International Journal of Basic and Applied Sciences, 14 (2) (2025) 247-259

SPC

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/xgbrcc61
Research paper

A Novel Genetic Algorithm-Based Decisive Approach for Detection of Influencing Node in Terrorist Network (An Anti-Terrorism Approach)

Saurabh Singh [1], Madhuri Gokhale [1] *, Om Prakash Chauhan [1], Dr. Kanchan Cecil [1], Dr. S. K. Mahobiya [1], Namarta Sahayam [1], Khushi Koshta [1], Abhay Bairagi [1], D. M. Balaji [1], Preshit Tiwari [1], Dr. Mahesh Motwani [2], Dr. Anu Sayal [3]

[1] Jabalpur Engineering College, Jabalpur, Madhya Pradesh, 482001, India
[2] Rajiv Gandhi Prodhyogiki Vishwavidyalaya, Bhopal, Madhya Pradesh, 462033 India
[3] School of Accounting and Finance, Taylor's University. Subang Jaya, 47500, MALAYSIA
**Corresponding author E-mail: mgokhale@jecjabalpur.ac.in*

Received: April 16, 2025, Accepted: June 10, 2025, Published: June 19, 2025

Abstract

In response to the destructiveness caused by terrorists, a framework for pinpointing pivotal nodes within their networks is necessary. This study introduces a Genetic Algorithm-based framework, progressing through three phases to identify crucial nodes. The first phase filters the network, the second employs the robust Genetic Algorithm to pinpoint critical nodes, and the third phase optimises for enhanced accuracy. Empirical results demonstrate the framework's improvement over conventional centrality-based methods, showing enhancements in concurrence, accuracy, and authenticity. The framework proposes a strategic shift toward focusing on the leaders of terrorist networks. This strategic recalibration optimises law enforcement efforts, streamlining their interventions for maximum impact. The inherent potential of this approach resonates in its capacity to significantly enhance the efficiency of security agencies. By concentrating resources on the nodes that truly matter, a more targeted and impactful counter-terrorism strategy can be forged. This innovative framework thus holds the promise of not only more effective counter-terrorism strategies but also a more adept response to the persistent challenges posed by terrorism.

Keywords: *Betweenness Centrality Measure (BT); Closeness Centrality (CL); Degree Centrality (D); Page Rank Measure (PR); Terrorist Network (Tn).*

1. Introduction

Today, in the internet world, many systems are being represented using networks. The data of these networks becomes social for special purposes. Tremendous progress in the IT world today has enabled the storage, collection, sharing, and processing of vast amounts of data. Also, more powerful CPUs and increased network bandwidth support wealthier data. Many techniques are being used for social data analysis in such networks. Some organisations tend to hide their data and hence refrain it from being shared. They follow covert network procedure, which is social network technique to keep secrecy about the number of entities. Network members keep their identities secret like criminal organisations. There may be activities kept secret because of their illegality. Agencies like INTERPOL and the FBI use network analysis to detect covert threats and disrupt organized terror networks, aiming to minimize the risks of attacks globally.

Terrorist organisations and cyber crimes are increasing day by day on the internet. They form networks very similar to traditional networks. Terrorist networks operate as a unique form of social organisation, placing a significant emphasis on both secrecy and efficiency. Their structure is carefully crafted to enable effective communication among members while avoiding detection.

A terrorist network comprises interconnected nodes and links. Nodes represent individuals within the network, including both masterminds and leaders who play pivotal roles in its structure. Nodes can also be gatekeepers, conveyors, or sleeper cells. Nodes can be grouped to form a community, which can be homogeneous or heterogeneous. Similarly, links are the relationships among nodes. Different criminal organisations connect to recruit new members, exchanging their ideology, propagation messages, and planning malicious objectives too.

Understanding these networks is crucial for counter-terrorism investigations and the formulation of effective strategies to prevent terrorist attacks. In this regard, terrorist network analysis has become a special focus for researchers. Since the terrorist network is growing drastically on the internet, researchers are setting up various social models to track their activities.

