International Journal of Engineering & Technology, 7 (1) (2018) 95-99

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i1.8828
Research paper

An innovative approach for identification of pivotal node in terrorist network using promethee method (an anti-terrorism approach)

Saurabh Singh [1] *, Shashikant Verma [2], Akhilesh Tiwari [3]

[1] Computer Science & Engineering, Jabalpur Engineering College Jabalpur India
[2] Computer Science & Engineering, GBPEC Pauri Garwal India
[3] Computer Science Engineering & IT , MITS Gwalior, India
**Corresponding author E-mail: ssingh@jecjabalpur.ac.in*

Abstract

Terrorist network analysis is vital for intelligence analysis and for deriving useful information from available raw data. Computer Science and Graph Theory provide instructive tools for the study and graphical interpretation of these networks. In this paper, we examine the 26/11 Mumbai attack terrorist network dataset and employ the Preference Ranking Organization Method for Enrichment of Evaluation (PROMETHEE) for identification of key node on the terrorist network. PROMETHEE is an effective multi-criteria decision-making model. It provides a framework to find the most suitable alternative by integrating the quantitative and qualitative factors to the decision problem and facilitates easy computation. From the 26/11 Mumbai attacks data set of terrorist network. It is found that out of several terrorists in the network "Wassi" was the focal actor. Based on the PROMETHEE framework, it is resolved that the obtained terrorist nodes can be instrumental for the intelligence and law enforcement agencies to confine their focus on important members of the terrorist network which can deter the functioning of these networks.

Keywords: *Terrorist Networks; Social Networks; Social Network Analysis (SNA); Preference Ranking Organization Method for Enrichment of Evaluation (PROMETHEE); Centrality; Betweenness Centrality; Closeness Centrality; Eigenvector Centrality; PageRank Centrality; Efficiency.*

1. Introduction

Terrorism is an inimical matter of global concern. It is a crucial and extensive problem which causes colossal damage to a society and the economy. The terrorist networks consist of radicalized individuals and groups that are organized to carry out hostile activities. With the advancement in technology, the destructive capability of these terrorist organizations has increased enormously. Therefore comprehensive techniques for the structuring and analysis of raw data to uncover critical information are required which can lead to the impediment of effective functioning of these networks.

A social network is a network of people or a network of groups of people. The people or groups form the nodes of the network, and the edges represent connections such as acquaintance, professional relationships or communication links between them. These networks provide an effective representation of a social system and facilitate the derivation of substantive information through their analysis. So far, there are various tools developed in the analysis, modeling and understanding of these networks. We can infer several significant characteristics of the network and one of them is to quantify and understand the traits of each node in the network. This role identification can thus lead to finding key actors in the network which is instrumental in various investigations.

There are various algorithms or measures, which quantify specific properties of a node based on a single criterion. For example, the degree centrality of a node in an undirected network is the number of edges attached to it. In a social network, it may be expected that the node with a higher degree will have greater influence or access in the information. Similarly, we can calculate the betweenness centrality which measures the extent to which a node lies on paths between other nodes. The nodes with high betweenness centrality may have marked influence within a network by virtue of their control over information passing between others. [2].

Employing a single measure to find the key or central node can be delusive and can lead to the ignorance of other crucial properties of a node. Therefore, in this research we incorporate multiple criteria, which are betweenness centrality, closeness centrality, eigenvector centrality, pagerank centrality and efficiency and apply a multi-criteria decision-making model to find the pivotal node in the network.

Multi-criteria decision making facilitates structuring and solving of complex decision problems. It is employed for the evaluation of different alternatives as the basis of multiple criteria to give the most preferred or suitable alternative. There are various multi-criteria decision making methods. In this paper, we apply the Preference Ranking Organization Method for Enrichment of

Evaluation (PROMETHEE), a multi-criteria decision-making model based on the mutual comparison of each alternative pair with respect to each of the selection criteria.

In this paper, we consider the 26/11 Mumbai Attacks data set [1]. The nodes in Fig 2 are the terrorists named in the terrorist attack, and the edges represent the communication link between the terrorists.

