An Effective Approach to Terrorist Threat Prediction Using Data Fusion for Warning Signals

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

[1]Department of Computer Science and Engineering, Jabalpur Engineering College, Jabalpur, Madhya Pradesh 482001, India

[2]Computer Science Department, Govind Ballabh Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand 246194, India

[3]Department of CSE & IT, Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh 474005, India

Emails: ssingh@jecjabalpur.ac.in; skverma.gbpec@rediffmail.com; atiwari.mits@gmail.com

Abstract

Terrorist network research is crucial for both anticipating terrorist acts and extracting valuable information from existing unauthenticated sources. The best method for deciphering intricate terror networks is graphic analysis. The suggested study used a data fusion technique to analyze the terrorist network using the dataset from the terrorist assault in Mumbai on 26/11. In order to effectively forecast the terror threat, the study also focuses on finding the critical node. Wassi led the attack and was a key controlling agent, according to the measurement analysis. The information matched the government's report.

Keywords: Terrorist Network; Data mining; Threat prediction; Graphics processors; Data models

1. 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 their vicious activities is a challenging task for government and intelligence agencies. Significant resource quantity is essential for monitoring these networks [1]. Most of the time, law enforcement agencies and intelligence entities lack technologically advanced resources to track the activities of terrorist organizations effectively. Hence, comprehensive techniques for analyzing structured data and raw data to unmask critical and perilous data are required. These techniques strengthen the tracking and monitoring capability of the intelligence agencies in identifying the threats from terrorist organizations [2]. Data fusion approaches are gaining significance due to their expanded approach to 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 use 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 [3]. 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 the 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 [4]. While threat assessment approximates the degree of

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

severity with which the events are engaged, the severity level is directly proportional to the perceived capability of the combatants 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 [5].

The preliminary objective of evaluation is to deduce the essential threat of a circumstantial condition estimation through an inferential process. The topic of multi-sensor data fusion has seen tremendous study. The fusion of multiple high-dimensional 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 [6]. The graphical models are derived from graphical analysis, which is then implemented in various applications such as enhanced explosive device detection, disease surveillance, cybersecurity, intelligence, and knowledge discovery and asymmetric warfare. In military and intelligence practices, the commander (also known as the decision-maker) frequently encounters challenging circumstances where they are required to develop a relationship between the graphical models obtained [7]. 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 absorbed charts. In ARG's, the nodes are used to represent individuals or locations, whereas edges signify links or communiqué devices such as mobile or satellite devices [8].

2. Literature review

An overview of the literature on the several methods created for terrorist network analysis is given in this section. The identification of agent networks and behavioral patterns is necessary for the Indications and Warning (I&W) of terrorist attacks, particularly IED strikes. [9] 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. The proposed research constitutes both attributes: identifying 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 triple statements wherein the position of the tuple is regarded as elements for action 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 influences others in terms of the multiplier effect. The issue of assigning centrality magnitudes to nodes in a graph was analysed by [10] in SNA. The proposed research methodology was adopted to measure the key node in a defined network. The study discusses the significance of measuring the 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 [11]. 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.

[12] used TOPSIS (a strategy for order preference by resemblance to ideal solution) is a multi-criteria decision-making (MCDM) technique that was developed to identify the important node in the graph. The proposed technique is characterized by identifying the principal node with less stipulated time, and this technique can be used for all relative analyses 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. [13] suggested a method for detecting cyber communities that is 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 [14]. 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

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

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. The individual planning the assault can be detected even if the police' monitoring indicates that the suspect is not actively involved in the planning but that the suspect's pals are involved.

3. Research Methodology

This section discusses the data considered for the study, simulation software used for data analysis, and performance evaluation criteria. The 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 envisage a terrorist attack employing a data fusion method for warning signals. 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.

A. 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. Indian intelligence services decoded the discussions between the terrorists and their Pakistani commanders. A coded format was used to portray the terrorists. 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 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

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.