Terrorist networks function with a high degree of complexity, making them particularly difficult to detect and destabalise. These networks depend on secrecy to escape law enforcement and intelligence agencies, using encrypted communication, anonymous online forums, and hidden financial transactions inorder to operate freely and undetected. The structure of these organisations is commonly hierarchical, with the key leaders' role being to oversee operations while minimizing their direct involvement to prevent exposure. Sleeper cells remain inactive until there's a need for them for specific missions, making their detection even more complex. These networks also utilize emerging technologies, like cryptocurrency for transactions and social media for recruitment and spreading their ideologies. Understanding the working of these hidden networks is crucial for counter-terrorism efforts. Law enforcement agencies employ advanced data analysis, artificial intelligence, and network mapping techniques to find connections between individuals and discover hidden relationships. Disrupting these networks requires a mix of technological soundness, intelligence gathering, and international cooperation. Preventive measures can be made, such as monitoring online activities of extremists, improving cybersecurity protocols, and implementing stricter regulations on online transactions; these factors can reduce the risk of terrorist activities. With terrorist organisations continuously evolving their practices, researchers and security experts must continuously improve their strategies to stay one step ahead of these threats and ensure global security.

One has to find the main leader seated in a higher-ranking position which communicates to lower-ranking individuals like sleeper cells. To gather this important information on how terrorists form the subgroups and to describe their communication pattern, a graph representation policy is used. Many techniques of traversing the graph are used to analyse the terrorist network. Researchers are focusing on making the early warning system with high accuracy. Identification of key nodes in a graph restricts the network or terrorist organisation to some extent from functioning normally and, to destabilise the network.

Beyond computer science and network theory, this work has meaningful overlap with fields such as criminology, where understanding the behavioural structure and social hierarchies of covert groups is essential. The framework also touches on data privacy concerns, as the extraction and analysis of network data, especially in real-world intelligence settings, necessitates ethical safeguards and anonymisation practices. Thus, this study is positioned at the confluence of computational modelling, security studies, and behavioural forensics, encouraging future interdisciplinary collaboration.

2. Literature survey

Detection and handling of terror-related content over the internet and, thereby, adapting measures to paralyse the actions of terrorist communities and alliances has been a topic of research in the past several years. Various methods and models have been proposed by different researchers across the globe working on the topic. In a paper authored by Alzahrani, T., and Horadam, K. J., a comprehensive analysis of bipartite networks is conducted. The main goal of this research is to reveal secretive terrorist communities that operate clandestinely, containing vital information within their hidden structures.[1]

An alternative organisational approach is proposed in the paper authored by Khaled Dawoud, Alhajj, and Rokne. In contrast to depicting the terrorist network as a graph, this method involves conveying significant information from higher to lower ranks. This is achieved by segmenting the network into levels, each furnishing insights about distinct subgroups within the terrorist network.[2]

In reference (Alzahrani & Horadam, 2014) [1], the network was fragmented into individual components, while in (Dawoud et al., 2010) [2], the network is perceived as a cohesive entity. This viewpoint facilitates the acquisition of detailed information about the key individuals within the network.

The connections among nodes within the terrorist network are considered informative, as suggested by the method proposed by Uffe Kock Wiil, Jolanta Gniadek, and Nasrullah Memon. The pivotal factors on which terrorist networks predominantly depend are efficiency and, secrecy. The calculation of link importance, derived from the betweenness among nodes, contributes to the overall performance product of secrecy and efficiency. This evaluation aids in identifying significant links, thereby facilitating the dismantling of the terrorist network.[3]

As suggested by Kaati L. and Prucha N., text analysis techniques are utilised to identify content associated with terrorism on the internet. In this, a framework is introduced for visualizing terrorism-related content on social networking platforms, particularly Twitter. This model entails the examination of tweets in diverse languages, such as English and Arabic, aiming to detect "media mujahedeen". The identification process involves multiple classifiers, encompassing categories like violence, racism, hate, and anger.[4]

The framework given by Kaati et al. [4] integrates data-independent features that can be universally applied to datasets with comparable characteristics, alongside data-dependent features, which are notably influenced by the unique attributes of the specific dataset in question. In contrast, Dawoud et al. [2] concentrate on deciphering communication patterns among diverse information sources by analyzing text published within mainstream network media. The significance of identifying key terrorists is paramount in the effort to dismantle terrorist networks.

