© 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Application of Centrality Principles for Terrorist Network Role Analysis

R. D. Gaharwar, Prof. D. B. Shah
G. H. Patel Department of Computer Science & Technology, Sardar Patel University, Vallabh Vidyanagar, Gujarat, India

ABSTRACT

Number of terrorist attacks are increasing rapidly around the globe and world is facing a constant need to strengthen counter-terror activities. Information about terrorist organizations/terrorists can be gathered by exploring internet. Enormous data on internet can be examined by sophisticated data mining tools to find useful information. Social Network Analysis tools such as Centrality Principles can be effectively used in this area. This article shows the usefulness of different centrality principles in analyzing and understanding terrorist networks.

Keywords : Data Mining, Social Network Analysis, Terrorist Networks, Terrorist Network Analysis, Centrality Principles

I. INTRODUCTION

Terrorist organizations/terrorists form a network during their operations. These networks have terrorist organizations/terrorists as their nodes and the association developed through the exchange of materialistic or non- materialistic things as links between nodes. Terrorist network nodes may exchange funds, arms, information, terrorist, ideology etc to form linkage between them [1]. At times studying such network may be a difficult task because these networks are dynamic, agile and covert [2]. Terrorist networks most of the times do not behave like normal network. Hence complete information to study such networks may not be available.

Role Analysis:

In network, different nodes play different roles. Every node has its own magnitude and significance in the network. Hence it becomes important to identify the nature of relationship and association these nodes exhibits [3]. Some nodes act as sustainer node of the network while some are just use for smooth information flow. Some are peripheral nodes while some are central nodes. Role Analysis can be used to find various roles in network, for example, leaders, gatekeepers and followers [4]. Centrality principles can be use to decode roles of different nodes in the network [5]. In terrorist network centrality principles can help to identify which is key node/leader; which node is future leader and which node is simply a broker. Decoding the role of different nodes aid in understanding terrorist networks and this may lead in destabilizing them.

1.1 LITERATURE REVIEW

Valdis E. Krebs wrote an article for mapping covert networks. In this article the author examined the tragic event of September 11th, 2001. During his study for this article the author found out that there were 19 hijackers involved in this happening. The author collected information about this event from major newspapers like New York Times, The Wall Street journal etc and World Wide Web. The data collected from these sources was used to create linkage map for

19 hijackers and various mathematical principles like Clustering Coefficient, Mean path length etc were applied. The author also applied centrality principles like Degree, Closeness and Betweenness. Based on this study the author concluded that Mohammed Atta was the leader of this series of attacks. This conclusion was made based on the fact that although Mohammed Atta did not score high on betweenness centrality, his degree and closeness scores were highest. This helped the author to find out the key node of the network. Finally the conclusion was made that to get an accurate picture of terrorist network one should identify the type of relationship the terrorist organization/ terrorist have among them. Here the author has considered only specific attack to get a complete picture of terrorist network but in such networks scope of investigation is large [6].

Sarita Azad and Arvind Gupta tried to quantitatively assess 26/11 Mumbai attacks. The author explained how Social Network Analysis can be used as an effective Network Analysis tool. During their research they examined the media reports about the call intercepts of 10 terrorists involved in 26/11 Mumbai attacks to create a network graph. The adjacency matrix was created to show the existence or non-existence of links between terrorists. Four centrality principles (degree, closeness, betweenness, eigen vector) were considered for terrorist understudy. The authors calculated centrality principle values of each terrorist link through mathematical formulas and concluded that the terrorist having highest value of eigenvector , betweenness and degree was identified as key player for entire operation [7].

Nisha Chaurasia et al. wrote that due to the advancement in technology, terrorists and criminals are now equipped with sophisticated techniques. The authors mentioned that there is a need to detect and analyze terrorist activities by exploring web traffic for which enormous data is to be analyzed within fraction of seconds by advanced data mining tools like Social Network Analysis. The block modeling approach was used by the authors in this article to uncover the interaction and association patterns between different terrorist groups. The authors mentioned the importance of centrality principles like degree, closeness, betweenness and eigen vector as Social Network Analysis tools. Other content-based terror detection methods like Intrusion Detection System, Vector Space Model, Clustering techniques and Content-based detection of terror related activities were also discussed in the article. Finally the authors concluded that hierarchical dependence centralities can aid law enforcement agencies to identify the key player from terrorist network [8].

