Volume 1 Issue 1 | April 2026

e-ISSN : Applied for (Online)

Journal of Integrated Engineering Innovation and Applications

An Efficient Methodology to Predict the Terrorist Threat using Data Fusion Approach for Warning Indications

Dinkar Dubey
Computer Science and Engineering
Jabalpur Engineering College, Jabalpur, India
dinkardubey2003@gmail.com

Saurabh Singh
Associate Professor
Department of Computer Science and Engineering
Jabalpur Engineering College, Jabalpur, India
ssingh@jecjabalpur.ac.in

Akhilesh Tiwari
Professor
Department of Information Technology
Madhav Institute of Technology and Science
(Deemed University), Gwalior, India
atiwari@mitsgwalior.in

ABSTRACT

Terrorist network analysis is important for predicting terror attacks and for obtaining significant data from unauthenticated data available. Graphical analysis is the most instructive tool for interpreting complex terror networks. In the proposed study, the data set from the 26/11 Mumbai attack terrorist was considered for analyzing the terrorist network by employing a data fusion approach. The study also focuses on identifying the key node to predict the terror threat accurately. From the measurement analysis, it was found that Wassi was predominant in leading the attack and was a prominent controlling agent. The data was in alignment with the report obtained from the government.

I. INTRODUCTION

Terrorism is one of the significant concerns for government agencies and law enforcement entities across the globe. With enormous advancements in perilous technology, the detrimental interest and destructive capability of the noxious terrorist organizations have accelerated tremendously. Vigorously monitoring terrorist organizational networks and tracking its vicious activities is a challenging task for government and intelligence agencies. Significant resource quantity is essential for monitoring these networks (Roper, 2003). Most of the time, law enforcement agencies and intelligence entities lack technologically advanced resources to track the functionalities of the terrorist organizations effectively. Hence comprehensive techniques for analyzing the structured data and raw data to unmask the critical and perilous data are required. These techniques strengthen the tracking and monitoring capability of the intelligent agencies in identifying the threats from terrorist organizations (Steinberg 2005). Data fusion approaches are gaining significance due to its widened approach in collecting and analyzing multiple data from various sources. Data fusion approaches are concerned with the prediction and evaluation of the current state of one or more suspected entities. Multiple evaluations of target recognition and target tracking computations are assumed while processing multiple data. Other data fusion techniques involve the usage of contexts to derive different states for different entities. These contexts can consist of the relation among other entities of interest and context type and appropriate situation (Chen et al., 2006). Data fusion approaches exhibit the capability of exploiting the situational and relational contexts, to characterize and identify the relationship between various situations. Situation and threat assessment are two major significant data fusion concepts that are dependent on each other. Generally, they are treated jointly in control processes by military commanding authorities. According to Waltz and Llinas, assessment of situation provides an overview of the suspected areas in terms of the suspicious activities, perilous functionalities, manoeuvres and organizational aspects of the terrorist groups and from the obtained overview, one can infer about the forthcoming outcome and be prepared to combat the upcoming threat (Benavoli et al., 2007). While threat assessment approximates the degree of severity through which the events are engaged and the severity level is directly proportional to the perceived capability of the combats to carry out disastrous activities on its hostiles. A high-priority constraint for successfully identifying the threats depends on the decision -maker who needs to be aware of the ground reality and forthcoming situation and vicious threats in order to combat them appropriately and rapidly (Liang 2007).

The preliminary objective of evaluating the threat assessment is to deduce the inherent threat of a circumstantial condition estimation through an inferential process. Tremendous research has been carried out in the field of multi-sensor data fusion. The fusion of multiple high-data involves comprehension of relationships between data association and alignment, tracking and identification of multiple data obtained from various sources. The obtained data can be modelled using graphical analysis (Najgebauer et al., 2008). The graphical models are derived from graphical analysis which is then implemented in various applications such as in enhanced explosive device detection, disease surveillance, cybersecurity, intelligence, and knowledge discovery and asymmetric warfare. In the military and intelligence practices, the commander (also known as decision-maker) encounters challenging circumstances frequently where they are required to develop a relationship between the graphical models obtained (Beaver et al., 2009). Another efficient technique apart from developing a graphical model is to present a situation using pictorial or schematic representation. In schematic representation, a scenario is represented in the form of a diagram. Data processing has transformed itself significantly in such a way that, any sensitive information can be transformed into pictorial representation (diagrams or figures). The diagrams are depicted in the form of attributed relational graphs (ARGs) which are an advanced version of directed graphs. In ARG's, the nodes are used to represent individuals or locations whereas edges represent links or communication devices such as mobile or satellite devices (Sambhoos et al., 2010).

