ISSN 2348-8565
Volume 10 Issue 1 | March 2022
ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

Identifying the Most Significant Node in a Terrorist Network Using a Minimized-Graph Analytical Hierarchy Process

Saurabh Singh
Department of Computer Science and Engineering
Jabalpur Engineering College
Jabalpur, (M.P.) India
Email: ssingh@jecjabalpur.ac.in@gmail.com

Madhuri Gokhale
Department of Computer Science and Engineering
Jabalpur Engineering College
Jabalpur, (M.P.) India
Email: mgokhale@jecjabalpur.ac.in@gmail.com

Abstract*—Communication networks connecting the people involved in planning and executing a terrorist attack, commonly termed terrorist networks, can be modelled as graphs in which individuals are vertices and their communications are edges. Identifying the most significant individual in such a network can give authorities a clear target for investigation and disruption. This paper proposes a method that combines graph reduction with the Analytical Hierarchy Process (AHP) to identify the most significant node in a terrorist network. Nodes are first ranked by degree and betweenness, and the network is reduced to fewer than half its original size to limit computation. Five centrality measures—Total Degree Centrality, Betweenness Centrality, Closeness Centrality, Eigenvector Centrality, and PageRank Centrality—are then computed for the remaining nodes and combined through a weighted fitness function using AHP pairwise comparisons to produce an overall priority score for each node. The method is demonstrated on the terrorist network involved in the 26/11 Mumbai attacks, correctly identifying the individual known to have played the most central operational role. The approach reduces the computation required to reach an actionable conclusion and can be applied more broadly to significant-node detection in other social networks.*

Keywords:*—Terrorist Networks, Covert Networks, Social Networks, Graph, Analytical Hierarchy Process (AHP), Degree, Centrality, Total Degree Centrality, Betweenness Centrality, Closeness Centrality, Eigenvector Centrality, PageRank Centrality.*

1. INTRODUCTION

Terrorism has become a widespread issue in the present world. Every now and then, we hear of an attack spreading terror and panic and leading to a huge loss of life and property. A majority of these attacks and activities are orchestrated by full-fledged organizations who use these to spread their anti-social agenda. These organizations comprise of thousands of people spread across countries and continents who come together due to their beliefs.

Communication is of prime importance to these terrorist organizations. It allows for them to exchange information, instructions, resources and even ideas critical to their plan.

However, unfortunately in this case, connectivity is achieved with an astonishing level of ease nowadays. The technological advancement of the world in the areas of communication has its drawbacks in conveniently connecting people with hostile intentions. The availability of cheap and viable communication makes it easier for terror figures to gather all forms of required

information, make plans and even execute them without stepping out of their safe havens. For any form of terrorist activity, a network of people involved, planners and executers alike, is always present to facilitate moving the plans to completion.

These networks, termed as "terrorist networks" are at the heart of nearly all modern terrorist activities. They are special forms of social network with emphasis on both secrecy and efficiency. These are the networks that represent communication links connecting the various people involved in the planning and execution of a terrorist attack. They are generally formed from communication networks like the internet, cellular networks etc. and mobile and stationary nodes comprising of cellphones, computers and other intelligent communication devices.

Terrorist networks generally adhere to the definition of a covert network. A covert network is a network which has some elements of secrecy about it. The members of these networks may keep their identities secret or the networks may form around secret activities. In the case of a terrorist network, the important members' identities are generally protected through aliasing or use of disposable devices. This is one of the most important features of a terrorist network as it allows the plans and the people involved to stay hidden from authorities.

Terrorist networks are very complex structures with many people involved and varied levels of communication between them. The network is not a hierarchical structure with heads on upper levels and subordinates on lower. It is more of a flat structure where importance of people depends on their level of connectivity in the network. The more important a person is on a terrorist network; the more amount of information can be extracted from him or her and the more critical he or she becomes for capturing.

Being part of a terrorist network does not necessarily mean that a person is a terrorist. However, it does highlight the possible suspects who have been in contact with the people involved in the attack. This is what makes these networks so important, because they give the authorities a direction for their investigation.

Apart from deciding the course of investigation, a terrorist network also helps in determining the structure of a terrorist organization. It can identify decision makers, communicators, planners, recruiters and people playing various other important roles in the group. Determining the hierarchy of the organization, however irrelevant it may seem, can help a great deal when we deal with terrorist activities, as removing the upper levels can immediately cripple the whole organization.

The identification and analysis of terrorist networks can not only help in avoiding a potential disaster and loss of many precious lives but can also help authorities catch people who wish to disrupt the peace of society for their personal gains and dangerous propaganda. Furthermore, their study can help establish patterns which can help in quick detection and avoidance of potential future cases. This is what makes their analysis so critical.

Study of terrorist networks has gained popularity in the recent years. The study is motivated by the unprecedented increase in terrorist activities. The 21st century has been marred by a number of disturbing attacks which have resulted in the deaths of thousands of people and have left countless others scarred for life. Even though the study and analysis cannot bring back those who died, it can save many others from the same fate and can help bring justice to the families of the deceased.