II. METHODS AND MATERIAL

Terrorist networks can be considered as a simple undirected graph and the role of each node in the network can be analyzed with the help of Social Network Analysis tools. Different centrality principles like degree, closeness, eigen vector and betweenness can be used to identify the key player from the network. The meaning and the interpretation of each centrality principle is as shown below:

1) **Degree:** Degree is a measure of the number of direct links a node has with other nodes in the network. It usually is an effective measure of the importance of the node in the network and its measure how strongly active that node is. It usually indicates leader/ hub node in the network. The degree D_l of any vertex l is [9]:
   $D_l = \sum_{i=0}^{n} A_{il}$
2) **Betweenness:** Betweenness is concern with whether or not a node in a communication network is central to the extent that it falls on the geodesics path between two nodes. It is a measure of the influence of a node over the flow of information, funds, arms etc between nodes. It usually indicates Brokerage / gatekeeper node

of the network. The betweenness B_l for any vertex l is [9]:

$B_l = \sum_i^n \sum_j^n g_{ij}(l)$

Where $g_{ij}(l)$ indicates number of the shortest geodesic paths between nodes i and j passing through l.

3) **Closeness:** Closeness is the sum of all shortest path between particular node and every other node appearing in the network. Closeness decides the robustness of the network understudy. It usually indicates sustainer / future leader of the network. The Closeness C_a for any vertex a is [9]:

$C_a = \sum_{j=0}^{n} L(j,a)$

Where L(j,a) is the extent of geodesic path between nodes j and a.

4) Eigen vector: Eigen vector considers that not all connections posses identical importance. The gravity of the nodes in the network connected to influencer nodes increases automatically. It usually indicates prestige/ influence of the node in the network. The Eigen vector E_a for any vertex a is [9]:

$E_a = \frac{1}{\lambda} \sum_{j=0}^{n} A_{ia} x_a$

Where λ is a constant

III. DEMONSTRATING THE ROLE ANALYSIS FOR TERRORIST NETWORKS USING SNA

The sample data used for analysis of terrorist networks are from the various authentic agencies like South Asia Terrorism Portal, news articles, government publications and reports on terrorism were collected. For the study, the sample data used is based on the terrorist attacks from 2005 to 2013. The co-occurrence of more than one organization in any single terrorist attack is inferred as the linkages between those terrorist organizations. Each and every vertex in the terrorist network represents a terrorist organization and an edge indicates a direct involvement of both the organizations in one of the terrorist attack. These links represent relationships or associations between terrorist organizations. Organizations selected for the study are mentioned in Table 1.

Table 1. List of Organizations selected for the study

Vertex No.	Organization Name
1	Akhil Bharat Nepali Ekta Samaj
2	Al Badr
3	All Parties Hurriyat Conference
4	Al Jehad
5	Al Mujahid Force
6	All-India Sikh Students Federation
7	Jamiat-ul-Mujahideen
8	All Tripura Bengali Regiment
9	Al-Umar-Mujahideen
10	Babbar Khalsa International
11	Al-Qaida
12	Bhindrawala Tigers Force of Khalistan
13	Communist Party of India (Maoist)
14	Communist Party of India (Marxist-Leninist)
15	Deendar Anjuman
16	Dukhtaran-e-Millat
17	Gorkha Tiger Force
18	Harkat-ul-Mujahideen
19	Hizb-ul-Mujahideen
20	Indian Mujahideen
21	International Sikh Youth Federation
22	Ikhwan-ul-Mujahideen
23	Islami Inquilabi Mahaz
24	Islami Jamaat-e-Tulba
25	Islamic Students League
26	Jaish-e-Mohammad
27	Jamiat-ul-Mujahideen
28	Jammu & Kashmir Islamic Front
29	Jammu & Kashmir Liberation Front
30	Jammu & Kashir National Liberation Army
31	Jammu & Kashmir Students