II. LITERATURE REVIEW

This section provides an overview of the existing literature works on the various techniques developed for analysing the terrorist network.

Indications and Warning (I and W) of terrorist attacks specifically IED attacks require the detection of networks of agents and patterns of behaviour. (McDaniel and Schaefer, 2014) presented Social Network Analysis (SNA) which attempts to identify a network and suspicious activities related to the network and activity analysis detects the abnormal functionalities of the network detected. The proposed research constitutes both attributes; to identify vicious elements and detecting network models of terrorist attack activity, resources, and agents responsible for the attack and network behaviour. The model or prototype of the network activity is determined as RDF triples statements wherein the position of the tuple is regarded as elements for activity models. The significance of the proposed model is that the elements used in network detection are dependent on each other which enhances the detection capability of the network and it influences others in terms of the multiplier effect. The issue of assigning centrality values to nodes in a graph was analysed by (Xuan et al., 2014) social network analysis (SNA). The proposed research methodology was adopted to measure the key node in a defined network. The study discusses the significance of measuring centrality of nodes in terrorist networks as these networks reveal sensitive information related to possible attacks in future and it is important to identify the key node in the network to protect the node carrying sensitive information. A terrorist network was modelled in terms of a graphical network with nodes and links representing individuals and communication devices respectively. This study also presents a centrality measure for nodes in the terrorist network, which consists of node-related information obtained from various sources. An IoT (Internet-of-Things) architecture for detecting terrorist attacks was proposed by (Petris et al., 2014). In the proposed study, an overall framework of IoT architecture for detecting terrorist attacks is presented. The architecture helps government and intelligence entities to exploit various sources of information such as SIGINT, OSINT, and HUMINT in obtaining the data related to suspicious terror-related activities. At the same time, IoT architecture exhibits influential reasoning capabilities for transforming the raw data into validated alerts. System implementation for predicting terror attacks was also performed based on the proposed architecture.

A multi-criteria decision making (MCDM) algorithm TOPSIS (a technique for order preference by similarity to ideal solution) to identify the key node in the graph was proposed by (Singh et al., 2018). The proposed technique is characterized for identifying the principal node with less stipulated time and this technique can be used for all relative analysis concerning key node detection. The study analyzed the dataset of the terrorist network responsible for the 26/11 Mumbai attack, using the TOPSIS technique. TOPSIS is an effective mechanism for analyzing such crucial datasets. (Saidi et al., 2018) proposed a cyber community detection technique based on the Constrained Evidential C-Means (CECM) algorithm. The proposed algorithm is an appropriate clustering mechanism that is employed to detect the activities and functionalities of cyber-terrorist organizations. The author classifies the network members or objects into multiple subclasses according to Must-link and Cannot-link conditions. The node membership belonging to a cluster community is determined using belief functions. The results of clustering exhibit the efficiency of the conditional approach not only in classifying the cyber-terrorist acts but also in assigning the membership degree for every member in the network class. A novel approach for monitoring the terror network was proposed by (Basu et al., 2018). The proposed technique predominantly minimizes the necessity of additional resources along with a reduction in the usage of existing resources. The proposed approach is capable of identifying suspicious individuals planning a terror attack with fewer resources efficiently. The approach assumes that, whenever a person is active in planning a terrorist attack, persons associated with him (such as friends) will have some linking with the planning of a terror attack. However, even if the person is not active in planning attack according to the surveillance by the authorities, but the suspected person’s friends are associated with the planning, then the person planning the attack can be identified.

III. RESEARCH METHODOLOGY

This section discusses the data considered for the study, simulation software used for data analysis and performance evaluation criteria. Data fusion approach aggregates multiple data from multiple sources to predict and evaluate the current state of one or more suspected entities planning for a terrorist attack. In the proposed research methodology, an efficient approach is presented to predict the terrorist attack employing a data fusion approach for warning indications. The study also discusses the significance of identifying a key node in the network graph. Key nodes carry sensitive information related to terrorist activities and possible terror attacks. From previous literary works, it was observed that most of the proposed methodologies do not provide an efficient approach for identifying the key nodes and crucial paths accurately.

3.1. Method Implementation

In the proposed study, the 26/11 Mumbai Attacks dataset is considered for detecting the terror network. After analyzing the report obtained from the Indian government, it was observed that the attackers used satellite phones to communicate with their leaders in Pakistan. The conversations between attackers and their leaders in Pakistan were decrypted by Indian intelligence agencies. The terrorists are represented in coded format. The terrorists are mapped as: A- Abu Kaahfa, B- Wassi, C- Zarar, D- Hafiz Arshad, E - Javed, F- Abu Shoaib, G - Abu Umer, H - Abdul Rehman, I - Fahadullah, J- Baba Imran, K- Nasir, L-Ismail Khan, M- Ajmal Amir Kasab. The binary representation of the conversation between attackers and their leaders is given in Table 1.

