TERRORIST NETWORK MINING: ISSUES AND CHALLENGES

R. D. Gaharwar[1], Prof. D. B. Shah[2], G. K. S. Gaharwar[3]

[1, 2] G. H. Patel Department of computer Science and Technology,
Sardar Patel University, Vallabh Vidyanagar (India)
[3]School of Business and Law, Navrachana University, Vadodara (India)

ABSTRACT

Before few decades Terrorism was merely considered as a law and order problem in many countries. But due exponential increase in the number of such organizations and their activities, they become threat for very existence of many countries. Many of these terrorist organizations are equipped with the advance technology based weapons. Also, it has been observed in last few decades that these terrorist organizations are communicating and coordinating with other terrorist organizations. Traditional war methods are not equipped to counter such an organized network of terrorist organizations and a systematic effort is greatly to study the architecture of such terrorist networks. This paper is a small step in that direction. This paper looks at the usefulness of Social Network Analysis and Graph Theory for decoding the structure of terrorist networks through Terrorist Network Mining.

Keywords: Betweeness, Closeness, Graph Theory, Prestige, Terrorism, Terrorist Network Mining, Social Network Analysis.

I. TERRORISM

During the past few decades terrorism is becoming a worldwide phenomenon and emerged as a threat to internal security to many nations. What can be called as the definition of the term "terrorism" is an attention seeking question. Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them [1].

Terrorism is a pejorative term; it is a word with inherently negative connotations that is generally applied to organizations working against the citizens of the country. All dictionaries agree that terrorism is all about fear, uncertainty and violence, and a terrorist is one who uses act of violence and terror, or other fear-inspiring means, to coerce a government or a community to agree on something that the terrorist wants. Most of the times these terrorist and terrorist organizations are involved in the armed attack which results in death of innocent citizens, loss and/or damage of private and/or public property. These organizations make a long term impact to the region of their operations by hindering development of the affected region; Jammu & Kashmir and Palestine are the examples of such terrorism. In the era where many countries are equipped with nuclear warheads, the traditional war between countries is distant reality and so such wars are been replaced by proxy wars better known as terrorism. The greatest security threat facing countries like India, Afghanistan, Pakistan, United States and

United Kingdom is not from other countries, but from terrorist organizations that attack informally, using terror at any time and place. The war against such proxy war can no longer be fought with structured battle that with structured military establishment, the war against terrorism can only be won with superior knowledge about these terrorist organizations. Knowledge which can be used to study the terrorist network helps security organizations to identify the role of each organization in the network, finding association of each of the organizations in the network and to foresee their next action. This systematic approach, called as Terrorist Network Mining (TNM), towards will lead us to the use of Social Network Analysis (SNA) and Graph Theory concepts for studying the behavior of these terrorist networks.

II. NETWORK ANALYSIS

Network analysis is the study of social relations among a set of actors. It is a field of study -- a set of phenomena or data which we seek to understand. Network analysis is based on the uncovering the patterning in data that seems unrelated initially. There are some theoretical perspectives in network analysis which focuses on relationships between actors and not on the attributes of these actors and that these patterns display important features of the lives these actors. Network analysis helps in explaining that how an individual actor's importance is defined by a fact that how that actor is tied into the larger web of social connections. Network analysis has following perspectives:

- focus on relationships between actors rather than attributes of actors
- structural and locational properties of actors
- focus on structural properties of actors
- emergent effects

Network Analysis focuses on the intuitive notion that the patterns of human interaction represent the behavior of the individuals who display them. Network analysts believe that the characteristics of individuals can be analyzed in better way by focusing on their role in web of social connections and this role will determine the stature of the individual in the society. Moreover the success or failure of any organization or social structure depends on the strength of the social connections.

III. TERRORIST NETWORK MINING (TNM)

Relationship among terrorists form the basis for the organized crimes and are essential for smooth operation of a terrorist organization which can be viewed as a network where nodes represents a terrorist or an terrorist organization and links represent relationships between terrorists and/or terrorist organizations. TNM has emerged as a novel field of research often applied to investigation of organized crimes. Relationships among criminals/terrorists form the basis for the organized crimes and are essential for smooth operation of a criminal/terrorist organization [2]. TNM is emerged a field of research often applied to investigation of such organized crimes from terrorists.