B. Evaluation Criteria

SNA provides a systematic approach for identifying and interpreting the roles of separate participants inside a network structure. It examines the patterns of interaction and connectivity among the nodes to understand how different entities are positioned and related to one another. To quantify the relative importance or influence of a node, various centrality measures are commonly employed. Each centrality metric evaluates node significance

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

from a different perspective, such as direct connectivity, accessibility to other nodes, intermediary position, or overall influence within the network. Consequently, centrality-based analysis has been widely applied to the investigation of terrorist networks, where it can assist in identifying influential individuals, critical intermediaries, and potentially high-risk actors. The different centrality measures used for assessing and predicting terrorist threats are discussed in this section.

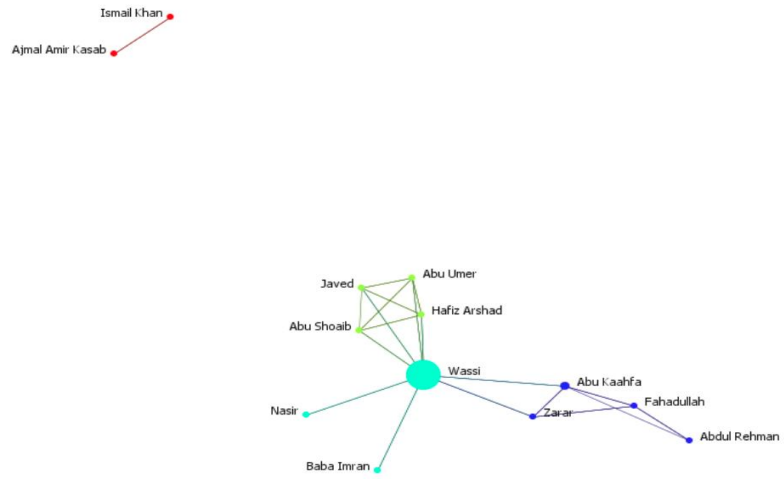

Figure 1. (26/11) Mumbai Attacks Network.

Total degree centrality (TDC)

Total Degree Centrality (TDC) quantifies the relative node importance according to the number of direct connections. It keeps up with other network nodes. The TDC value of a particular node is determined by its degree, representing the total number of edges directly associated with that node. Nodes possessing a larger number of direct links generally exhibit greater structural prominence within the network. For better comparison among nodes, particularly across networks of different sizes, the degree value is commonly normalized. For a graph G, the normalized Total Degree Centrality can be expressed as follows [15]:

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

In a directed network, there are two types of degree centrality measurements: in-degree and out-degree centrality. Degree centrality is dependent on the graph's edges, regardless of whether the network is directed or undirected. The degree centrality value increases with the quantity of edges for a given node [16].

In-degree and Out-degree centrality

In-degree and out-degree centrality are two ways that degree centrality is expressed. At its core, it is an expression of popularity and breadth. In-degree centrality is the degree to which two node groups, A and B, are related. Nodes in group A get information from nodes in group B during communication. Because they are more active than other nodes, nodes with high in-degree centrality draw more information. When Node A has a high in-degree centrality score, it has more weight and impact in the network conversation. Information sharing between a node and others (A→B) is referred to as out-degree centrality. When it comes to sharing information and opinions with others, nodes with a high out-degree centrality rating are more engaged. It also refers to the extent to which the nodes can actively participate in communication activities [17].

Betweenness Centrality (BC)

BC is a metric used to assess how significant a node is in serving as a link between the other two nodes. A node with a high betweenness centrality has greater power over the network than other nodes since more information flows through it. A node is considered to have a high BC if information is going through it indirectly through the network. According to [18], these nodes serve as a binding force to stop network disruptions.