Table 3.1. Dataset of 26/11 Mumbai Attacks

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	0	1	1	0	0	0	0	0	1	0	0	0	0
B	1	0	1	1	1	1	1	0	0	1	1	0	0
C	1	1	0	0	0	0	0	0	1	0	0	0	0
D	0	1	0	0	1	1	1	0	0	0	0	0	0
E	0	1	0	1	0	0	1	0	0	0	0	0	0
F	0	1	0	1	1	0	1	0	0	0	0	0	0
G	0	1	0	1	1	1	0	0	0	0	0	0	0
H	1	0	0	0	0	0	0	0	1	0	0	0	0
I	1	0	1	0	0	0	0	1	0	0	0	0	0
J	0	1	0	0	0	0	0	0	0	0	0	0	0
K	0	1	0	0	0	0	0	0	0	0	0	0	0
L	0	0	0	0	0	0	0	0	0	0	0	0	1
M	0	0	0	0	0	0	0	0	0	0	0	1	0

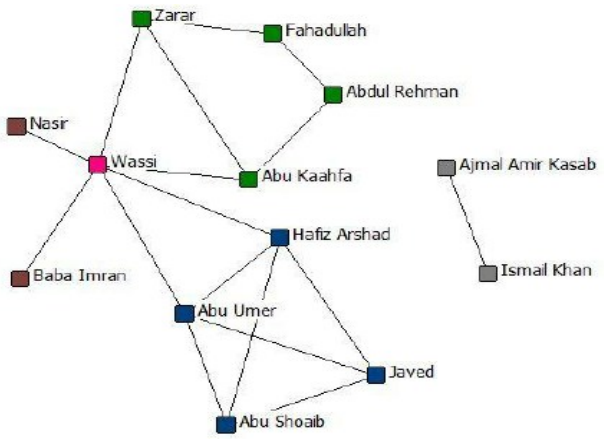

Figure 3.1. (26/11) Mumbai Attacks Network.

The data from Table 1 was visualized as a network using a simulation software known as ORA-LITE. The data were obtained for 13 terrorists involved in the terror attack.

3.2 Evaluation criteria

Analyzing social networks categorizes the participant's role in the network. Network analysis evaluates the relation between every node present in the network. In such cases, centrality measures are adopted to evaluate the relative significance of the nodes in a network. There are different versions of centrality measurements to evaluate the significance of the node in the network with respect to various aspects of the node relationship in the network. Centrality is frequently used to determine the terrorist activities; different centrality mechanisms involved in predicting terrorist threat is discussed in this section.

3.2.1. Total degree centrality (TDC)

The TDC estimates the importance of a node by evaluating the nu of the direct relationship of the node with other nodes in the network.

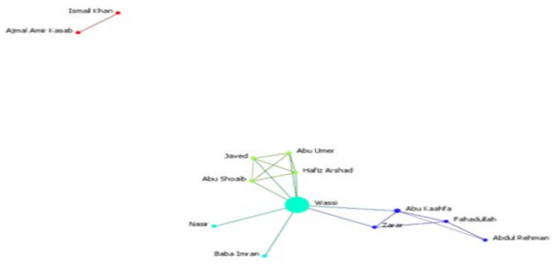

Figure Total degree centrality (TDC)

A node's total degree centrality corresponds to the degree of the considered node. The normalization of the total degree centrality measure in graph G is defined as (Berzinji et al., 2012);

$$C_G{}^d(v) = \frac{d_G(v)}{|V| - 1} \ldots\ldots(1)$$

In an instance of a directed network, two types of degree centrality measures are employed: in-degree and out-degree centrality. Irrespective of a directed or in-directed network, degree centrality depends on the edges in the graph. More the number of edges for a particular node, higher is the value of degree centrality (Campedelli et al., 2019).