Researchers S. Singh, S. K. Verma, and A. Tiwari employed the ELECTRE method for this purpose. In their analysis of the 26/11 Mumbai attack, "Wassi" was identified as the master node.[5]

In another approach outlined in by Duo-Yong S. et al., Call Detail Records (CDR) are utilised to establish a network connecting callers and receivers. This method proves beneficial in discerning communication patterns among terrorist groups.[6]

The paper written by Maheshwari S. and, Tiwari A. employ a combined knowledge approach involving Multi-meta-Network Analysis, Social Network Analysis (SNA), and Fuzzy Analytical Network Process (FANP). This methodology is utilised to derive scores for different terrorists within the network, encompassing parameters such as total degree, betweenness, closeness, etc., computed by ORA. Weights are assigned based on various criteria and indices, reflecting diverse skills (Role, Resource, Knowledge, and Task) of individual terrorists. The cumulative weight determines the significance of the role a terrorist plays in the network, with a higher weight indicating greater importance and consequently posing a greater threat to society.[7]

In the approach presented by Petersen R. R., Rhodes C. J., and Wiil U. K., the primary objective is to address the Person Successor Problem, aiming to pinpoint the individual most likely to assume the role of a terrorist if they are removed from the network [8]. Conversely, in reference proposed by Ranjan P. and Vaish A., a method involving the amalgamation of various social network user graphs through information sharing is employed. This strategy provides an enhanced understand,ing of all users across different net- works [9].

In 2012, Sachan A. introduced a method based on genetic-based optimisation. This method is designed for optimizing large social networks that include both non- terrorist and terrorist nodes. The initial stage involves the removal of non-terrorist nodes, resulting in a graph comprising exclusively promising nodes. Additionally, a weighted degree centrality measure is proposed to assist in disrupting the terrorist network [10].

Another method uses Grey Relational Analysis to analyse and derive important conclusions from a given data set. This generalisation by S. Singh, S. K. Verma, and A. Tiwari is helpful in the realm of identifying and destabilizing the terrorist networks in a country like India, where terrorism is a constant threat [5].

In 2011, terrorist financing was examined. Methods discussed by Sakharova I described about transferring and storing funds of a terrorist network. The goal of the study is to defeat terrorism by fighting the financial structure of terrorist organisations through the disruption and disablement of their financial network [11].

Another study, proposed in 2012, Spezzano F. and Mannes A., described Dark web analysis. They discussed the dark web as a hotspot where terrorists communicate to spread their ideology and propaganda in various websites embedded in the public internet [12].

In 2011, the research by Tang X. and Yang C. C. delved into the investigation of potential terrorist activities and their interconnectedness in the context of epidemic spread. The research paper utilised various datasets to characterise the dynamics of the epidemic's propagation and employed situational awareness approaches to analyse the associated threats [13].

In a different strategy detailed in a paper by Wiil U. K., Gniadek J., and Memon N., they introduce an algorithm for removing nodes in criminal networks. The selection of nodes for removal considers both the available information and the topology of the criminal networks. The authors present a node removal approach that combines two critical perspectives: an inference-based prediction of new potential links and adjustments in the standard social network degree centrality [3].

In the investigation carried out by B. Collins, D. T. Hoang, N. T. Nguyen, and D. Hwang, researchers presented a novel method for dismantling terrorist networks by utilizing a 4-centrality measure. Following the application of link prediction, they employed Galton-Watson extinction probability-based methods. The results highlighted the significant role of link prediction in uncovering hierarchical structures within terrorist networks. Additionally, the analysis of the 9/11 incident involved an evaluation of link prediction within the M-19 network [14].

In their research, I. Shafi, S. Din, Z. Hussain, I. Ashraf, and G. S. Choi conducted experiments aimed at identifying criminal groups based on their textual data from social media platforms. The textual content was subjected to feature extraction and subsequently trained using a Support Vector Machine (SVM). The efficiency of this method was confirmed in terms of both time and space complexity [15].

In the study by S. Singh, D. Indurkhya, and A. Tiwari, a four-step process is discussed to study the 9/11 terrorist data setdataset based on Betweenness, Closeness, and PageRank centrality network parameters. This study involves allocating ranks based on the computed fitness function, removing the node with the highest rank, and generating a structure using the max heap algorithm [16].