TNM is the process of posing questions and digging useful information often earlier unknown from huge amounts of data of social communication using various known techniques.

Recently data mining is becoming an effective tool for counter-terrorism applications. For example, data mining can be used to detect unusual patterns, terrorist activities and fraudulent behavior. To carry out effective terrorist network mining and extract useful information for counter-terrorism and national security, we need to gather all

kinds of information about terrorist organizations. However, these terrorist organizations operate in a covert manner and their secrecy proves to be their strength hence this information is not available in open source.

IV. SOCIAL NETWORK ANALYSIS (SNA)

Nowadays TNM can successfully be used for the investigation of organized crimes. Relationships among criminals/terrorist form the basis for the organized crimes and are essential for smooth operation of a criminal/terrorist organization which can be viewed as a network where nodes represent terrorist and links represent relationship or associations between terrorist [3]. This mining of terrorist networks used to be a time consuming task in past because it was done manually, moreover no prominent techniques were available for it. However nowadays SNA has emerged as an effective technique for destabilizing these terrorist networks. In past few years the techniques of SNA have brought about a paradigm shift in counter terrorism planning and strategies [4]. Study of the linkage patterns of terrorist networks can usefully draw upon the academic perspectives provide by Social Network Analysis and modern statistical and visualization tools [5]. In past few years there has been tremendous increase in the number of articles on Social Network Analysis. Fig. 1 shows the increase in number of users on social network (Data Source: *http://dstevenwhite.com/2013/ 02 /09/ social-media-growth-2006-to-2012/).*

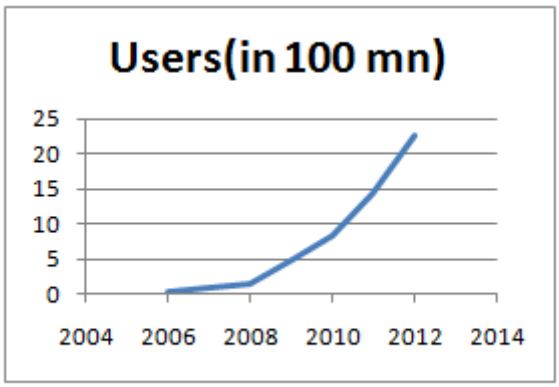

Fig. 1: Increase in Number of Social Network Users

The social network paradigm which is the theoretical and formal bases for the relational study for social structures is nowadays used for the analysis of relational data measured on groups of social actors and studying structural properties of actors interaction. The SNA focuses on destabilizing the pattern of human interaction. SNA uses graph theoretic calculations to study the behavior of networks and multivariate analysis to create visual displays [6]. In some form or other these methods have been used to track and uncover associations of criminals. SNA has a long history of application to evidence mapping in both fraud and criminal conspiracy cases [7]. The terrorist organization can be represented as a network using a technique known as SNA which studies social relationships amongst nodes and ties. In case of a terrorist network, the members are considered as the nodes and the ties describe the interactive or collaborative relationships between the pairs of nodes [8]. SNA helps to answer the following questions [9]:

- Who is central node in the networks?
- What sub-groups exist in the network?
- What are the patterns of interaction between sub-groups?
- What is the overall structure of the networks?

- How does information flow in the network?

Terrorist networks are well-suited to study using social network analysis, as they consist of networks of individuals that span countries, continents, and economic status, and form around specific ideology. Most importantly, social network analysis can be used to understand terrorist networks and form the basis of a more effective counter-measure.

V. DIFFERENT APPLIANCE OF SNA FOR TNM

The government agencies are intensely interested in data mining. A 2004 survey by the Government Accountability Office found that federal agencies were engaged in or planning 199 data mining projects, including 122 involving personal data. A database of phone records wouldn't be hard to create; the data exists.[reference]

Valdis Krebs, founder of social networking analysis company OrgNet.com, conducted his own analysis of the 9/11 terrorists by collecting information from press reports such as who called whom, the addresses shared by the terrorists and their known associates, and information that they used the same frequent flier number. Krebs found that more links led to the group's leader, Mohammad Atta, than to any other terrorist.