3.2.2 In-degree and Out-degree Centrality:

Degree centrality is represented in the form of in-degree and out-degree centrality. Fundamentally it is an expression in terms of popularity and expansiveness. In-degree centrality is the degree of relation between two node groups A and B. i.e. During communication between nodes, nodes in group A receives information from other nodes (A←B). Nodes with high in-degree centrality value are more active and hence they attract more information compared to others. High in-degree centrality value indicates that Node A is more influential and has more weightage in the network discourse. Out-degree centrality refers to the exchange of information from Node to others (A→B). Nodes with high out-degree centrality value are more interactive in providing comments and information to others. It also refers to the extent to which the nodes can actively participate in communication activities (Yusof and Rahman, 2009)

3.2.3 Betweenness Centrality (BC)

BC is a measure to evaluate the extent of node's importance in acting as a bridge between the other two nodes. Nodes with a High value of betweenness centrality possess more control over the network compared to other nodes because more information flows across that node. If the information flowing through the network is indirect and is passing through a specific node, then that node is said to have high betweenness value. These nodes act as a binding force to prevent network disruption (Saurabh et al., 2019).

3.2.4 Closeness Centrality (CC)

Degree centrality alone cannot accurately predict the importance of the node in a network. The process also depends on the closeness between the nodes in a network. Nodes which are situated close to each other are comparatively effective in transmitting information compared to nodes placed at a longer distance. The closeness between nodes is referred to the minimum distance between other nodes- geodesics. A geodesic is the minimum path length from Node A to B (Saurabh et al., 2019). Closeness centrality of a node is determined as the total graph-theoretic distance between all other nodes in the network. Mathematically it is represented as;

$$C_A = \frac{(N-1)}{\sum_{B \in G} d_{AB}} \ldots\ldots(2)$$

Where, d_{AB} is the distance between two nodes A and B. Nodes with low closeness centrality (i.e. it is highly central) quickly attract all information passing through the network. This is because the speed with which the information flows through the network is directly proportional to the number of links in the paths traversed. Hence, nodes with less CC value are close to all nodes in the network.

3.2.5. Eigenvector Centrality (EC)

An EC is an evaluation of the significance of a node in terms of node influence on adjacent nodes in the network. EC is basically used to identify the most central node in the network. A node with a greater value of eigenvector is regarded as the most central node with greater prominence among other nodes in the network. In terrorist network analysis, EC identifies the suspected person and other individuals associated with the person.

Mathematically, Eigenvector Centrality is defined as;

$$X_i = \frac{1}{\lambda} \sum_{j \in NB_i} A_{ij}.X_j....(3)$$

Where Nb_i is the adjacent nodes of i, λ is the eigenvalue. A_{ij} is the element in the adjacent matrix A at ij^th position. X_j is the eigenvector centrality of node j (Choudhary and Singh, 2015).

3.2.6. PageRank Centrality (PC)

PageRank (PR) of a node is defined as a measure for evaluating the relative significance and ranking of the nodes in the network. PR of a node is basically defined by the number of communication link received by the node, propensity of the linkers and its centrality. In terrorist network analysis, PageRank identifies a person depending on the position of the node in a network (Lv et al., 2019). PageRank is mathematically expressed as;

$$PR(\alpha) = \sum_{b \in Nb_a} \left(\frac{PR(b)}{L(b)} \right) ....(4)$$

Where Nb_α are the nodes connect to node α and L(b) is the total number of links outgoing from note b. PR(b) is the PageRank of node b

3.2.7. Ego Betweenness Centrality (EBC):

The EBC of a node is referred to the betweenness value within the vicinity of own ego network. The ego network consists of the following: the node itself, its adjacent neighbour nodes, and all links between them (Everett and Borgatti, 2005).

3.2.8 Contribution Centrality

CC evaluates Eigenvector centrality while transforming the input network. Transformation of link values is proportional to the dissimilarities in the nodes. It is assumed that the link connecting two nodes with the same neighbouring nodes is not considered an important link as they do not gain new neighbours from the connection. Specifically, each link is weighted by the inverse of the Jaccard similarity of its nodes (Landherr et al., 2010).

IV. RESULTS AND DISCUSSION

4.1 Total Degree Centrality

If the value interest node is greater than the normal value (greater than 1 standard deviation above the mean), the row is coloured as red. The row is coloured green if the node value is within 1 standard deviation of the mean. If the node value falls below the normal value (less than one standard deviation(s) below the mean) then the row is coloured blue. Input network: Agent x Agent (size: 13, density: 0.24359). The ranking of the suspected agents based on the context is defined in Table 4.1.

The scaled value statistics considered for measuring total degree centrality is Min:0.083 Mean:0.244 Mean in the random network: 0.244, Lower quartile: 0.083, Upper quartile: 0.313, Max: 0.667 Std.dev: 0.244 Std.dev in random network: 0.119, Median: 0.250.