2. Literature survey

Social Network Analysis (SNA) and its application within the field of criminal surveillance has been a major topic of research in the recent years. A large number of techniques have been developed to extract and analyze data from a network. Following is some of the works available in the field of SNA and its consequent application for terrorist networks. Furthermore, few works associated with PROMETHEE are listed.

In [3] and [8] we find descriptive and introductory literature on the relevance of network analysis to the analysis of criminal intelligence. It discusses the data mining perspective useful in finding the structural properties of a criminal network.

In [3] the use of centrality measures to identify key actors in criminal networks is surveyed and in [4] centrality measures are used to identify the group leader of the 9/11 attackers.

In literature [7] Memon and co-authors to have developed a toolkit for subgroup detection and terrorist intelligence analysis. The techniques make also use of centrality measures combined with data mining techniques to find the hierarchy of a group and the leader of the group. Fox and co-authors to have employed hybrid AHP and TOPSIS methods for the identification of key nodes in the network in [16].Also, recent works like [15] have suggested methods for the ranking of each node and determination of the most important path through the network.

PROMETHEE was presented by J.P. Brans in 1982 [10]. Subsequently, many researches like [13] and [14] worked on its application in varied fields.

In this paper we implement the PROMETHEE decision making model to find the key node in the 26/11 Mumbai attack network.

3. Methodology

The PROMETHEE I (partial ranking) and PROMETHEE II (complete ranking) were developed by J.P. Brans and presented in 1982. A few years later J.P. Brans and B. Mareschal developed PROMETHEE III (ranking based on intervals) and PROMETHEE IV. They proposed the visual interactive module GAIA in 1988. In 1992 and 1994, J.P. Brans and B. Mareschal further suggested two extensions: PROMETHEE V (MCDA including segmentation constraints) and PROMETHEE VI (representation of the human brain). The application of the PROMETHEE methodology has been successful in various fields such as Industrial Location, Mines, Water resources, Investments. The success of the methodology is due to its mathematical properties, its uncomplicated approach and excellent software support.

PROMETHEE II is a well-known MCDM technique. It requires information about the weights of the criteria and the preference function which characterizes the contribution of the alternatives when comparing it with respect to each criterion. It is suitable for single as well as multidimensional decision making problems. Tradeoffs between the alternatives are avoided and complete rankings are provided by PROMETHEE II. Following is the stepwise description of PROMETHEE II.

1) From the decision problem we obtain a set of attributes A and a set of criteria C on the basis of which we evaluate the alternatives. Weights are assigned for each criterion to specify their relative importance.
2) The deviation between the values of two alternatives on a particular criterion, d_j (a, b) = c_j (a) – c_j (b) is calculated for all possible pair of alternatives. Here c_j (a) is the value of the attribute a corresponding to criterion j.
3) In PROMETHEE we define a preference function P_j (a, b) = f [d_j (a, b)] where a, b belong to A.

- This function depicts the preference of an alternative over another alternative by assigning a real number between 0 and 1.
- There are six types of preference functions proposed for the evaluation [12].
- The decision maker can choose any preference function for a criterion.
- For example, for the usual case if cj(a) > cj(b) that is d(a, b)>0 then Pj (a, b) = 1 and if cj(a) < cj(b) that is d(a, b)<0 then Pj (a, b) = 0 , as shown in Fig 1

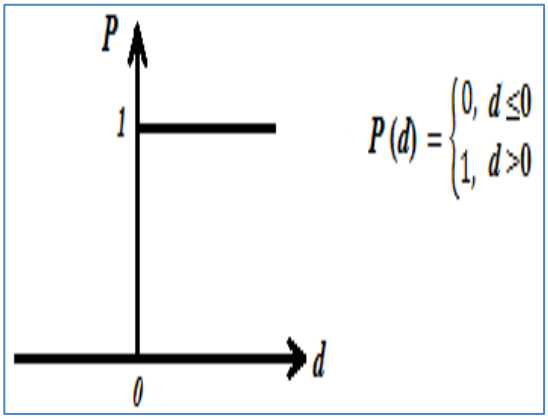

Fig. 1: Type 1 Usual Preference Function.