The method mentioned by G. Li, J. Hu, Y. Song, Y. Yang, H.-J. Li, social network theory was employed to analyse the patterns of regularity within terrorist attacks. The study involved an examination of the construction pattern using a distinctive dynamic iterative clustering algorithm. Furthermore, a community division method was utilised to delineate the structure of the terrorist organisation [17].

Jiang et al. (2023) proposed an integrated deep-learning framework that incorporates background context, social networks, and past actions of terrorist groups to discover behavior patterns. Their model outperformed conventional base models at different spatio-temporal resolutions, providing groundbreaking insights into terrorism and other organized violent crimes [26].

Anwar et al. (2022) developed a hybrid deep learning-based framework using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) models to predict future terrorist activities. Their model achieved superior performance in classification tasks, with accuracy exceeding 96% for bi-classification and 99.2% for multi-classification tasks [27].

Building on these insights from prior work, we propose a Genetic Algorithm-based framework that integrates multiple centrality measures to identify the most influential nodes within terrorist networks.

3. Methods

This section delineates the methodology put forth to identify the prominent and impactful members within a terrorist network. A terrorist network often comprises a substantial number of terrorists, here referred to as nodes. Performing operations on this voluminous network and extracting the desired result can be difficult as well as time-consuming. For addressing this issue, a Genetic algorithm has been used to first minimise the solution set and then perform operation on the produced minimised solution set (the reduced terrorist network).

The reduction of the complete terrorist network to the desired nodes is shown in Figure1. Within this framework, we assess several metrics, including Betweenness Centrality (BT), Closeness Centrality (CL), Page Rank (PR), and, Degree Centrality (D) for every node in the given terrorist network or graph.

Analyzing social networks categorises 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.

3.1. Betweenness centrality

BC deal to measure to evaluate the intensity of node's importance in acting as a bridge between the other two nodes. Nodes with aelevated 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 [21].

3.2. Closeness centrality

The process also depends on the closeness between the nodes in a network. Nodes that are situated close to each other are comparatively effective in transmitting information compared to nodes placed at a longer distance. The closeness between nodes refers to the minimum distance between other nodes, geodesics. A geodesic is the minimum path length from Node A to B.21 Closeness centrality of a node is determined as the total graph distance between all other nodes in the network.

Where, as is the distance between two nodes A and B. Nodes with minimum closeness centrality (ie, 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 ratio to the number of links in the paths traversed. Hence, nodes with less CC value are neighbours to most of the nodes in the network.

3.3. Page rank

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 defined by the number of communication links 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 [22].

3.4. Degree centrality

The TDC estimates the importance of a node by evaluating the number of direct relationships of the node with other nodes in the network. 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 [23].

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 undirected network, degree centrality depends on the edges in the graph. The higher the number of edges for a particular node, the higher the value of degree centrality [24].

In-degree and Out-degree Centrality: In-degree and out-degree centrality of degree centrality are shown. Essentially, though, it's an expression in terms of popularity and expansiveness. i.e., in degree centrality is the degree of relation between two node groups A and B. When nodes in group A communicate with other nodes, nodes in group A become (A+B), no matter the source of that information. Nodes with high(in) degree centrality value are more active and therefore they attract more information. The higher the value, the higher will be the degree of centrality and hence the greater will be the power of Node A in the network discourse. An out-degree centrality is related to how information is exchanged between Node (B—A). Nodes with higher out-degree centrality value are likely to be highly interactive nodes from the center of providing comments and information to other nodes in the network. Additionally, it refers to the level of what nodes are actively involved in communication activities [25].