	Liberation Front
32	Kanglei Yawol Kanna Lup
33	Kangleipak Communist Party
34	Kashmir Jehad Force
35	Khalistan Commando Force
36	Khalistan Liberation Army
37	Khalistan Zindabad Force
38	Lashkar-e-Taiba
39	Lashkar-e-Jabbar
40	Lashkar-e-Omar
41	Manipur People's Liberation Front
42	Mahaz-e-Azadi
43	Maoist Communist Centre
44	Muslim Janbaz Force
45	Mutahida Jehad Council
46	Muslim Mujahideen
47	National Democratic Front of Bodoland
48	National Liberation Front of Tripura
49	People's Revolutionary Party of Kangleipak
50	Students Islamic Movement of India
51	Tamil Nadu Liberation Army
52	Tamil National Retrieval Troops
53	Tehrik-ul-Mujahideen
54	Tehrik-e-Hurriat-e-Kashmir
55	Tehrik-e-Jehad
56	Tripura Liberation Organisation Front
57	Liberation Tigers of Tamil Eelam
58	United Liberation Front of Assam
59	United National Liberation Front
60	Students Islamic Movement of India
61	Inter-Service Intelligence

IV. RESULT OF THE STUDY DEGREE

On analysis it has been found that from remaining 24 out of total of 61 organizations taken into the study, ten organizations share 77.98% of links. Table-2 represents the list of these ten terrorist organizations. Though simple, degree is often a highly effective measure of importance of a node in many social settings people with more connection tend to have more power [10].

It is evident from the Table-2 that terrorist organizations like Hizb-ul-Mujahideen, Lashkar-e-Taiba, and Harkat-ul-Mujahideen are prominent in the terrorist operations. Pakistani intelligence agency, Inter-Service Intelligence (ISI) is also found in top five which indicates that it provide support in terror attacks in the region. An interesting observation is about the "All Parties Hurriyat Conference (APHC)", APHC has always distant itself from any terrorist group but the name in the top ten suggest that it may not be true and APHC may be connected to one or more terrorist organizations.

Table 2. Ten Organizations with the highest links

Rank	Organization	Percentage Links
1	Hizb-ul-Mujahideen	14.009 %
2	Lashkar-e-Taiba	11.35 %
3	Harkat-ul-Mujahideen	8.69 %
4	Inter-Service Intelligence	8.21 %
5	Jaish-e-Mohammad	7.97 %
6	All Parties Hurriyat Conference	7.48 %
7	Babbar Khalsa International	6.76 %
8	Khalistan Zindabad Force	5.79 %
9	Al Badr	3.86 %
10	United Liberation Front of Assam	3.86 %

The concepts of graph theory are used to calculate the role/position of any terrorist organization in the network. Betweenness measures the extent to which a particular node lies between other nodes in a network [11]. The betweenness index is an indicator of a 'brokerage' role. The role of brokerage is important

in network as it provides the means of communication to the distinct nodes. Organizations with high betweenness index are at the centre of networks. According to this view, a point in a communication network is central to the extent that it falls on the shortest path between pairs of other points. Other members of the network were assumed to be "responsive" to persons in such central positions who could influence the group by "withholding information (or) coloring or distorting it in transmission" [12].

Since long India is claiming that the Inter-Service Intelligence (ISI) is providing logistics and financial support to different terrorist organizations operating in India, form the Table 5 of organizations having highest betweenness index it is comprehensible that ISI is working as broker between terrorist groups operating in India. United Liberation Front of Assam (ULFA) is found to be second most between organizations in the network. It infers that ULFA is behaving as a broker between to ISI and two sub networks, one consist of terrorist organizations operating in the state of Jammu and Kashmir other consists of militant organizations operating eastern part of India.