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

Closeness Centrality (CC)

Degree centrality alone cannot accurately predict the importance of the node in a network. The proximity of a network's nodes affects the process as well. When it comes to information transmission, nodes that are close to one another are more efficient than those that are farther apart. Geodesics, or the shortest distance between nodes, is used to describe how close two nodes are to one another. The shortest path between Node A and Node B is called a geodesic [18]. A node's CC is determined by adding the graph-theoretic distances between each other node in the network. Mathematically it is represented as;

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

where dAB is the separation between nodes A and B. All information flowing through the network is swiftly drawn to nodes with low proximity centrality, which is highly central. This is due to the fact that the number of links in the tracks traversed strongly correlates with the speed at which information moves across the network. As a result, nodes with lower CC magnitude are near every other node in the network.

Eigenvector Centrality (EC)

An EC is an evaluation of the significance of a node in terms of node influence on adjacent bulges in the network. EC is basically used to identify the most central node in the network. A node with a greater value of EC is regarded as the most central node, with greater prominence among other nodes in the network. The suspected individual and other people connected to them are identified by EC in terrorist network analysis.

Mathematically, EC is defined as;

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

Where Nb_i is the adjacent nodes of i, λ is the eigenvalue. A_{ij} is the component in the adjacency matrix A at ij^{th} location. X_j is the EC of node j [19].

PageRank Centrality (PC)

A node's PageRank (PR) is a metric used to assess each node's relative importance and ranking inside the network. A node's PR is primarily strong-minded by the number of communication links it accepts, the linkers' inclination, and its centrality. PageRank uses the location of a node in a network to identify an individual in terrorist network analysis [20] . PageRank is mathematically expressed as:

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

Where Nb_a are the nodes connected to node a and L(b) is the total number of links outgoing from node b, PR(b) is the PageRank of node b.

Ego Betweenness Centrality (EBC)

The EBC of a node is referred to the betweenness value within the vicinity of its own ego network. The ego network consists of the following: the node itself, its adjacent neighbour nodes, and all links between them [21].

Contribution Centrality

Contribution Centrality evaluates Eigenvector centrality while transforming the input network. The transformation of link magnitude 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. Each link is weighted by the inverse of the Jaccard similarity of its nodes [22]. Input network(s): Agent x Agent.

4. Results and Discussion

A. Total Degree Centrality

Nodes exceeding the mean by more than one standard deviation are marked red, those within ±1 standard deviation are shown in green, and magnitude below this range are indicated in blue. The input Agent × Agent network contains 13 nodes with a density of 0.24359. The ranking of the suspected agents based on the context is defined in Table 2.

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

Table 2: Node Magnitude To Determine Total Degree Centrality

RANK	AGENT	NORMALIZED SCORE	RAW SCORE	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

* A random network with the similar size and thickness's standard deviations from its mean

Total degree centrality is measured using the scaled value statistics Min:0.083 Mean:0.244. The random network's mean is 0.244, its lower quartile is 0.083, its upper quartile is 0.313, its maximum is 0.667, its standard deviation is 0.119, and its median is 0.250.

B. Out-degree Centrality

In out-degree significance, the information flows from the individual node to other nodes. The ranking of the suspected agents based on the node normalized score is defined in Table 3.

Table 3: The node normalized score analysis for determining out-degree centrality

Rank	Agent	normalized score	Raw Score
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

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

11	J	0.083	1
12	L	0.083	1
13	K	0.083	1

The normalized score statistics considered for evaluating out-degree centrality are Min: 0.083, Mean: 0.244, Lower quartile: 0.083, Max: 0.667, SD: 0.155, Median: 0.250 and Upper quartile: 0.333

C. 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 Normalized centrality score as it is calculated by considering the sum of the raw scores in the input network.

