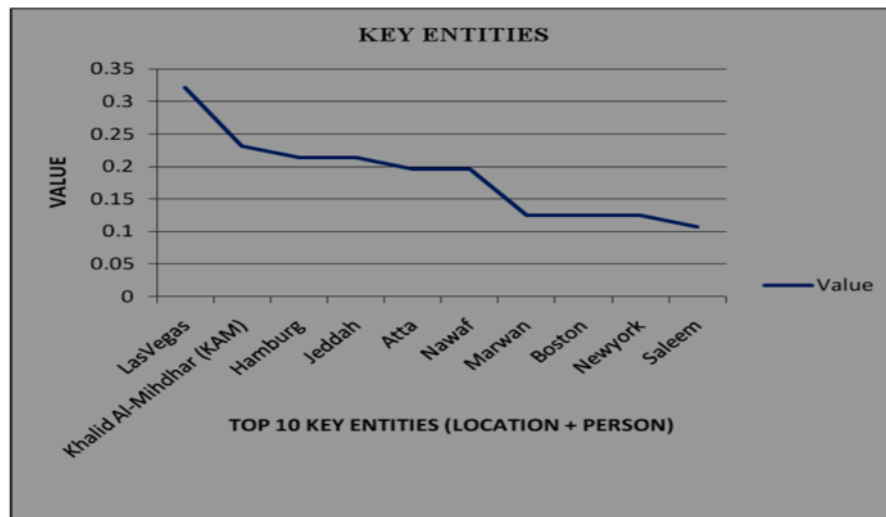


Figure 4. Key entities in figure 2

4. LIMITATIONS AND FUTURE DIRECTIONS

The major limitation of this area is all the research work has been done under the assumption that the data collected is complete information but in real world the data are incomplete. It's very difficult to collect the complete data about any terrorist activity. A lot of research has been done till now in which some of the following problems have not yet been addressed. In node discovery problem radial transmission is being always used. The hub-and-spoke model could also be implemented for influence transmission. Further study is also needed to solve the discovery of fake node and spoofing node. In DNA the behavioral impacts of social or political context and regional based specialties of the nodes are not represented in the graph. In CNA, the network could be formed not only between the persons but also between locations and properties for which temporal patterns are needed to help us predict the trend and operations of a criminal enterprise. The expansions of such enterprises are to be studied based on cross-regional analysis.

5. CONCLUSION

In this paper we have presented various social network analysis methods like link analysis, DNA, CNA for homeland security, exploring network structure of various terrorist networks, counter terrorism, key player identification and sub-group detection for terrorist network. The influence of the node on the network has been studied using three main indices of centrality namely degree, closeness and betweenness. A social graph has been visualized and generated using the 9/11 attack dataset which includes the terrorist and the locations.

REFERENCES

- [1] Jennifer J.Xu and Hsinchun Chen, "CrimeNet Explorer: A framework for criminal network knowledge discovery," *ACM Transactions on Information Systems*, vol.23, no.2, pp. 201-226, April (2005).
- [2] Steve Ressler, "Social network analysis as an approach to combat terrorism: past, present, and future research," *Homeland Security Affairs*, vol. II, no. 2, JULY (2006).
- [3] Hsinchun Chen, Wingyan Chung, Jennifer Jie Xu, Gang Wang Yi Qin and Michael Chau "Crime Data Mining: A general framework and some examples," *IEEE Computer Society*, vol.37, no.4, pp.50-56, (2004).
- [4] Nasrullah Memon and Henrik Legind Larsen "Practical approaches for analysis, visualization and destabilizing terrorist networks," presented at first international conference on availability, reliability and security , (2006).
- [5] Jennifer Schroeder, Hsinchun Chen, Jennifer Xu and Michael Chau "Automated criminal link analysis based on domain knowledge," *Journal of the American society for information science and technology*, vol. 58, no.6, pp. 842-855, (2007).
- [6] Robert D. Duval, Kyle Christenseny, Arian Spahiuz "Bootstrapping a terrorist network," presented in the conference of Southern Illinois University Carbondale, (2010).
- [7] C. C. Yang and T. D. Ng, "Terrorism and crime related weblog social network: link, content analysis and information visualization," presented in IEEE international conference on intelligence and security informatics, New Brunswick, NJ, (2007).
- [8] Xu J. J., Chen H., "Using shortest path algorithms to identify criminal associations," *Decision Support Systems*, vol. 38, pp. 473-487, (2004).