The first widespread use of the term "terrorist network" came after the 9/11 terrorist attacks in United States in 2001., which happens to be one of the most popular terrorist attacks in history. The day involved a collection of four highly coordinated hijacks

and attacks orchestrated by the terrorist group Al-Qaeda which resulted in close to 3000 deaths and destruction of the famous World Trade Center. The study of the attack revealed that the terrorists were in close contact with each other. The information revealed from the study helped United States government in capturing many important faces of terror in later years.

Another infamous attack is the 26/11 attack in Mumbai, India. The three days long attack involved shooting and bombing at some of the most famous and busiest spots in the city and crippled the financial capital of the country. It was later revealed that it was made possible by an intricate terrorist network which facilitated information exchange, training of terrorists and even funding required for the operation. The study of the network brought to the attention of the authorities the fact that the attackers were being given constant instructions by their superiors. These instructions guided their whole course of action and resulted in the nearly 200 killings and 300 injuries.

The 7/7 bombings in London are another name in the series of most disturbing attacks by terrorists. The attack, which took place in 2005 comprised of a series of coordinated suicide bombings targeted at the public transportation systems. The fact that three of the four bombers were British reveals how important a role these networks play in spreading the agenda of their organizations. The network was used to identify potential attackers and provided them with information to use the explosives along with the instructions of the attack. The bombing is regarded as the biggest attack of the nation.

There are thousands of other instances when terrorists have wreaked havoc on innocent lives for their personal vendetta. The Besan School Hostage Crisis of 2004, Peshawar School Massacre of 2014, Norway Attacks of 2011, Dubrovka Theatre Siege of 2002, Madrid Train Bombings of 2004 are just a few in a long list of heinous attacks against innocent lives. Their studies have shown that none of these attacks could have been possible without the elaborate networks connecting the people responsible. It would not be wrong to say that no part of the world is safe from terror.

These studies have revealed that terrorist networks play the key role in the orchestration and subsequent execution of terrorist activities. Without communication, the terrorists are just individuals with an anti-social ideology who can be easily dealt with by the authorities. Thus, the identification and analysis of terrorist networks is a priority to maintain the peace in world and to make it a safer place to live in.

Computers have become an important part of any form of analysis today. Like in every other field, computers play a major role in investigation of terrorist and criminal activities. Their capability of processing huge amounts of information and drawing fast and accurate insights from it makes them an integral part of investigation agencies. Even apart from the computational power, the concepts of mathematics and computer science which are so easily representable with computers can help in a more efficient and concrete study of terrorist networks.

Graph theory holds a significant position in both computer science and mathematics. It constitutes the study of graphs, which are mathematical structures to model pairwise relations between objects. A graph consists of two main elements: vertices, which represent objects in space and edges, which signify the connection between those objects. The edges may or may not have specified directions and may or may not have weights which determine their relevance in the graph.

The terrorist networks can be very conveniently modelled through graphs with terrorists represented as vertices while their communications can be represented as edges. With this form of modelling, we can easily determine the important people in the network by just the analysis of the degree of vertices.

Furthermore, it can be determined who acts as the middleman between two people. These middlemen, if removed can break the communication links and avoid potential attacks. Apart from the plain analysis, the algorithms of graph theory can give the authorities some important, less obvious insights into the whole structure of the network which can help them in planning their course of action. Graph theory, thus, facilitates an easier and acute analysis of terrorist networks.

In this paper, we use Analytical Hierarchy Process (AHP) on a minimized terrorist network to determine the most important node in the network. AHP which is used for analyzing complex decisions based on multiple criteria can help in determining the most critical node of a terrorist network through simple calculations. We decide a "fitness function" – which specifies which criteria is more important to us than the other. We also minimize the graph by removal of less important nodes. This would help in reducing the amount of calculation required. The node selected after applying AHP can then be used by authorities to determine the appropriate action. It can thus help authorities by providing them a target to focus on.

2. LITERATURE SURVEY

Terrorist Network analysis has been in constant limelight since the 9/11 attacks. As the terrorist organizations have expanded and become more efficient, counter-terrorist forces have also developed in response. Researchers are coming up with new methods to fight against the hostile forces. Some of these contributions are highlighted in this section.

Social network data is usually owned by different organizations. Therefore, for getting a complete picture of the network for analysis, integration of this data is required which is difficult as organizations have to hold back information due to privacy concerns. Tang and Yang [1] addressed this issue by proposing generalization algorithms which allow an organization to generalize its part of the network, holding back sensitive information while still making useful data available. They proposed creation of subgraphs and then generalization of these subgraphs. These generalized subgraphs would hold relevant insensitive information. The generalized network of organizations can now be integrated to form a global network which can be analyzed effectively.

Li et al. [2] used a combination of Social Network Analysis (SNA), Multi-meta Network Analysis and Fuzzy Analytical Network Process (FANP) to detect key individuals in a terrorist network. They propose creating an index system and then within the system, calculating the scores of the various terrorists involved which reference the measures in the network which are calculated by the network analysis tools. Using artificial judgment and fuzzy science, it is a good method when information available is uncertain, as is the case of terrorist networks. It can be helpful to authorities in detecting important individuals for counter-terrorist process.

On the other hand, Dawoud et al. [3] proposed an effective way of discovering and predicting terrorist networks. They argued that measuring the degree of organization of the whole network through SNA measures like degree, betweenness and closeness; without focusing on individuals involved would help in faster discovery of these networks. With time, even terrorists' intelligence has grown and they now have efficient means to hide individuals. Therefore, focusing on the network organization is more practical as more organized terrorist networks are more dangerous. Furthermore, knowledge of network structure can help authorities develop strategies.