Table 4: The node normalized score analysis for determining in-degree centrality

RANK	AGENT	NORMALIZED SCORE	RAW SCORE
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 normalized score statistics considered for evaluating the in-degree centrality are: Min: 0.083 Mean: 0.244, Lower quartile: 0.083, Max: 0.667, SD: 0.162, Median: 0.250 and Upper quartile: 0.333

D. Betweenness Centrality & 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 5: The node normalized score analysis for determining Betweenness centrality

Rank	Agent	normalized score	Raw Score	Context*
1	B	0.503	66.333	6.370
2	A	0.136	18	0.536
3	C	0.080	10.500	-0.369

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

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 normalized score statistics considered for evaluating betweenness centrality are: Min: 0, Mean: 0.061, Lower quartile: 0, Max: 0.503, SD: 0.061

E. Ego Betweenness Centrality

Table 6: The node normalized score analysis for determining Ego Betweenness centrality

Rank	Agent	normalized score
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 normalized score statistics considered are: Min: 0, Mean: 0.127, Lower quartile:

0, Max: 0.756, SD: 0.220, Median: 0, Upper quartile: 0.208

F. Closeness Centrality and Closeness Centrality (Inverted)

The node proximity between two nodes in a network is known as the CC. The proximity is defined as the inverse of the total distance between a node and every other node in the network.

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

Table 7: The node normalized score analysis for determining Closeness centrality

RANK	AGENT	NORMALIZED SCORE	RAW SCORE	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 normalized score statistics considered are: Min: 0.083, Lower quartile: 0.242, Max: 0.308, SD: 0.237, SD in random network: 0.075, Median: 0.261, Upper quartile: 0.273.

G. 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 8: The node normalized score analysis for determining Eigenvector centrality

Rank	Agent	Normalized score	Raw Score	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

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

The normalized score statistics considered are: Min: 0.088, Lower quartile: 0.142, Max: 0.612, SD: 0.290, SD in random network: 0.307, Median: 0.230, Upper quartile: 0.469

H. Contribution Centrality

Table 9: The node normalized score analysis for determining Contribution centrality

RANK	AGENT	NORMALIZED SCORE	RAW SCORE
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, SD: 0.142, Median: 0.297, Upper quartile: 0.344

I. 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 10: The node normalized score analysis for determining Eigenvector hub centrality

Rank	Agent	normalized score	Raw Score
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

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

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 normalized score statistics considered are: Min: 0, Mean: 0.267, Lower quartile: 0.113, Max: 0.632, SD: 0.197, Median: 0.242, Upper quartile: 0.475

J. 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 11: The node normalized score analysis for determining authority centrality

RANKS	AGENT	NORMALIZED SCORE	RAW SCORE
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 normalized score statistics considered are: Min: 0,Mean: 0.264 , Lower quartile: 0.086 Max: 0.627, SD: 0.201, Median: 0.240, Upper quartile: 0.475

A. 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.

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

Table 12: The node normalized score analysis for determining node constraints

Rank	Agent	normalized score
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 normalized score statistics considered are: Min: 1.853, Mean: 3.796, Lower quartile: 3.455 , Max: 4.859, SD: 0.776, Median: 4, Upper quartile: 4.191

B. Effective Network Size

The redundancy of ties determines the effective size of a node's ego network.

Table 13: The node normalized score for analyzing the effective network size

Rank	Agent	Normalized score
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 NORMALIZED SCORE STATISTICS CONSIDERED ARE: MIN: -1.500, MEAN: 0.487, LOWER QUARTILE: -1.250,

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

MAX: 4.750, SD: 1.618, MEDIAN: 1, UPPER QUARTILE: 1

C. Efficiency (structural holes)

the percentage of redundant nodes in an ego network.

Table 14: The node Magnitude for analyzing the efficiency of the network

RANK	AGENT	NORMALIZED SCORE
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 normalized score 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

D. PageRank Centrality

PageRank centrality evaluates the significance of a node depending on the prominence of its in-coming nodes. According to the network of probabilities, a node's PR is calculated as the percentage of times it would be visited when traveling the network.