- [9] Boongoen, T., Q. Shen, and C. Price. "Disclosing false identity through hybrid link analysis," *AI and Law*, in press.
- [10] Yoshiharu Maeno and Yukio Ohsawa "Analyzing covert social network foundation behind terrorism disaster," *Int. J. Services Sciences*, vol. 2, no. 2, (2007).
- [11] Yoshiharu Maeno "Node discovery problem for a social network," *Connections*, vol. 29, pp. 62-76, (2009).
- [12] Dombroski, Matthew and Kathleen M. Carley "NETEST: Estimating a terrorist network's structure," *Computational & Mathematical Organization Theory*, vol.8, pp.235-241, (2002).
- [13] Christopher E. Hutchins and Marge Benham-Hutchins "Hiding in plain sight: criminal network analysis," *Computational & Mathematical Organization Theory*, vol.16, no.1 pp.89-111, (2009).
- [14] Dombroski, M., P. Fischbeck, and K. Carley, "Estimating the shape of covert networks," presented in the proceedings of 8th International Command and Control Research and Technology Symposium, Washington, DC, June (2003).
- [15] S. Appavu , R. Rajaram, M. Muthupandian, G. Athiappan, K.S. Kashmeera " Data mining based on intelligent analysis of threatening e-mail," *Knowledge-Based Systems*, vol. 22, pp.392–393, (2009).
- [16] Carley, K.M." A dynamic network approach to the assessment of terrorist groups and the impact of alternative courses of action," In *Visualizing Network Information. Meeting Proceedings RTO-MP-IST-063*. Neuilly-sur-Seine, France: RTO, pp. KN1-1 – KN1-10, (2006).
- [17] Ian A. McCulloh and Kathleen M. Carley "Social network change detection," Carnegie Mellon University, School of Computer Science, Technical Report, CMU-CS-08-116.
- [18] Carley, K. M. "Estimating vulnerabilities in large covert networks," presented in the proceedings of 9th International Command and Control Research and Technology Symposium held at Loews Coronado Resort, CA. Evidence Based Research, Vienna, VA, (2004).
- [19] BORGATTI, S. "The key player problem," presented in the proceedings of the National Academy of Sciences Workshop on Terrorism. National Academy of Sciences, Washington DC, (2002).
- [20] Shou-de Lin and Hans Chalupsky "Discovering and explaining abnormal nodes in semantic graphs," *IEEE Transactions on knowledge and data engineering*, vol. 20, no. 8, pp.1039-1052, (2008).
- [21] Nasrullah Memon, Nicholas Harkiolakis and David L. Hicks "Detecting High-Value Individuals in Covert Networks: 7/7 London Bombing Case Study," in the proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, pp. 206-215, (2008).
- [22] Nasrullah Memon, Abdul Rasool Qureshi, Uffe Kock Wiil, David L. Hicks "Novel algorithms for subgroup detection in terrorist networks," presented in the International Conference on Availability, Reliability and Security, Fukuoka Institute of Technology, Fukuoka, Japan, (2009).
- [23] Yuval Elovici, Bracha Shapira, Mark Last, Omer Zaafrany and Menahem Friedman, Moti Schneider and Abraham Kandel "Detection of access to terror-related web sites using an Advanced Terror Detection System (ATDS)," *Journal of the American society for information science and technology*, vol.61, no.2, pp.405–418, (2010).
- [24] Aparna Basu "Social network analysis of terrorist organizations in India," paper presented at the North American Association for Computational Social and Organizational Science (NAACSOS) Conference, Notre Dame, Indiana, pp. 26-28, (2005).
- [25] Sudhir Saxena, K. Santhanam, Aparna Basu "Application of Social Network Analysis (SNA) to terrorist networks in Jammu & Kashmir," *Strategic Analysis*, vol. 28, no.1, (2004).

- [26] Uffe Kock Wiil, Nasrullah Memon and Jolanta Gniadek “Knowledge management processes, tools and techniques for counterterrorism,” presented in the International conference on Knowledge Management and Information Sharing, pp. 29-36, (2009).
- [27] C. Weinstein, W. Campbell, B. Delaney, and J. O’Leary, “Modeling and detection techniques for counter-terror social network analysis and intent recognition,” presented in the proceedings of the IEEE Aerospace Conference, (2009).
- [28] Christopher C. Yang, Nan Liu, and Marc Sageman “Analyzing the terrorist social networks with visualization tools,” *Intelligence and Security Informatics, Lecture Notes in Computer Science*, vol. 3975, pp. 331-342, (2006).
- [29] Rebecca Goolsby “Combating terrorist networks: An evolutionary approach,” presented in the proceedings of the 8th International Command and Control Research and Technology Symposium held at National Defense War College Washington DC, Evidence Based Research Vienna VA, (2003).
- [30] Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, Gabriel Weimann “Uncovering the dark web: A case study of Jihad on the web,” *Journal of the American society for information science and technology*, vol.59, no.8, pp.1347–1359, (2008).
- [31] Valdis E. Krebs “Mapping networks of terrorist cells,” *Connections*, vol.24, no.3, pp. 43-52, (2002).
- [32] Linton C. Freeman “Centrality in Social Networks Conceptual Clarification,” *Social Networks*, vol.1, pp. 215-239, (1978/79).