Table 4.1. Node Values To Determine Total Degree Centrality

Rank	Agent	Value	Un-scaled	Context*
1	B	0.667	16	3.554
2	G	0.333	8	0.754
3	D	0.333	8	0.754
4	A	0.292	7	0.404
5	F	0.292	7	0.404
6	E	0.292	7	0.404
7	I	0.250	6	0.054
8	C	0.250	6	0.054
9	H	0.125	3	-0.996
10	M	0.083	2	-1.346
11	J	0.083	2	-1.346
12	L	0.083	2	-1.346
13	K	0.083	2	-1.346

* Number of standard deviations from the mean of a random network of the same size and density

4.2 Out-degree Centrality

In out-degree centrality, the information flows from the individual node to other nodes. The ranking of the suspected agents based on the node value is defined in Table 4.2.

Table 4.2 The node value analysis for determining out-degree centrality

Rank	Agent	Value	Unscaled
1	B	0.667	8
2	F	0.333	4
3	G	0.333	4
4	D	0.333	4
5	A	0.250	3
6	I	0.250	3
7	E	0.250	3
8	C	0.250	3
9	H	0.167	2
10	M	0.083	1
11	J	0.083	1
12	L	0.083	1
13	K	0.083	1

The scaled value statistics considered for evaluating out-degree centrality are Min: 0.083, Mean: 0.244, Lower quartile: 0.083, Max: 0.667, Std.dev: 0.155, Median: 0.250 and Upper quartile: 0.333

4.3 In-degree Centrality

In evaluating in-degree centrality, the normalization of the node which is directed by number of links by considering the maximum number of such links. This state is also known as column degree centrality as it is calculated by considering the sum of the column values in the input network. Input network(s): Agent x Agent

Table 4.3 The Node Value Analysis for Determining in-degree Centrality

Rank	Agent	Value	Unscaled
1	B	0.667	8
2	A	0.333	4
3	G	0.333	4
4	D	0.333	4
5	E	0.333	4
6	F	0.250	3
7	I	0.250	3
8	C	0.250	3
9	H	0.083	1
10	M	0.083	1
11	J	0.083	1
12	L	0.083	1
13	K	0.083	1

The scaled value statistics considered for evaluating the in-degree centrality are: Min: 0.083 Mean: 0.244, Lower quartile: 0.083, Max: 0.667, Std.dev: 0.162, Median: 0.250 and Upper quartile: 0.333

4.4 Betweenness Centrality and Betweenness centrality (Inverted)

The BC is defined as the percentage of information passing across the node which is acting as a bridge between two nodes. If the weight of the data passing through the node is more, then that node link is considered as a high-value link. Potential individuals or organizations are basically positioned as mediators between groups and to influence the activities of a group, while another group serves as the barrier between groups.

Table 4.4: The node value analysis for determining Betweenness centrality

Rank	Agent	Value	Un-scaled	Con-text*
1	B	0.503	66.333	6.370
2	A	0.136	18	0.536
3	C	0.080	10.500	-0.369
4	I	0.072	9.500	-0.490
5	G	0.003	0.333	-1.597
6	D	0.003	0.333	-1.597
7	H	0	0	-1.637
8	F	0	0	-1.637
9	M	0	0	-1.637
10	J	0	0	-1.637
11	L	0	0	-1.637
12	E	0	0	-1.637
13	K	0	0	-1.637

The scaled value statistics considered for evaluating betweenness centrality are: Min: 0, Mean: 0.061, Lower quartile: 0, Max: 0.503 Std.dev: 0.061

4.5. Ego Betweenness Centrality

Input network(s): Agent x Agent

Table 4.5 The node value analysis for determining Ego Betweenness centrality

Rank	Agent	Value
1	B	0.756
2	I	0.417
3	A	0.250
4	C	0.167
5	G	0.028
6	D	0.028
7	H	0
8	F	0
9	M	0
10	J	0
11	L	0
12	E	0
13	K	0

The scaled value statistics considered are: Min: 0, Mean: 0.127, Lower quartile: 0, Max: 0.756, Std.dev: 0.220, Median: 0, Upper quartile: 0.208

4.6. Closeness Centrality and Closeness Centrality (Inverted)

The CC is defined as the node closeness with two nodes in a network. The closeness is considered as an inverse of the sum of distances in the network from a node to all other nodes.

Table 4.6: The node value analysis for determining Closeness centrality

Rank	Agent	Value	Un-scaled	Context*
1	B	0.308	0.026	-2.420
2	A	0.279	0.023	-2.799
3	C	0.279	0.023	-2.799
4	F	0.267	0.022	-2.964
5	G	0.267	0.022	-2.964
6	D	0.267	0.022	-2.964
7	E	0.261	0.022	-3.041
8	J	0.250	0.021	-3.185
9	K	0.250	0.021	-3.185
10	I	0.245	0.020	-3.252
11	H	0.240	0.020	-3.317
12	M	0.083	0.007	-5.394
13	L	0.083	0.007	-5.394

The scaled value statistics considered are: Min: 0.083, Lower quartile: 0.242, Max: 0.308, Std.dev: 0.237, Std.dev in random network: 0.075, Median: 0.261, Upper quartile: 0.273.