One data mining effort within the Defense Department, called Pathfinder, involves analyzing government and private-sector databases, including rapidly comparing and searching multiple large databases for anti-terrorism intelligence. The FBI's Foreign Terrorist Tracking Task Force culls data from the Department of Homeland Security, the FBI, and public data sources to prevent foreign terrorists from entering the country. Other tools for counterterrorism include technology from Autonomy that searches Word documents across various intelligence agency databases; Verity's K2 Enterprise, which mines data from the intelligence community and through Internet searches; and Insight's Smart Discovery, which looks into and categorizes data in unstructured text.

VI. GRAPH THEORY FOR SOCIAL NETWORK ANALYSIS

The graph theories are use to create the models which will help in the analysis of network. Basically, the graph is the collection nodes (n) and the edges (e) such that e= (n_i, n_j) where n_i and n_j are any two connected nodes. When graph theory is used to represent the social network then such graph is called sociogram, where nodes are the actors and edges are the lines of connection between these actors. These sociogram can be both directional as well as non-directional.

There are various concepts of graph theory like closeness between the actors, positions of prestige, centrality etc which can be applied in the analysis of social networks.

Degree	Number of *direct connections that a node has*
Betweenness	The number of paths that *connect pairs of nodes that pass through a given node*
Prestige	A measure of *links to other highly central nodes*
Closeness	The number of *other nodes that are linked to a given node*

These parameters have calculated indices based on matrix algebra with direct network implications. An entity with a high Degree index means that it is very strongly networked and active. An entity with a high Betweenness index would have a strong ‘brokerage’ role. A centralised network with a very high Degree index in one or a few nodes can become a single point of failure. A less centralised network would be resilient in the

face of collapse or failure; it would experience graceful degradation. [*Application of Social Network Analysis (SNA) to Terrorist Networks*]

VII. PRIVACY ISSUES

Data mining is nowadays used for detecting unusual behavior patterns, terrorist activities and fraudulent behavior. Terrorist network data mining applications can be beneficial to human lives but it may pose threat to the privacy of individuals. Data mining tools that are easily available on the internet can be used by the notorious individuals to extract the information of some individuals from the data stored on the databases and this may consequently violate the privacy of individuals. Therefore there is very thin line of difference between gathering the information about individuals for national security and for violating the civil liberties.

VIII. CONCLUSION

The complex web of terrorist organizations can be decoded with the help of systematic approach of Social Network Analysis. Good old graph theory concepts like degree, betweenness, prestige and closeness can effortlessly identify the role and contacts of each organization in the terrorist network. Terrorist network mining tools develop to study these terrorist networks and help law enforcement agencies to destabilize this networks.

REFERENCES

[1] "Measures to Eliminate International Terrorism," The UN General Assembly Resolution 49/60, December 9, 1994.

[2] N. Chaurasia, M. Dhakar, A. Tiwari and R. K. Gupta, "A survey on Terrorist Network Mining: Current Trends and Opportunities," International Journal of Computer Science & Engineering Survey (IJCSES), vol. 3, no. 4, pp. 59-66, August, 2012.

[3] M. A. Shaikh and W. Jaixin, "Investigative Data Mining : Identifying Key Nodes in Terrorist Networks," IEEE International Conference Multi Topic, 2006.

[4] U. K. Will, N. Menon and P. Karampelas, "Detecting new trends in terrorism networks," in International Conference on Advances in Social Networks Analysis and Mining, 2010.

[5] S. Wasserman and K. Faust, "Social Network Analysis: Methods and Applications," Structural Analysis in the Social Sciences, Cambridge University Press, vol. 8, 2002.

[6] M. K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," Social Networks, vol. 13, no. 3, pp. 251-274, September, 1991.

[7] W. E. Baker and R. R. Faulkner, "The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry," America Sociological Review, vol. 58, no. 3, pp. 837-860, 1993.

[8] S. Azad and A. Gupta, "A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis," Journal of Terrorism Research, vol. 2, no. 2, 2011.

[9] H. Chen and J. J. Xu, "CrimeNet Explorer : a framework for criminal network knowledge discovery," ACM Transactions on Information Systems, vol. 23, no. 2, pp. 201-226, 2005.