1) After deciding the preference function the Aggregate Preference Indices is calculated which expresses the degree with which a is preferred to b.

$$\pi(a, b) = \sum_{j=1}^{k} P(a, b).w_j$$

Here w_j is the weight of criterion j.

2) Next the outranking flows are calculated. The Positive outranking flow gives how a is outranking others. Higher the Φ^+(a) better the alternative.

$$\Phi^+(a) = \frac{1}{n-1} \sum_{x \in A} \pi(a, x)$$

The Negative outranking flow gives how a is outranked by others.

$$\Phi^-(a) = \frac{1}{n-1} \sum_{x \in A} \pi(x, a)$$

3) Finally, the Net Outranking Flow

$$\Phi(a) = \Phi^+(a) - \Phi^-(a)$$

Provides the complete ranking of the alternatives.
Higher the Φ (a), better the alternative.

4. Method implementation and results

In this paper we examine the 26/11 Mumbai Attacks dataset [1]. After analysis the government of India's report [18], it is found that satellite phones were being used by attackers. Attackers used to talk their masters in Pakistan. The phone conversations between these attackers and remote masters in Pakistan were interpreted by Indian government and are given in the report [18]. Binary relationships between the attackers and the masters are shown in Table 1

With the help of ORA–LITE software the data is visualized as a network [Fig 2] and various centrality measures are calculated for all the alternatives. Amongst the 13 terrorists, PROMETHEE is applied taking 4 alternatives namely Wassi, Hafiz Arshad, Zarar and Abdul Rehman and the results are visualized using the Visual PROMETHEE software. This paper does not suggest any specific method for the subset selection or reduction of graph. The selection of the alternatives is based on the ORA-LITE rankings.

Table 1: 26/11 Mumbai Attacks Dataset

	Abu Kaahfa	Wassi	Zarar	Hafiz Arshad	Javed	Abu Shoaib	Abu Umer	Abdul Rehman	Fahadullah	Baba Imran	Nasir	Ismail Khan	Ajmal Amir Kasab
Abu Kaahfa	0	1	1	0	0	0	0	1	0	0	0	0	0
Wassi	1	0	1	1	0	0	1	0	0	1	1	0	0
Zarar	1	1	0	0	0	0	0	0	1	0	0	0	0
Hafiz Arshad	0	1	0	0	1	1	1	0	0	0	0	0	0
Javed	0	0	0	1	0	1	1	0	0	0	0	0	0
Abu Shoaib	0	0	0	1	1	0	1	0	0	0	0	0	0
Abu Umer	0	1	0	1	1	1	0	0	0	0	0	0	0
Abdul Rehman	1	0	0	0	0	0	0	0	1	0	0	0	0
Fahadullah	0	0	1	0	0	0	0	1	0	0	0	0	0
Baba Imran	0	1	0	0	0	0	0	0	0	0	0	0	0
Nasir	0	1	0	0	0	0	0	0	0	0	0	0	0
Ismail Khan	0	0	0	0	0	0	0	0	0	0	0	0	1
Ajmal Amir Kasab	0	0	0	0	0	0	0	0	0	0	0	1	0