4.7 Eigenvector Centrality

A node with a greater value of eigenvector is regarded as the most central node with greater prominence among other nodes in the network.

Table 4.7 The node value analysis for determining Eigenvector centrality

The scaled value statistics considered are: Min: 0.088, Lower quartile: 0.142, Max: 0.612, Std.dev: 0.290, Std.dev in random network: 0.307, Median: 0.230, Upper quartile: 0.469

Rank	Agent	Value	Un-scaled	Context
1	B	0.612	0.433	0.421
2	F	0.469	0.331	-0.046
3	G	0.469	0.331	-0.046
4	D	0.469	0.331	-0.046
5	E	0.469	0.331	-0.046
6	A	0.246	0.174	-0.770
7	C	0.230	0.162	-0.824
8	M	0.154	0.109	-1.071
9	L	0.154	0.109	-1.071
10	J	0.142	0.101	-1.109
11	K	0.142	0.101	-1.109
12	I	0.131	0.093	-1.146
13	H	0.088	0.062	-1.287

4.8 Contribution Centrality

Input network(s): Agent x Agent

Table 4.8 The node value analysis for determining Contribution centrality

Rank	Agent	Value	Unscaled
1	B	0.722	0.511
2	A	0.421	0.298
3	C	0.391	0.276
4	F	0.297	0.210
5	G	0.297	0.210
6	D	0.297	0.210
7	E	0.297	0.210
8	J	0.256	0.181
9	K	0.256	0.181
10	I	0.250	0.177
11	H	0.186	0.131
12	M	0.154	0.109
13	L	0.154	0.109

The scaled value statistics considered are: Min: 0.154, Mean: 0.306, Lower quartile: 0.218, Max: 0.722, Std.dev: 0.142, Median: 0.297, Upper quartile: 0.344

4.9 Acts as a Hub (hub centrality)

The network nodes are considered to be hub-central when the out-link of the node is connected to multiple in-links. Any person or organizational entities acting as hubs are transferring the information to others. In technical terms, a node is said to be hub-central if the out-links of the nodes consist of various other nodes forwarding links to that node. The mathematical expression of this measurement analysis is known as hub centrality and it is computed on a node by node matrices.

Table 4.9 The node value analysis or determining hub centrality

Rank	Agent	Value	Unscaled
1	B	0.632	0.447
2	F	0.498	0.352
3	G	0.475	0.336
4	D	0.475	0.336
5	E	0.378	0.267
6	C	0.248	0.175
7	A	0.242	0.171
8	J	0.150	0.106
9	K	0.150	0.106
10	I	0.129	0.091
11	H	0.097	0.069
12	M	0	0
13	L	0	0

The scaled value statistics considered are: Min: 0, Mean: 0.267, Lower quartile: 0.113,

Max: 0.632, Std.dev: 0.197, Median: 0.242, Upper quartile: 0.475

4.10 Acts as an Authority (authority centrality):

The network nodes are considered to be authority-central when the in-links from the node have multiple out-links. Any individual person or organizational entity that behaves as authorities are receiving sensitive data from multiple sources with each of whom transmits the data to more number of people.

Table 4.10 The node value analysis for determining authority centrality

Ranks	Agent	Value	Unscaled
1	B	0.627	0.443
2	E	0.498	0.352
3	G	0.475	0.336
4	D	0.475	0.336
5	F	0.379	0.268
6	A	0.265	0.187
7	C	0.240	0.170
8	J	0.152	0.107
9	K	0.152	0.107
10	I	0.141	0.099
11	H	0.031	0.022
12	M	0	0
13	L	0	0

The scaled value statistics considered are: Min: 0, Mean: 0.264 , Lower quartile: 0.086

Max: 0.627, Std.dev: 0.201, Median: 0.240, Upper quartile: 0.475

4.11. Constraint (structural holes)

The extent to which every node in a square network is refrained from acting due to its link with other neighbouring nodes. Input network (s): Agent x Agent

Table 4.11: The node value analysis for determining node constraints

Rank	Agent	Value
1	G	4.859
2	D	4.859
3	F	4.191
4	E	4.191
5	M	4
6	J	4
7	L	4
8	K	4
9	C	3.707
10	I	3.596
11	A	3.314
12	H	2.778
13	B	1.853