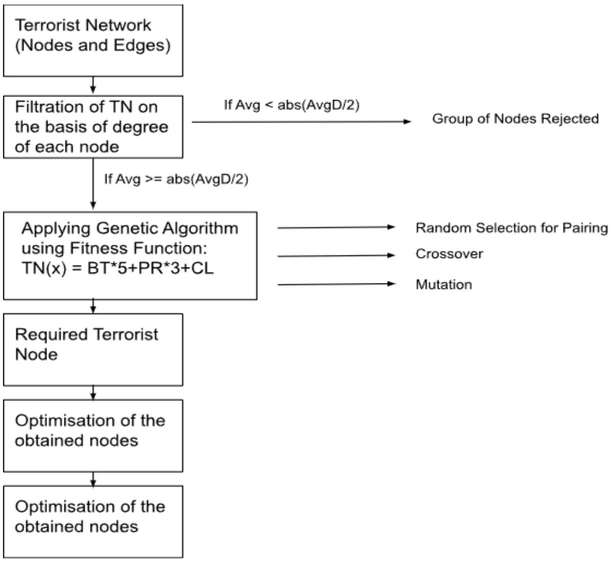
Terrorist Network (Nodes and Edges)
Filtration of TN on the basis of degree of each node
If Avg < abs(AvgD/2)
Group of Nodes Rejected
If Avg >= abs(AvgD/2)
Applying Genetic Algorithm using Fitness Function: TN(x) = BT*5+PR*3+CL
Random Selection for Pairing
Crossover
Mutation
Required Terrorist Node
Optimisation of the obtained nodes
Optimisation of the obtained nodes

Fig. 1: Genetic Algorithm-Based Framework.

The methodology is divided into three phases, namely:

- Filtration of the Terrorist Network.
- Application of Genetic Algorithm on the reduced nodes.
- Optimisation of the obtained nodes.

3.5. Filtration of the terrorist network

To streamline computation and ensure precision in results, the pruning of the provided terrorist network is executed based on the Average Degree Centrality (D). Initially, the Degree Centrality of each node within the terrorist graph is computed, and subsequently, the values are arranged in descending order of D.

The overall average value of D is stored in AvgD Averages of AvgD taken 4 at a time (Avg) are compared with the absolute value of AvgD /2.

If
Avg >= abs(AvgD /2)
A group of nodes are accepted for further operations.

If
Avg < abs(AvgD/2)
A group of nodes are rejected.

3.6. Application of genetic algorithm on reduced nodes

After obtaining the reduced graph containing the terrorist nodes, a Genetic Algorithm (GA) is employed. The GA operates in three main phases:

- Random Selection for pairing
- Crossover
- Mutation

A crucial component of the GA is the fitness function, which identifies and ranks the most significant nodes. This involves evaluating three parameters for each node within the terrorist network: Betweenness Centrality (BT), Closeness Centrality (CL), and Page Rank (PR).
The fitness function for node x is defined as:

$$TN(x)=BT\times 5+PR\times 3+CL \tag{1}$$

This function assigns different weights to each parameter based on their priority, with Betweenness Centrality receiving the highest priority and Closeness Centrality the lowest.
Upon filtration, 12 nodes remain in the graph. The fitness function is calculated for each node before proceeding with the three phases. During the Random Selection phase, four nodes are chosen randomly and paired together, forming three groups from the 12 nodes. The sum of the fitness function values for these four nodes constitutes the group's fitness function.
During the Crossover phase, nodes are interchanged between groups at corresponding positions. For example, if nodes A, B, C, D, E, F, G, and H are involved:

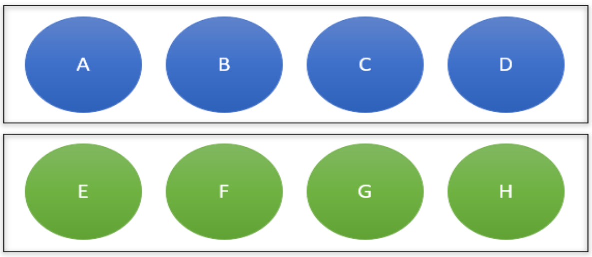

Fig. 2: Before Crossover.

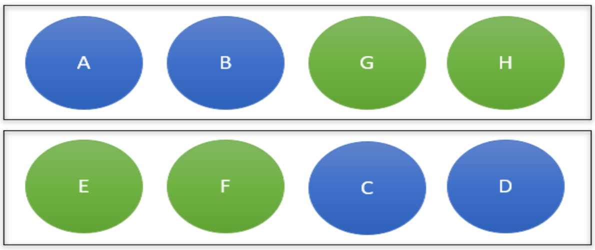

Fig. 3: After Crossover.