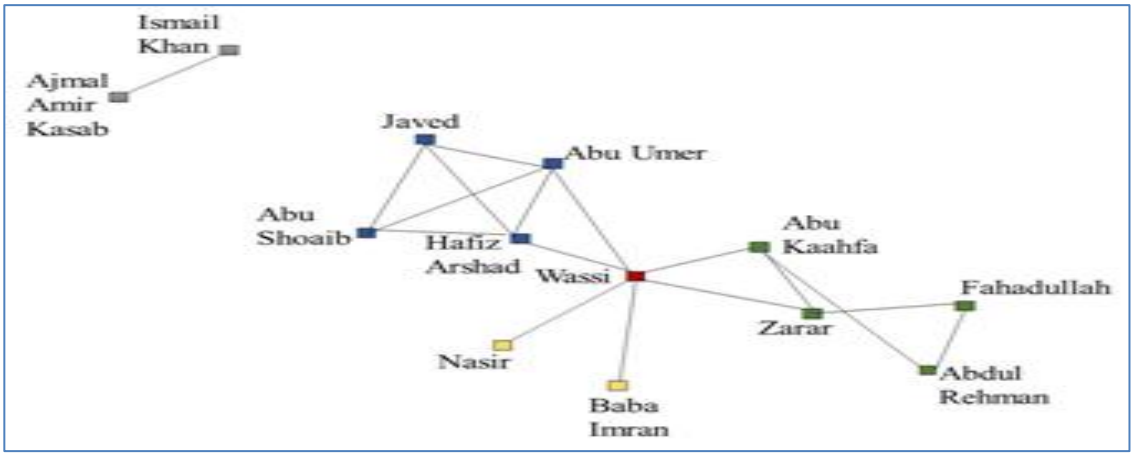

Fig. 2: (26/11) Mumbai Attacks Network.

Following are the criteria used for evaluation.

1) Betweenness Centrality (BC): quantifies the number of times a node acts as a bridge along the shortest path between two other nodes. A node with a higher Betweenness Centrality has more control over the network, as more information passes through that node. It can thus be a potential target to disrupt a terrorist network.
2) Closeness Centrality (CC): Closeness Centrality of a node can be considered as the inverse of the sum of distances in the network from a node to all other nodes. Thus, the more central a node is, the closer it is to all other nodes.
3) Eigenvector Centrality (EC): Eigenvector Centrality is a measure of the influence of a node in a network. It assigns relative scores to all nodes in the network based on the concept that connections to high-scoring nodes contribute more to the score of the node in question than equal connections to low-scoring nodes.
4) PageRank Centrality (PC): PageRank of a node can be interpreted as the fraction of times a node would be visited when traversing the network according to the network of probabilities. PageRank of a node is determined by the number of links it receives, the link propensity of the linkers, and the centrality of the linkers.
5) Efficiency (EF) is the fraction of nodes in an ego network that are not redundant. Here ego network is a network surrounding one particular node and its immediate contacts.

Problem structure is defined well in Fig 3 in the form of Goal, Criteria and Alternatives.

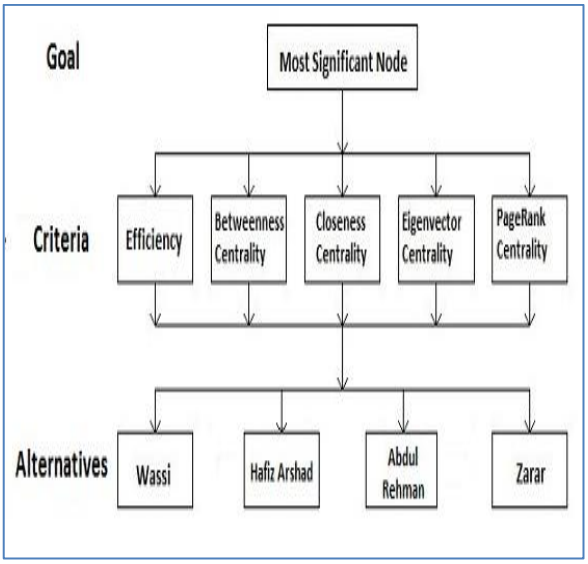

Fig. 3: Decision Problem Structuring.

The measure calculations are arranged in Table 2

Table 2: Evaluations on the Basis of Criteria

	BC	CC	EC	PC	EF
Weight	0.4	0.1	0.2	0.2	0.1
Wassi	0.409	0.194	0.532	0.198	0.778
Hafiz Arshad	0.095	0.188	0.546	0.113	0.125
Zarar	0.057	0.176	0.247	0.084	0.556
Abdul Rehman	0.004	0.231	0.097	0.020	1.000

The deviations between the values of alternatives on a particular criterion for all possible pair of alternatives are displayed in Table 3.