The scaled value statistics considered are: Min: 1.853, Mean: 3.796, Lower quartile: 3.455, Max: 4.859, Std.dev: 0.776, Median: 4, Upper quartile: 4.191

4.12 Effective Network Size

The effective size of a node's ego network based on the redundancy of ties. Input network(s): Agent x Agent

Table 4.12 The node values for analyzing the effective network size:

Rank	Agent	Value
1	B	4.750
2	A	1.250
3	M	1
4	J	1
5	I	1
6	L	1
7	K	1
8	H	0.500
9	C	0.333
10	F	-1.250
11	E	-1.250
12	G	-1.500
13	D	-1.500

The scaled value statistics considered are: Min: -1.500, Mean: 0.487, Lower quartile: -1.250, Max: 4.750, Std.dev: 1.618, Median: 1, Upper quartile: 1

4.13 Efficiency (structural holes)

The fraction of nodes in an ego network that is not redundant. Input network(s): Agent x Agent

Table 4.13 The node values for analyzing the efficiency of the network:

Rank	Agent	Value
1	M	1
2	J	1
3	L	1
4	K	1
5	B	0.594
6	I	0.333
7	A	0.313
8	H	0.250
9	C	0.111
10	F	-0.313
11	E	-0.313
12	G	-0.375
13	D	-0.375

The scaled value statistics considered are: Min: -0.375, Mean: 0.325 , Lower quartile: -0.313, Max: 1, Std.dev: 0.536, Median: 0.313, Upper quartile: 1

4.14 PageRank Centrality

PageRank centrality evaluates the significance of a node depending on the prominence of its in-coming nodes. The PR of the node is computed as the fraction of times a node would be visited when traversing the network according to the network of probabilities. Input network(s): Agent x Agent

Table 4.14 The node values for analyzing the PageRank centrality:

Rank	Agent	Value
1	B	0.187
2	G	0.089
3	D	0.089
4	A	0.087
5	E	0.084
6	M	0.077
7	L	0.077
8	C	0.076
9	I	0.071
10	F	0.069
11	H	0.032
12	J	0.031
13	K	0.031

The scaled value statistics considered are: Min: 0.031, Mean: 0.077, Lower quartile: 0.050, Max: 0.187, Std.dev: 0.038 , Median: 0.077 and Upper quartile: 0.088.

4.15 Clustering coefficient

Clustering coefficient evaluates the degree of clustering in a network by providing the average value of the clustering coefficient of every node, defined as the density of the node's ego network.

Table 4.15 The node values for analyzing the Clustering coefficient:

Rank	Agent	Value
1	H	1
2	F	1
3	E	1
4	G	0.917
5	D	0.917
6	C	0.667
7	A	0.500
8	I	0.500
9	B	0.232
10	M	0
11	J	0
12	L	0
13	K	0

The scaled value statistics considered are: Min: 0, Mean: 0.518, Lower quartile: 0, Max: 1 Std.dev: 0.411, Median: 0.500 and Upper quartile: 0.958

4.16 Recurring Top Ranked Agent

This chart shows the Agent that is repeatedly top-ranked in the node-level measures listed below. The value shown is the percentage of measures for which the Agent node was ranked in the top three. If there are multiple networks, then a measure is computed multiple times and nodes are ranked multiple times for the measure. There are 13 nodes in the node-set.

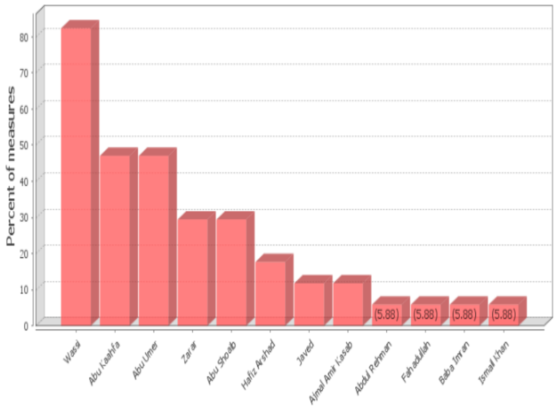

Figure 4.1: Graphical representation of the ranking of different agents

V. CONCLUSION

The proposed methodology provides a detailed analysis of data fusion approach to predict the terrorist threat. The study discusses various approaches to derive an optimal solution to identify the terrorist attack efficiently. The data considered for visualization was for 26/11 Mumbai terror attack, data was obtained from reports obtained from the Government of India (GOI, 2009). Measurement analysis shows that Wassi was the most central, leading and controlling agent which is in alignment with the report obtained from the government. This suggests that the proposed methodology can be used to develop a counterterrorism strategy which concentrates on the key node identification and its ego network to obtain maximum network disruption.