Ozgul, Erdem and Bowerman [4] developed Crime Prediction Model (CPM) to predict individuals or organizations responsible for unsolved terrorist activities. CPM first creates clusters of the various terrorist activities based on similarities such

as time, location, modus operandi etc. These clusters are then given to classification module, which then places similarly behaving crimes together. If these clusters then have majority of solved crimes, then the individuals responsible are regarded as responsible for the unsolved crimes in that cluster. This system can help authorities determine culprits easily.

With the growing popularity of Internet, even terrorists are using it for spreading their ideologies. Dark Web is a part of internet which serves as a hotspot where they can communicate their messages. Therefore, dark web analysis can be an effective method for counter- terrorism by detection and avoidance of threats. Sachan [5] proposed a dark web analysis model which collects data from dark web forums and creates tables of message posters based on their activity levels. Every entry is then checked for message vulnerability and a table of vulnerable posters is created. The model then analyses links between posts and posters to discover hidden patterns and generate warnings. The method can play an important role in counter-terrorism.

Terrorist network analysis has predominantly focused on the analysis of nodes in the network. Wiil et al. [6] proposed a method to analyze the importance of links in a terrorist network. The method, inspired by transportation networks, measures the performance and the change in link betweenness of the network with and without the link. These are then multiplied to calculate link importance. The removal of a link with higher importance will quickly destabilize the network and help authorities avoid terrorist attacks.

A terrorist network is not a static entity. It reshapes itself and people involved get replaced by other suitable candidates when needed. Spezzano et al. [7] leveraged the solution of Person Successor Problem to predict the person who replaces an individual in a terrorist network and to decide which set of individuals should be replaced to minimize the network lethality. Their method involves calculating the replacement probability of candidate nodes which can replace a given node. Moreover, the propose calculation of lethality of the network before and after replacement to significance determine most suitable candidates to target. This can help maim a terrorist network efficiently.

3. METHOD

New forms of interactive, community-oriented media have evolved on the internet in recent years. These generate a lot of complex data in public domain. Schreck and Keim [8] proposed visual analysis of this social media data. This approach combines computational data analysis with interactive visualization to create effective data analysis systems which can help in getting deeper insights into social networks.

Terrorist networks are naturally bipartite, where individuals represent one node set, while common actions, events or affiliations represent the other node set, through which links between individuals are inferred. Alzahrani and Horadam [9] applied the SNA tool of community detection to two criminal bipartite networks, through the approach of weighted projection into a random-walk based algorithm, Infomap. They found that the communities extracted by Infomap on the weighted primary network projected from the bipartite network reflect valuable and meaningful information in the bipartite network framework.

One of the most important parts of a terrorist organization is its finance network which provides funding for the various activities of the organization. Sakharova [10] examined terrorist financing, particularly Al Qaeda's financing and determined how information technology can be used to detect and disrupt these financial networks. She proposes the use of modified data mining to uncover hidden dependencies in the uncertain and inaccurate finance networks of the organization. These hidden dependencies can then be removed to cripple the terrorist

organization.

Growing hostility towards terrorist organizations has led to cooperation between them. Similar terrorist organizations frequently exchange information and resources to coordinate attacks. Ozgul, Atzenbeck and Erdem [11] proposed the use of Crime Ontology Similarity Measure to calculate how similar two terrorist networks are. A crime ontology is created in which a terrorist group, with all of its attacks and modus operandi skills, can be represented as a node, and overall ontology can be represented as a graph. It is then possible to use such crime ontology to guess the extent of similarity and relationship between terrorist groups. Foreseeing possible cooperation can help authorities in avoid possible catastrophes.

We are not aware of any research that uses AHP on a minimized graph to determine the most significant node. We are using a predetermined fitness function as the criteria through which we can determine the relative priority of the nodes. Applying the method on a reduced graph can help give faster results as matrix size is reduced. Therefore, this method can help reduce the calculation involved in determining node

AHP is one of the most widely used decision making approach in the world. Developed my Thomas L. Saaty in 1970s, it has been extensively studied and enhanced since then. It has particular application in group decision making, and is used around the world in a wide variety of decision situations, in fields such as government, business, industry, healthcare, shipbuilding and education.

Rather than prescribing a "correct" decision, the AHP helps decision makers find one that best suits their goal and their understanding of the problem. It provides a comprehensive and rational framework for structuring a decision problem, for representing and quantifying its elements, for relating those elements to overall goals, and for evaluating alternative solutions.

The AHP methodology compares criteria, or alternatives with respect to a criterion, in a natural, pairwise mode. To do so, the AHP uses a fundamental scale of absolute numbers that has been proven in practice and validated by physical and decision problem experiments. It converts individual preferences into ratio scale weights that can be combined into a linear additive weight w(a) for each alternative a. The resultant w(a) can be used to compare and rank the alternatives and, hence, assist the decision maker in making a choice.

We are employing Analytical Hierarchy Process (AHP) in our method to determine the most significant node in a reduced terrorist network based on a predetermined fitness function. The node selected after application of AHP can be used by authorities to take appropriate action.