Table 3: Deviations

Deviations between Alternatives	BC	CC	EC	PC	EF
c(Wassi)-c(HA)	0.314	0.006	-0.014	0.085	0.653
c(Wassi)-c(Zarar)	0.352	0.018	0.285	0.114	0.222
c(Wassi)-c(AR)	0.405	-0.037	0.435	0.178	-0.222
c(HA)-c(Zarar)	0.038	0.012	0.299	0.029	-0.431
c(HA)-c(AR)	0.091	-0.043	0.449	0.093	-0.875
c(Zarar)-c(AR)	0.053	-0.055	0.150	0.064	-0.444

We define the usual case preference function for all the criteria that is, for d (a, b)>0, P_j (a, b) = 1 and for d (a, b)<0 , P_j (a, b) = 0. Using the preference function values the Aggregate Preference Indices are computed as displayed in Table 4

Table 4: Aggregate Preference Indices

Deviations between Alternatives	π(a, b)
c(Wassi)-c(HA)	0.80
c(Wassi)-c(Zarar)	1.00
c(Wassi)-c(AR)	0.80
c(HA)-c(Wassi)	0.20
c(HA)-c(Zarar)	0.90
c(HA)-c(AR)	0.80
c(Zarar)-c(Wassi)	0.00
c(Zarar)-c(HA)	0.10
c(Zarar)-c(AR)	0.80
c(AR)-c(Wassi)	0.20
c(AR)-c(HA)	0.20
c(AR)-c(Zarar)	0.20

The Positive and Negative outranking values are displayed in Table 5 and Table 6 respectively.

Table 5: Positive Outranking Flow

	Φ^+(a)
Wassi	0.86
Hafiz Arshad	0.63
Zarar	0.30
Abdul Rehman	0.20

Table 6: Negative Outranking Flow

	Φ^-(a)
Wassi	0.13
Hafiz Arshad	0.36
Zarar	0.70
Abdul Rehman	0.80

The Net Outranking Flows are shown in Table 7 which provides the complete ranking of the alternatives.

Table 7: Net Outranking Flows

	Φ (a)
Wassi	0.73
Hafiz Arshad	0.27
Zarar	-0.4
Abdul Rehman	-0.6

The following is obtained using the Visual PROMETHEE software [Fig 4]. The graph depicts the four alternatives in order of their rankings along with the corresponding net outranking values.

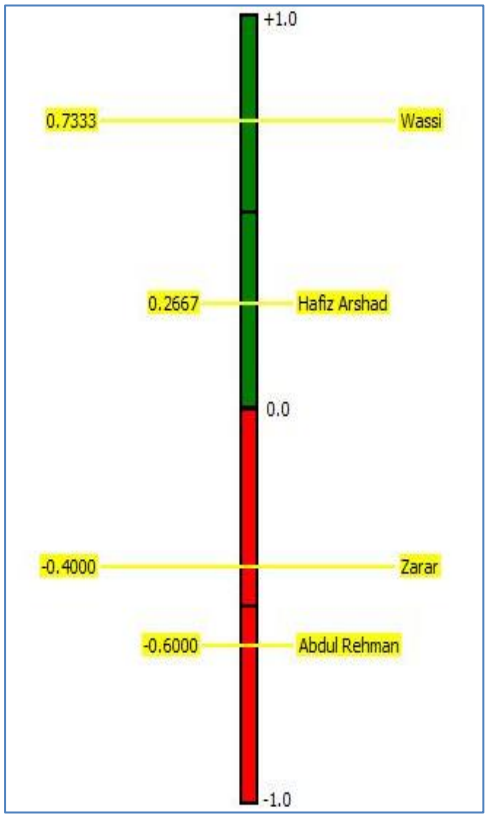

Fig. 4: Node Rankings.

Thus, according to the net outranking values we find that Wassi has the highest ranking. One more thing to be analyzed here that after dismissal of Wassi, Hafiz Arshad was ready to play role of Wassi.

5. Conclusion

In this work we present a technique for finding the pivotal node in a terrorist network. The approach involved the application of PROMETHEE taking various centrality measures as the criteria.
For the 26/11 Mumbai attack network the result suggests that Wassi was the most central and controlling actor which is congruent with the reports [17] and data released by the government [18].
Thus the suggested method can be used to design counterterrorism strategy which focuses on the key node and its ego network to achieve maximum disruption of the network.