Table 15: The node Magnitude for analyzing the PageRank Centrality

Rank	Agent	normalized score
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

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

9	I	0.071
10	F	0.069
11	H	0.032
12	J	0.031
13	K	0.031

The normalized score statistics considered are: Min: 0.031, Mean: 0.077, Lower quartile: 0.050, Max: 0.187, SD: 0.038, Median: 0.077 and Upper quartile:

0.088.

E. Clustering coefficient

By calculating the average value of each node's clustering coefficient—which is the density of the node's ego network—the clustering coefficient assesses the degree of clustering in a network.

Table 16: The node Magnitude for analyzing the Clustering coefficient

Rank	Agent	normalized score
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 normalized score statistics considered are: Min: 0, Mean: 0.518, Lower quartile:

0, Max: 1 SD: 0.411, Median: 0.500 and Upper quartile: 0.958

F. Recurring Top Ranked Agent

The agent that consistently ranks first in the node-level metrics described below is seen in Figure 2. The % of measurements for which the Agent node was placed in the top three is shown by the normalized score. A measure is calculated numerous times and nodes are rated many times for the metric if there are multiple networks. The node-set consists of 13 nodes.

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

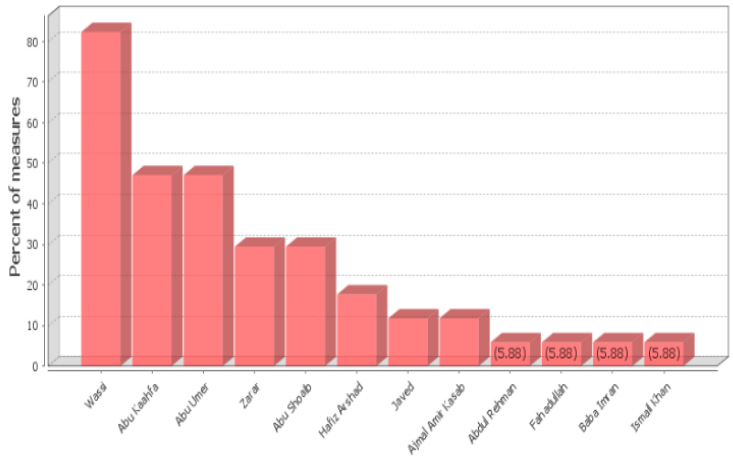

Figure 2: Graphical representation of the ranking of different agents

5. Conclusion

The proposed methodology provides a detailed analysis of data fusion approaches to predict the terrorist threat. The study discusses various approaches to derive an optimal solution to identify the terrorist attack efficiently. The Government of India's reports on the 26/11 Mumbai terror assault provided the data that was taken into consideration for the visualization [23]. Wassi was the most central, leading, and controlling actor, according to measurement analysis, which is consistent with the official claim. This implies that a counterterrorism strategy that focuses on identifying the critical node and its ego network in order to achieve maximal network disruption may be developed using the suggested technique.

References

[1] J. M. Beaver, R. A. Kerekes, and J. N. Treadwell, "An information fusion framework for threat assessment," in *Proc. 2009 12th International Conference on Information Fusion*, Jul. 2009, pp. 1903–1910.

[2] A. Benavoli, B. Ristic, A. Farina, M. Oxenham, and L. Chisci, "An approach to threat assessment based on evidential network," in *Proc. 2007 10th International Conference on Information Fusion*, Jul. 2007, pp. 1–8.

[3] A. Berzinji, L. Kaati, and A. Rezine, "Detecting key players in terrorist networks," in *Proc. 2012 European Intelligence and Security Informatics Conference*, Aug. 2012, pp. 297–302.

[4] K. Basu, C. Zhou, A. Sen, and V. H. Goliber, "A novel graph analytic approach to monitor terrorist networks," in *Proc. 2018 IEEE International Conference on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, Dec. 2018, pp. 1159–1166.

[5] G. M. Campedelli, I. Cruickshank, and K. M. Carley, "A complex network approach to find latent clusters of terrorist groups," *Applied Network Science*, vol. 4, no. 1, Art. no. 59, 2019.