We are ranking the nodes in terrorist network based on certain criteria. For this paper, we are using a few graph centrality measures as criteria, namely, Total Degree Centrality, Betweenness Centrality, Closeness Centrality, Eigenvector Centrality and PageRank Centrality.

The Total Degree Centrality of a node is the normalized sum of its row and column degrees. Degree is a simple centrality measure that counts how many neighbors a node has. A node with higher number of neighbors is more significant because it has more connections to other nodes in the network. In a terrorist network, this might mean that a person with higher Total Degree Centrality has more information about the network and its operations.

Betweenness Centrality 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.

The Closeness Centrality of a node is calculated as the sum of the length of the shortest paths between the node and all other nodes in the graph. Thus, the more central a node is, the closer it is to all other nodes. It can be loosely considered as the inverse of the sum of distances in the network from a node to all other nodes.

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. Individuals or organizations who are connected to many otherwise isolated individuals or organizations will have a much lower score in this measure then those that are connected to groups that have many connections themselves.

PageRank Centrality is the importance of a node based on the importance of its in-coming neighbors. The input network links are normalized and interpreted as the probability of a transition from node i to node j. The 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.

The foremost requirement of our method is to have the measures of the chosen criteria for all nodes in the terrorist network. We need to calculate the values of criteria like Total Degree Centrality, Betweenness Centrality etc. for the nodes in our graph. These values will be required in later steps. Our method only requires the values for comparison purposes, hence, we shall not recommend any specific algorithm for calculation of these values. Any suitable algorithm may be applied for these computations.

The next step in our method is to reduce the graph. This involves removal of less significant nodes from the graph on the basis of degree and betweenness. Our aim in this step is to reduce the number of nodes in the graph to less than n/2, where n is the original number of nodes in the terrorist network graph. We rank the nodes based on their degree and betweenness and then choose the top nodes in the table. This helps in reducing the amount of calculation involved in the process.

Now, we have to set up a fitness function. This involves deciding the importance of the various criteria. While making a decision, some criteria might have more weightage than others. For example, if we are to determine the most important person in a terrorist network, betweenness of the node may be considered most important. So, we decide the percentage weightage of each criteria in this step. This depends on individual requirement of every case.

Now we are ready to apply AHP to the network nodes. The first step in the AHP is represent the problem in terms of the overall goal, the criteria, and the decision alternatives. Our overall goal is to determine the most important node in the terrorist network, the criteria can be Betweenness Centrality, Closeness Centrality etc. and our alternatives are the different nodes.

Next step is the pairwise comparison of nodes for each criterion. For this comparison, the AHP employs an underlying scale with values from 1 to 9 to rate the relative preferences for two items. It is described as follows:

Table 1: Verbal Description of Various Preference Ratings

Verbal Judgment of Preference	Numerical Rating
Extremely preferred	9
Very strongly to extremely preferred	8
Very strongly preferred	7
Strongly to very strongly preferred	6
Strongly preferred	5
Moderately to strongly preferred	4
Moderately preferred	3
Equally to moderately preferred	2
Equally preferred	1

Element $C_{i,j}$ of the matrix is the measure of preference of the item in row i when compared to the item in column j. AHP assigns a 1 to all elements on the diagonal of the pairwise comparison matrix, as when we compare any alternative against itself (on the criterion) the judgment must be that they are equally preferred. AHP obtains the preference rating of $P_{j,i}$ by computing the reciprocal (inverse) of $P_{i,j}$ (the transpose position).

We make this comparison based on the calculated values of nodes for each criterion. The calculated values can be mapped onto a scale from 1 to 9 and the nodes can then be compared depending on the distance they lie at from each other on the scale. This is demonstrated below:

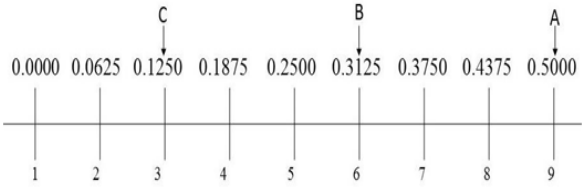

Figure 1: Preference Rating Comparison Example Scale

For example, if the value of Total Degree Centrality for node A is 0.500, while for node B is 0.33, then $C_{A,B}$ = 4.as 0.33 would approximately be on 6th position on the scale However, if the value for node C is 0.125, then $C_{A,C}$ = 7. These values depend on the range of values in consideration and also on individual judgement.

The next step is synthesization which is the procedure to estimate the relative priority for each decision alternative in terms of the criterion. The three-step process is as follows:

1. Sum the values in each column of the pairwise comparison matrix.
2. Divide each element in the pairwise matrix by its column total. The resulting matrix is referred to as the normalized pairwise comparison matrix.
3. Compute the average of the elements in each row of the normalized matrix. These averages provide an estimate of the relative priorities of the elements being compared.

The process has to be repeated for all criteria in consideration. Furthermore, we also need to perform pairwise comparison of all criteria and calculate their priorities. The overall priority for each decision alternative is obtained by summing the product of the criterion priority (with respect to the overall goal) times the priority of the decision alternative with respect to that criterion. Ranking these priority values, we will have AHP ranking of the decision alternatives.