Table 3. Ten Organizations with the highest betweenness index

Rank	Organization	Betweenness index
1	Inter-Service Intelligence	13.39 %
2	United Liberation Front of Assam	9.13 %
3	Harkat-ul-Mujahideen	8.98 %
4	All Parties Hurriyat Conference	7.61 %
5	Jammu & Kashmir Liberation Front	7.61 %
6	Al Badr	6.24 %
7	Hizb-ul-Mujahideen	5.33 %
8	United National Liberation Front	5.18 %
9	Jammu & Kashmir Islamic Front	4.72 %
10	Lashkar-e-Taiba	3.65 %

V. RESULTS AND DISCUSSION

During the above data mining exercise, two centrality indicators were used to identify the role/position of organizations in terrorist networks. Interesting result has been derived. Here the application of centrality principles has correctly identified ISI as a brokerage player in the network although it does not have largest number of links to other organizations. As most of the media reports suggest that ISI is the central player in the terrorist network operating in India. Therefore the result of this study can be strongly supported by the real life information. Also, periodic check of these principles can also help in identifying the changing relationship among different militant organizations in the country.

Moreover the power analysis indicates that Hizb-ul-Mujahideen and Lashkar-e-Taiba have prominent influence over other organization. Both of these organizations can also be seen very frequently in media reports for their influence on terrorist networks in India.

VI. CONCLUSION

Terrorist networks are very complicated networks and the information available about them is very limited. Social Network Analysis tools can prove effective and powerful weapon to understand such complex networks. These tools aid to create fairly clear picture of terrorist networks and analyze them even when limited information is available about them. Moreover from the results also it appears that open source data can be suitable for such research and Social Network Analysis can be an effective tool for such Terrorist Network mining. The law enforcement agency who regularly intercepts web traffic, satellite signals and phone conversation can effectively use these tools to understand, analyze and destabilize these dark networks and strengthen their counter-terrorist actions.

However terrorist networks are immensely complex networks and should be analyzed in multidimensional space with other modern methods too. Social Network Analysis tools can be used with other modern techniques such as Swarm intelligence algorithms, Fuzzy logic, neural networks and Genetic Algorithms to enhance the results.

VII. REFERENCES

[1]. Gaharwar, R., Shah D., and Gaharwar, G.(2016): The Study of Multi-Search Services for Terrorist Network Mining. International Journal of Computer Applications, 147(11): 30-32.

[2]. Sparrow, M.(1991): The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks 13: 251-274.

[3]. Yang, X., Chau, M., Hom, A., and Chen,H.(2005): Visualizing criminal relationships: comparison of a hyperbolic tree and a hierarchical list. Decision Support Systems: 69-83.

[4]. Memon, N. and Larsen, H.(2006): Structural Analysis and Destabilizing Terrorist Networks. In Proceeding Conference on Data Mining.

[5]. Gaharwar, R., Shah D., and Gaharwar, G.(2015): Terrorist Network Mining: Issues and Challenges. International Journal of Advance Research in Science and Engineering,4(1) ; 33-37.

[6]. Krebs, V.(2001) "Mapping networks of terrorist cells. Connections 24 : 43-52.

[7]. Azad, S. and Gupta, A. (2011): A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis. Journal of Terrorism Research, 2(2).

[8]. Chaurasia, N.,Dhakar, M., Tiwari, A., and Gupta, R.(2012): survey on Terrorist Network Mining: Current Trends and Opportunities. International Journal of Computer Science & Engineering Survey (IJCSES), 3(4) : 59-66

[9]. Shaikh, M., and Jaixin, W.(2006): Investigative Data Mining : Identifying Key Nodes in Terrorist Networks. In Proceeding IEEE International Conference Multi Topic.

[10]. Chen, H. and Xu, J.,(2005):CrimeNet Explorer : a framework for criminal network knowledge discovery. ACM Transactions on Information Systems, 23(2):201-226.

[11]. Karthika, S. and Bose, S.(2011): A comperative study of social networking approaches in identifying the covert nodes. International Journal on Web Services Computing (IJWSC), 2(3), : 65-78.

[12]. M. E. J. Newman(2003):The structure and function of complex networks. SIAM Review, 45:167-256.