[6] P. Choudhary and U. Singh, "A survey on social network analysis for counter-terrorism," *International Journal of Computer Applications*, vol. 112, no. 9, pp. 24–29, 2015.

[7] G. Chen, D. Shen, C. Kwan, J. B. Cruz, and M. Kruger, "Game theoretic approach to threat prediction and situation awareness," in *Proc. 2006 9th International Conference on Information Fusion*, Jul. 2006, pp. 1–8.

[8] M. Everett and S. P. Borgatti, "Ego network betweenness," *Social Networks*, vol. 27, no. 1, pp. 31–38, 2005.

[9] A. Landherr, B. Friedl, and J. Heidemann, "A critical review of centrality measures in social networks," *Business & Information Systems Engineering*, vol. 2, no. 6, pp. 371–385, 2010.

[10] Y. Liang, "An approximate reasoning model for situation and threat assessment," in *Proc. Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007)*, vol. 4, Aug. 2007, pp. 246–250.

[11] L. Lv, K. Zhang, T. Zhang, D. Bardou, J. Zhang, and Y. Cai, "PageRank centrality for temporal networks," *Physics Letters A*, vol. 383, no. 12, pp. 1215–1222, 2019.

[12] D. McDaniel and G. Schaefer, "A data fusion approach to indications and warnings of terrorist attacks," in *Proc. Next-Generation Analyst II*, vol. 9122, May 2014, Art. no. 912204.

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022

[13] A. Najgebauer, R. Antkiewicz, M. Chmielewski, and R. Kasprzak, "The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution," *Journal of Telecommunication and Information Technology*, pp. 14–20, 2008.
[14] S. Petris, C. Georgoulis, J. Soldatos, I. Giordani, R. Sormani, and D. Djordjevic, "Predicting terrorist attacks in urban environments: An Internet-of-Things approach," *International Journal of Security and Its Applications*, vol. 8, no. 4, pp. 195–218, 2014.
[15] W. E. Roper, "Spatial data fusion for infrastructure condition assessment," *Technical Memorandum of Public Works Research Institute*, pp. 270–288, 2003.
[16] F. Saidi, Z. Trabelsi, and H. B. Ghazela, "A novel approach for terrorist sub-communities detection based on constrained evidential clustering," in *Proc. 2018 12th International Conference on Research Challenges in Information Science (RCIS)*, May 2018, pp. 1–8.
[17] K. Sambhoos, R. Nagi, M. Sudit, and A. Stotz, "Enhancement to high level data fusion using graph matching and state space search," *Information Fusion*, vol. 11, no. 4, pp. 351–364, 2010.
[18] S. Singh, S. Verma, and A. Tiwari, "An innovative approach for identification of pivotal node in terrorist network using PROMETHEE method (an anti-terrorism approach)," *International Journal of Engineering & Technology*, vol. 7, no. 1, pp. 95–99, 2018.
[19] S. Singh, S. Verma, and A. Tiwari, "Identification of pivotal nodes in terrorist network using TOPSIS method," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9, 2019.
[20] A. N. Steinberg, "An approach to threat assessment," in *Proc. 2005 7th International Conference on Information Fusion*, vol. 2, Jul. 2005, p. 8.
[21] D. Xuan, H. Yu, and J. Wang, "A novel method of centrality in the terrorist network," in *Proc. 2014 Seventh International Symposium on Computational Intelligence and Design*, vol. 2, Dec. 2014, pp. 144–149.
[22] N. Yusof and A. A. Rahman, "Students' interactions in an online asynchronous discussion forum: A social network analysis," in *Proc. 2009 International Conference on Education Technology and Computer*, Apr. 2009, pp. 25–29.
[23] Government of India, *Mumbai Terrorist Attack (Nov. 26–29, 2008)*, 2009.

DOI: https://doi.org/10.54216/FPA.090206
Received: June 28, 2022 Accepted: September 14, 2022