The node ranked highest in the ranking is the required node, which requires most attention. It can then be optimized as needed. The node may be the master-mind of the terrorist network, or the gate-keeper. The important point is that the authorities now have a target to focus on and this gives direction for appropriate action.

The algorithm for the process is as follows:

Algorithm 1: Algorithm to find the most significant node in a terrorist network

Input: Terrorist Network Graph G (V, E), List of selected criteria C, Criteria values $CV_{c,v}$ for each node v ϵ V and each criteria c ϵ C

Output: Most significant node x

1: Based on degree and betweenness, reduce the number of nodes to < n/2,

where n is the total number of nodes. Let the new number of nodes be m.

2: Decide Fitness Function. Give percentage importance Ic to all c ϵ C. Let number of criteria be r.

3: **for** every c ϵ C

4: Create pairwise comparison matrix Pc (m X m) based on CVc,v

5: **for** j = 1 to m

6: **for** i = 1 to m

7: sumc, j = sumc,j + Pc[i][j] 8: **for** i = 1 to m

9: **for** j = 1 to m

10: Pc[i][j] = Pc[i][j]/sumc, j

11: **for** I = 1 to m

12: **for** j = 1 to m

13: sumc, i = sumc, i + Pc[i][j]

14: RPc, i = sumc, i/m

15: Create pairwise comparison matrix for criteria M (r X r) based on Ic

16: **for** j = 1 to r

17: **for** i = 1 to r

18: sumj = sumj + M[i][j]

19: 19: **for** i = 1 to r

20: **for** j = 1 to r

21: M[i][j] = M[i][j]/sumj

22: **for** i = 1 to r

23: **for** j = 1 to r

24: sumi = sumi + M[i][j]

25: RPi = sumi/r

26: **for** v = 1 to m

27: **for** c = 1 to r

28: OPv = OPv + (RPc, v X RPc)

29: x = v with highest OPv

30: return x

The flowchart of the process is as follows:

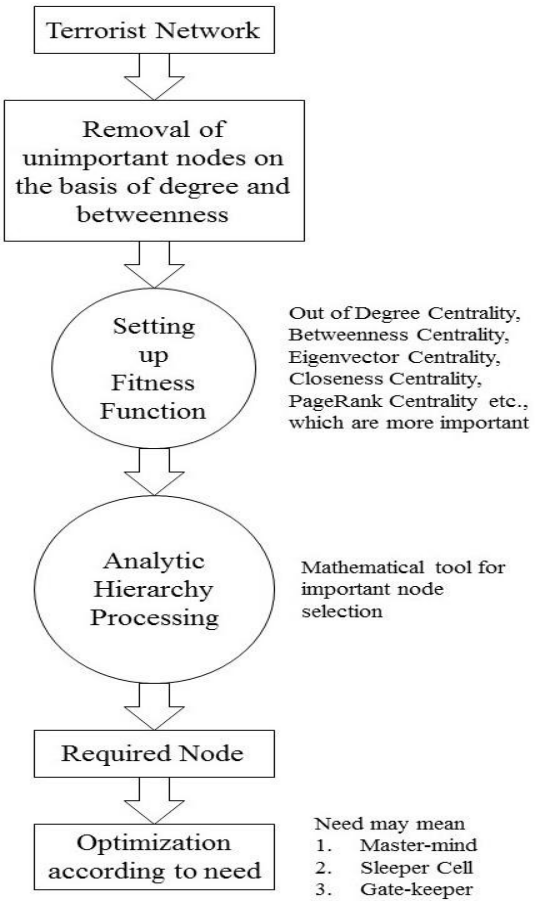

Figure 2: Flowchart

4. RESULTS

In this paper, we are using the terrorist network of 26/11 attacks in Mumbai to demonstrate the application of our method. 26/11 attacks are regarded as one of the biggest terrorist attacks of the modern world. The network image is as follows:

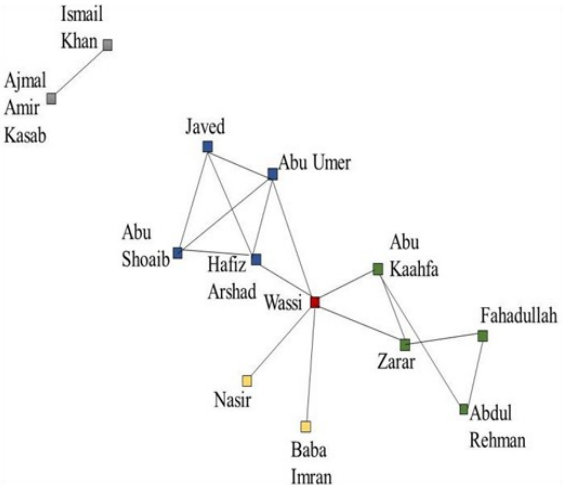

Figure 3: Network Image of 26/11 Terrorist Attacks in Mumbai

We are considering five criteria on the basis of which to determine the most significant node. They are:

- Total Degree Centrality
- Betweenness Centrality
- Closeness Centrality
- Eigenvector Centrality
- PageRank Centrality

The measures of these centrality for each node of the graph is as follows:

The Total Degree Centrality of the nodes is as follows:

Table 2: Total Degree Centrality of nodes in Flowchart.