REFERENCES:

[1] Roper, W. E. (2003). Spatial Data Fusion for Infrastructure Condition Assessment (pp. 270-288). Technical Memorandum of Public Works Research Institute.

[2] Steinberg, A. N. (2005, July). An approach to threat assessment. In 2005 7th International Conference on Information Fusion (Vol. 2, pp. 8-pp). IEEE.

[3] Chen, G., Shen, D., Kwan, C., Cruz, J. B., and Kruger, M. (2006, July). Game theoretic approach to threat prediction and situation awareness. In 2006 9th International Conference on Information Fusion (pp. 1-8). IEEE.

[4] Benavoli, A., Ristic, B., Farina, A., Oxenham, M., and Chisci,L. (2007, July). An approach to threat assessment based on evidential network In 2007 10th International Conference on Information Fusion (pp. 1-8). IEEE.

[5] Liang, Y. (20017, August). An approximate reasoning model for situation and threat assessment. In Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007) (Vol.4, pp. 246-250). IEEE.

[6] Najgebauer, A., Antkiewicz, R., Chmielewski, M., and Kasprzak, R. (2008). The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution. Journal of Telecommunication and Information Technology, 14-20.

[7] Sambhoos, K., Nagi, R., Sudit, M., and Stotz, A. (2010). Enhancement to high level data fusion using graph matching and state space search. Information Fusion, 11(4), 351-364.

[8] McDaniel, D., and Schaefer, G. (2014, May). A data fusion approach to indications and warnings of terrorist attacks. In Next-Generation Analyst II (Vol. 9122, p. 912204). International Society for Optics and Photonics.

[9] Xuan, D., Yu, H., and Wang, J. (2014, December). A novel method of centrality in terrorist network. In 2014 Seventh International Symposium on computational Intelligence and Design (Vol. 2, pp. 144-149). IEEE.

[10] Petris, S., Georgoulis, C., Soldatos, J., Giordani, I., Sormani, R., and Djordjevic, D.(2014). Predicting terroristic attacks in

urban environments: an internet-of-things approach. International Journal of Security and its Applications, 8(4), 195-218.

[11] Singh, S., Verma, S., and Tiwari, A. (2018). An innovative approach for identification of pivotal node in terrorist network using promethee method (an anti-terrorism approach). International Journal of Engineering and Technology, 7(1), 95-99

[12] Saidi,F., Trabelsi, Z., and Ghazela, H. B. (2018, May). A novel approach for terrorist sub-communities detection based on constrained evidential clustering. In 218 12th International Conference on Research Challenges in Information Science (RCIS) (pp. 1-8). IEEE.

[13] Basu, K., Zhou, C., Sen, A., and Goliber, V. H. (2018, December). A Novel Graph Analytic Approach to Monitor Terrorist Networks. In 2018 IEEE Intl Conf on Parallel and Distributed Processing with Applications, Ubiquitous Computing and Communications, Big Data and Cloud Computing, Social Computing and Networking, Sustainable Computing and Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom) (pp. 1159-1166). IEEE.

[14] Saurabh Singh, Shashikant Verma, Akhilesh Tiwari. (2019). Identification of Pivotal node in Terrorist Network using TOPSIS Method. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9,

[15] Berzinji, A., Kaati, L., and Rezine, A. (2012, August). Detecting key players in terrorist networks. In 2012 European Intelligence and Security Informatics Conference (pp. 297-302). IEEE.

[16] Campedelli, G. M., Cruickshank, I., and Carley, K. M. (2019). A complex networks approach to find latent clusters of terrorist groups. Applied Network Science, 4(1), 59.

[17] Yusof, N., and Rahman, A. A. (2009, April). Students' interactions in online asynchronous discussion forum: A Social Network Analysis. In 2009 International Conference on Education Technology and Computer (pp. 25-29). IEEE.

[18] Choudhary, P., and Singh, U. (2015). A survey on social network analysis for counter-terrorism. International Journal of Computer Applications, 112(9), 24-29.

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

[20] Everett, M., and Borgatti, S. P. (2005). Ego network betweenness. Social networks, 27(1), 31-38.

[21] Lv, L., Zhang, K., Zhang, T., Bardou, D., Zhang, J., and Cai, Y. (2019). PageRank centrality for temporal networks. Physics Letters A, 383(12), 1215-1222.

[22] Landherr, A., Friedl, B., and Heidemann, J. (2010). A critical review of centrality measures in social networks. Business and Information Systems Engineering, 2(6), 371-385.

* * * * *