References

[1] Sarita Azad and Arvind Gupta, "A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis" Journal of Terrorism Research, Volume 2, Issue 2, November 2011. https://doi.org/10.15664/jtr.187.

[2] M.E.J Newman, Networks: An Introduction, Oxford University Press, 2010. https://doi.org/10.1093/acprof:oso/9780199206650.001.0001.

[3] M. K. Sparrow. The application of Network Analysis to criminal intelligence: An assessment of the prospects. 1991. Social Networks. Esevier13, 251-274.

[4] V.E.Krebs. Mapping networks of terrorist cells. 2002. Connections 24(3): 43-52 International Network for Social Network Analysis.

[5] S. Wasserman and K. Faust. Social Network Analysis: Methods and Applications, Addison-Wesley, 1994. https://doi.org/10.1017/CBO9780511815478.

[6] Nasrullah Memon, Henrik Legind Larsen, David L. Hicks, and Nicholas Harkiolakis. Detecting Hidden Hierarchy in Terrorist Networks: Some Case Studies. Springer-Verlag, pages 477–489, 2008. Proceedings of the IEEE ISI 2008 PAISI, PACCF, and SOCO international workshops on Intelligence and Security Informatics.

[7] Nasrullah Memon, David L. Hicks, and Henrik Legind Larsen. How Investigative Data Mining Can Help Intelligence Agencies to Discover Dependence of Nodes in Terrorist Networks. In Proceedings of the 3rd international conference on Advanced Data Mining and Applications ADMA '07, pp. 430–441, Berlin, Heidelberg, 2007. Springer-Verlag. https://doi.org/10.1007/978-3-540-73871-8_40.

[8] Jennifer Xu and Hsinchun Chen. Criminal network analysis and visualization. Commun. Association for Computing Machinery, 48:100–107, June 2005. https://doi.org/10.1145/1064830.1064834.

[9] Ala Berzinji, Lisa Kaati, Ahmed Resine, Detecting Key Players in Terrorist Networks. European Intelligence and Security Informatics Conference (EISIC), 2012. https://doi.org/10.1109/EISIC.2012.13.

[10] Brans J.P., Lingenierie de la decision. Elaboration dinstruments daide a la decision. Methode PROMETHEE. In: Nadeau, R., Landry, M. (Eds.), Laide a la decision: Nature, instruments et perspectives davenir, Presses de lUniversite Laval, Quebec, Canada. pp. 183-214, 1982.

[11] De Keysar, Keyser, W., Peeters, P., A note on the use of PROMETHEE multi criteria methods. European Journal of Operational Research 89, 457–461, 1996. https://doi.org/10.1016/0377-2217(94)00307-6.

[12] Brans J.P. and Ph. Vincke A preference ranking organization method: The PROMETHEE method. Management Science Vol. 31, 647–656, 1985 https://doi.org/10.1287/mnsc.31.6.647.

[13] Gilles D'Avignon and Bertrand Mareschal. Specialization of Hospital Services in QUEBEC: An application of the PROMETHEE and GAIA methods. Mathl Cornput. Modelling, Vol. 12, No. 10/l1, pp. 1393-1400, 1989.

[14] VTomic, Danijel Markovic, Miomir Jovanovic. Application of PROMETHEE method on decision process in mines, International Journal of Engineering, pp. 79-84, 2013.

[15] Saurabh Singh, Shashikant Verma, Akhilesh Tiwari, Divyani Indurkhya and Aditya Tiwari. An Innovative Investigation on the Importance of Link in Terrorist Network Using Prim's Algorithm (Anti - Terrorism Approach), In Proceedings of International Conference on Recent Developments in Engineering, Science and Management, 2017.

[16] Fox, William P., and Sean F. Everton. 2014. "Using Mathematical Models in Decision Making Methodologies to Find Key Nodes in the Noordin Dark Network." American Journal of Operations Research, 4, pp. 255-67. https://doi.org/10.4236/ajor.2014.44025.

[17] Rahi Gaikwad, Mumbai attackers made two earlier attempts: Headley, The Hindu, February 8, 2016.

[18] A report on Mumbai attack, "Mumbai terrorist attack (Nov. 26-29, 2008)", Govt. of India, 2009.