Node	Total Degree Centrality
Wassi	0.500
Abu Umer	0.333
Hafiz Arshad	0.333
Abu Kaahfa	0.208
Abu Shoaib	0.208
Javed	0.208
Zarar	0.208
Abdul Rehman	0.125
Fahadullah	0.125
Ajmal Amir Kasab	0.083
Baba Imran	0.083
Ismail Khan	0.083
Nasir	0.083

The Betweenness Centrality of the nodes is as follows:

Table 3: Betweenness Centrality of nodes in Flowchart.

Node	Betweenness Centrality
Wassi	0.409
Abu Umer	0.095
Hafiz Arshad	0.095
Abu Kaahfa	0.057
Zarar	0.057
Abdul Rehman	0.004
Fahadullah	0.004
Javed	0.000
Abu Shoaib	0.000
Ismail Khan	0.000
Ajmal Amir Kasab	0.000
Nasir	0.000
Baba Imran	0.000

The Closeness Centrality of the nodes is as follows:

Table 4: Closeness Centrality of nodes in Flowchart

Node	Closeness Centrality
Abdul Rehman	0.231
Fahadullah	0.231
Wassi	0.194
Abu Umer	0.188
Hafiz Arshad	0.188
Abu Kaahfa	0.176
Zarar	0.176
Abu Shoaib	0.174
Baba Imran	0.174
Nasir	0.174
Javed	0.171
Ajmal Amir Kasab	0.083
Ismail Khan	0.083

The Eigenvector Centrality of the nodes is as follows:

Table 5: Eigenvector Centrality of nodes in Flowchart

Node	Eigenvector Centrality
Abu Umer	0.546
Hafiz Arshad	0.546
Wassi	0.532
Abu Shoaib	0.429
Javed	0.429
Abu Kaahfa	0.247
Zarar	0.247
Ajmal Amir Kasab	0.154
Ismail Khan	0.154
Baba Imran	0.150
Nasir	0.150
Abdul Rehman	0.097
Fahadullah	0.097

The PageRank Centrality of the nodes is as follows:

Table 6: PageRank Centrality of nodes in Flowchart.

Node	PageRank Centrality
Wassi	0.198
Abu Umer	0.113
Hafiz Arshad	0.113
Abu Kaahfa	0.084
Zarar	0.084
Ajmal Amir Kasab	0.077
Ismail Khan	0.077
Javed	0.076
Abu Shoaib	0.060
Baba Imran	0.040
Nasir	0.040
Abdul Rehman	0.020
Fahadullah	0.020

On the basis of betweenness and degree, the top-ranking nodes (< n/2) are:

1. Wassi
2. Abu Umer
3. Hafiz Arshad
4. Abu Kaahfa
5. Zarar

Now, we remove all the other nodes from consideration as they have a very low chance of being the most significant.

We consider the following fitness function for our calculations:

Table 7: Importance Percentage for Criteria

Criteria	Importance Percentage
Total Degree Centrality	10
Betweenness Centrality	50
Closeness Centrality	20

Mapping these percentage on the preference rating scale and comparing the rating of different criteria, we get the following pairwise comparison matrix:

Table 8: Pairwise Comparison Matrix for Criteria

Criteria (Centrality)	Total Degree	Betweenness	Closeness	Eigen-vector	Page Rank
Total Degree	1.000	0.250	0.500	1.000	1.000
Betweenness	4.000	1.000	3.000	4.000	4.000
Closeness	2.000	0.333	1.000	2.000	2.000

After dividing each element by column total, the matrix changes to:

Table 9: Relative Priority Vector Calculation for Criteria

Relative Priority Vector Calculation for Criteria

Criteria	Total Degree	Between-ness	Close-ness	Eigen-vector	Page Rank	Row Average
Total Degree	0.111	0.120	0.091	0.111	0.111	0.109
Between-ness	0.444	0.480	0.545	0.444	0.444	0.472
Close-ness	0.222	0.160	0.182	0.222	0.222	0.202
Eigen-vector	0.111	0.120	0.091	0.111	0.111	0.109
Page Rank	0.111	0.120	0.091	0.111	0.111	0.109
Total						1.000

Thus, the criteria priority vector is:

After dividing each element by column total, the matrix changes to

$$\begin{bmatrix} 0.109 \\ 0.472 \\ 0.202 \\ 0.109 \\ 0.109 \end{bmatrix}$$

The equation for Fitness Function will therefore be as follows:

$$Overall\ Priority\ of\ Node\ OP = (0.109\ X\ TDC) + (0.472\ X\ BC) + (0.202\ X\ CC) + (0.109\ X\ EVC) + (0.109\ X\ PRC)$$

Where

- TDC is the relative priority vector value of node for Total Degree Centrality
- BC is the relative priority vector value of node for Betweenness Centrality
- CC is the relative priority vector value of node for Closeness Centrality
- EVC is the relative priority vector value of node for Eigenvector Centrality
- PRC is the relative priority vector value of node for PageRank Centrality
- Now we apply AHP for comparison based on each criterion.
- The pairwise comparison matrix for Total Degree Centrality is as follows:

Table 10: Pairwise Comparison Matrix for Total Degree Centrality

Total Degree Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar
Wassi	1.000	4.000	4.000	6.000	6.000
Abu Umer	0.250	1.000	1.000	3.000	3.000
Hafiz	0.250	1.000	1.000	3.000	3.000

After dividing each element by column total, the matrix changes to:

Table 11: Relative Priority Vector Calculation for Total Degree Centrality

Total Degree Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar	Row Average
Wassi	0.545	0.600	0.600	0.429	0.429	0.521
Abu Umer	0.136	0.150	0.150	0.214	0.214	0.173
Hafiz Arshad	0.136	0.150	0.150	0.214	0.214	0.173
Abu Kaahfa	0.091	0.050	0.050	0.071	0.071	0.067
Zarar	0.091	0.050	0.050	0.071	0.071	0.067
Total						1.000

Thus, the relative priority vector for Total Degree Centrality is:

$$\begin{bmatrix} 0.521 \\ 0.173 \\ 0.173 \\ 0.067 \\ 0.067 \end{bmatrix}$$

Table 12: Pairwise Comparison Matrix for Betweenness Centrality

Betweenness Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar
Wassi	1.000	7.000	7.000	8.000	8.000
Abu Umer	0.143	1.000	1.000	2.000	2.000
Hafiz Arshad	0.143	1.000	1.000	2.000	2.000
Abu Kaahfa	0.125	0.500	0.500	1.000	1.000
Zarar	0.125	0.500	0.500	1.000	1.000
Column Total	1.536	10.000	10.000	14.000	14.000

After dividing each element by column total, the matrix changes to:

Table 13: Relative Priority Vector Calculation for Betweenness Centrality

Between-ness Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar	Row Average
Wassi	0.651	0.700	0.700	0.571	0.571	0.639
Abu Umer	0.093	0.100	0.100	0.143	0.143	0.116
Hafiz Arshad	0.093	0.100	0.100	0.143	0.143	0.116
Abu Kaahfa	0.081	0.050	0.050	0.071	0.071	0.065
Zarar	0.081	0.050	0.050	0.071	0.071	0.065
Total						1.000

Thus, the relative priority vector for Betweenness Centrality is:

$$\begin{bmatrix} 0.639 \\ 0.116 \\ 0.116 \\ 0.065 \\ 0.065 \end{bmatrix}$$

The pairwise comparison matrix for Closeness Centrality is as follows:

Table 14 : Pairwise Comparison Matrix for Closeness Centrality

Closeness Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar
Wassi	1.000	1.000	1.000	2.000	2.000
Abu Umer	1.000	1.000	1.000	1.000	1.000
Hafiz Arshad	1.000	1.000	1.000	1.000	1.000
Abu Kaahfa	0.500	1.000	1.000	1.000	1.000
Zarar	0.500	1.000	1.000	1.000	1.000
Column Total	4.000	5.000	5.000	6.000	6.000

After dividing each element by column total, the matrix changes to:

Table 15 : Relative Priority Vector Calculation for Closeness Centrality

Close-ness Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar	Row Average
Wassi	0.250	0.200	0.200	0.333	0.333	0.263
Abu Umer	0.250	0.200	0.200	0.167	0.167	0.197
Hafiz Arshad	0.250	0.200	0.200	0.167	0.167	0.197
Abu Kaahfa	0.125	0.200	0.200	0.167	0.167	0.172

is: Thus, the relative priority vector for Closeness Centrality

$$\begin{bmatrix} 0.263 \\ 0.197 \\ 0.197 \\ 0.172 \\ 0.172 \end{bmatrix}$$

The pairwise comparison matrix for Eigenvector Centrality is as follows:

Table 16: Pairwise Comparison Matrix for Eigenvector Centrality

Eigenvector Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar
Wassi	1.000	1.000	1.000	5.000	5.000
Abu Umer	1.000	1.000	1.000	5.000	5.000
Hafiz Arshad	1.000	1.000	1.000	5.000	5.000
Abu Kaahfa	0.200	0.200	0.200	1.000	1.000
Zarar	0.200	0.200	0.200	1.000	1.000
Column Total	3.400	3.400	3.400	17.000	17.000

After dividing each element by column total, the matrix changes to

Table 17 : Relative Priority Vector Calculation for Eigenvector Centrality

Eigen-vector Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar	Row Average
Wassi	0.294	0.294	0.294	0.294	0.294	0.294
Abu Umer	0.294	0.294	0.294	0.294	0.294	0.294
Hafiz Arshad	0.294	0.294	0.294	0.294	0.294	0.294
Abu Kaahfa	0.059	0.059	0.059	0.059	0.059	0.059

is: Thus, the relative priority vector for Eigenvector Centrality

$$\begin{bmatrix} 0.294 \\ 0.294 \\ 0.294 \\ 0.059 \\ 0.059 \end{bmatrix}$$

The pairwise comparison matrix for PageRank Centrality is as follows:

Table 18 : Pairwise Comparison Matrix for PageRank Centrality

PageRank Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar
Wassi	1.000	4.000	4.000	6.000	6.000
Abu Umer	0.250	1.000	1.000	3.000	3.000
Hafiz Arshad	0.250	1.000	1.000	3.000	3.000
Abu Kaahfa	0.167	0.333	0.333	1.000	1.000
Zarar	0.167	0.333	0.333	1.000	1.000
Column Total	1.834	6.666	6.666	14.000	14.000

After dividing each element by column total, the matrix changes to

Table 19 : Relative Priority Vector Calculation for PageRank Centrality

Page-Rank Centrality	Wassi	Abu Umer	Hafiz Arshad	Abu Kaahfa	Zarar	Row Average
Wassi	0.545	0.600	0.600	0.429	0.429	0.521
Abu Umer	0.136	0.150	0.150	0.214	0.214	0.173
Hafiz Arshad	0.136	0.150	0.150	0.214	0.214	0.173
Abu Kaahfa	0.091	0.050	0.050	0.071	0.071	0.067

is: Thus, the relative priority vector for PageRank Centrality

$$\begin{bmatrix} 0.521 \\ 0.173 \\ 0.173 \\ 0.067 \\ 0.067 \end{bmatrix}$$

Now, we perform pairwise comparison of the various criteria.

Now, accumulating the results, we see that the priority vectors are:

Table 20 : Relative Priority Vectors for Various Criteria

	Total Degree	Betwee n-ness	Close- ness	Eigen- vector	Page Rank
Wassi	0.521	0.639	0.263	0.294	0.521
Abu Umer	0.173	0.116	0.197	0.294	0.173
Hafiz Arshad	0.173	0.116	0.197	0.294	0.173
Abu Kaahfa	0.067	0.065	0.172	0.059	0.067
Zarar	0.067	0.065	0.172	0.059	0.067

Table 21 : Relative Priority Vector of Criteria

	Criterion
Total Degree Centrality	0.109
Betweenness Centrality	0.472
Closeness Centrality	0.202
Eigenvector Centrality	0.109
PageRank Centrality	0.109

is: The overall priority of all nodes, now, are as follows:

Table 22 : Overall Priority of Nodes

Alternative	Priority
Wassi	0.500
Abu Umer	0.164
Hafiz Arshad	0.164
Abu Kaahfa	0.086
Zarar	0.086

Thus, we find that Wassi was the most significant node in the 26/11 terrorist attack's network as he has the highest overall priority value of 0.500 which is significantly higher than that of other nodes.

5. CONCLUSION

The method is very efficient in drawing useful conclusions out of a social network. It minimizes the amount of computation required to discover a point of action and is fast and easy to implement.

We worked with the data of 26/11 attacks of Mumbai, India and found that the method yielded results consistent with the previously known information about the terrorist network. With Betweenness as the most important and crucial criteria, we found that Wassi was the most important person in the whole terrorist operation, a fact that has been confirmed by the information released by the authorities.

However, the number of matrices involved is still significant. This indicates that a large amount of calculation and storage is still required by this method. Furthermore, in a network graph where degree of nodes is somewhat uniform, or graphs where a very large number of nodes have very high degree, the amount of calculation would be extensive, making the process inefficient. Further work is required to solve these issues.

All in all, the method can play a very crucial role in counter-terrorist measures. When applied to potential terrorist networks, it can help authorities find the best node to attack to disrupt the hostile organization's activities. Furthermore, the application is not limited to only terrorist networks. It can be applied to analyze any social network based on a set of criteria to detect significant nodes. With a little bit of improvement, it might take the center-stage in social network analysis and in the fight against terrorism.

REFERENCES:

[1] X. Tang and C. C. Yang, "Generalizing terrorist social networks with K-nearest neighbor and edge betweeness for social network integration and privacy preservation," *ISI 2010 - 2010 IEEE Int. Conf. Intell. Secur. Informatics Public Saf. Secur.*, pp. 49–54, 2010.

[2] Z. Li, D. Y. Sun, S. Q. Guo, and B. Li, "Detecting key individuals in terrorist network based on FANP model," *ASONAM 2014 - Proc. 2014 IEEE/ACM Int. Conf. Adv. Soc.*

Networks Anal. Min., no. Asonam, pp. 724–727, 2014.

[3] K. Dawoud, R. Alhajj, and J. Rokne, "A global measure for estimating the degree of organization of terrorist networks," *Proc. - 2010 Int. Conf. Adv. Soc. Netw. Anal. Mining, ASONAM 2010*, pp. 421–427, 2010.

[4] F. Ozgul, Z. Erdem, and C. Bowerman, "Prediction of Unsolved Terrorist Attacks Using Group Detection Algorithms," pp. 25–30, 2009.

[5] A. Sachan, "Countering terrorism through dark web analysis," *2012 3rd Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2012*, no. July, 2012.

[6] U. K. Wiil, J. Gniadek, and N. Memon, "Measuring link importance in terrorist networks," *Proc. - 2010 Int. Conf. Adv. Soc. Netw. Anal. Mining, ASONAM 2010*, pp. 225–232, 2010.

[7] F. Spezzano and A. Mannes, "STONE : Shaping Terrorist Organizational Network Efficiency," *2013 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Min. STONE*, pp. 348 –355, 2013.

[8] T. Schreck and D. Keim, "Visual Analysis of Social Media Data," 2012.

[9] T. Alzahrani and K. J. Horadam, "Analysis of two crime-related networks derived from bipartite social networks," *ASONAM 2014 - Proc. 2014 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Min.*, no. Asonam, pp. 890–897, 2014.

[10] I. Sakharova, "Al Qaeda terrorist financing and technologies to track the finance network," *Proc. 2011*