In the proposed model, nodes are swapped as illustrated, and the fitness function for each new group is recalculated. If the new group's fitness function is greater than the previous one, it is retained for further processing; otherwise, the best previous group remains unchanged.
Finally, the Mutation phase addresses situations where adjusting the position of a single node is necessary to achieve the maximum fitness function. Here, the position of a single node may be flipped to optimise the group's overall fitness.
To ensure reproducibility and transparency, we define the key parameters used in our Genetic Algorithm framework:

- Population Size: 3 groups of 4 nodes (12 nodes in total after filtration)
- Crossover Rate: 0.8
- Mutation Rate: 0.1
- Number of Generations: 10
- Selection Mechanism: Random pairing followed by fitness-based evaluation
- Crossover Strategy: Two-point crossover, where node positions are swapped between groups
- Mutation Strategy: Swap or flip individual nodes based on fitness gain
- Fitness Function: TN(x)=BT×5+PR×3+CLTN(x) = BT \times 5 + PR \times 3 + CLTN(x)=BT×5+PR×3+CL

Parameter Tuning:
Initial experimentation was conducted using values ranging from 0.6 to 0.9 for crossover rate and 0.05 to 0.2 for mutation rate. The final values (0.8 crossover, 0.1 mutation) were selected as they produced the most stable convergence in fewer generations without overfitting. Convergence was assessed by observing the stabilization of the group fitness value over iterations (as illustrated in Figure 13).
Computational Complexity:
The complexity is primarily driven by the number of nodes and the centrality calculations. For a network of NNN nodes:

- Degree, Closeness, and PageRank centralities: O(N2)O(N^2)O(N2)
- Genetic operations (selection, crossover, mutation): O(G·P)O(G \cdot P)O(G·P), where GGG is the number of generations and PPP is population size

The overall framework remains efficient for medium-sized graphs (10–500 nodes), and filtration based on Degree Centrality significantly reduces computational overhead.

3.7. Optimisation of the obtained nodes

After executing the three phases, the best group—defined as the one with the maximum fitness function—is identified as the required terrorist group. To achieve the most accurate and optimised result, further refinement is necessary. This involves ordering the obtained nodes based on their Page Rank measure. By doing so, we can identify the most influential node within the group, thereby obtaining the desired result.

4. Experimental result

The information regarding individuals associated with Lashkar-e-Taiba implicated in the 26/11 Mumbai bomb blast, along with their associates, is presented [18] in Table 1. This table presents the communication data among members of the terrorist group involved in the 26/11 Mumbai attacks. The data is structured as an adjacency matrix, representing the connections between 13 members. Each row and column corresponds to an individual, with entries indicating communication links between them. The data taken into consideration is the communication between their members, taken from Ze L., et al., which is in the form of an adjacency matrix. This sample data contains 13 members of the terrorist group [19].

Using the given data in Table 1, a terrorist network graph is generated as shown in Figure 4, representing the nodes as well as the links between each of the 13 nodes.

Table 1: Sample Data of 26/11 Attack

	Ajmal Amir Kasab	Ismail Khan	Na-sir	Baba Imran	Fahad-ullah	Abdul Rehman	Abu Umer	Abu Shoaib	Javed	Hafiz Arshad	Zarar	Wassi	Abu Kaahfa
Ajmal Amir Kasab	0	0	0	0	0	0	0	0	0	0	0	1	0
Ismail Khan	0	0	0	0	0	0	0	0	0	0	0	0	1
Nasir	0	1	0	0	0	0	0	0	0	0	0	0	0
Baba Im-ran	0	1	0	0	0	0	0	0	0	0	0	0	0
Fahad- ul-lah	0	0	0	0	0	0	0	1	0	0	0	0	0
Abdul Rehma-n	0	0	0	0	0	0	0	0	1	0	0	0	0
Abu Umer	0	1	0	1	1	1	0	0	0	0	0	0	0
Abu Shoaib	0	0	0	1	0	0	1	0	0	0	0	0	0
Javed	0	0	0	1	0	1	1	0	0	0	0	0	0
Hafiz Ar-shad	0	1	0	0	1	1	1	0	0	0	0	0	0
Zarar	1	1	0	0	0	0	0	0	1	0	0	0	0
Wassi	1	0	1	1	0	0	1	0	0	1	1	0	0
Abu Kaahfa	0	1	1	0	0	0	0	1	0	0	0	1	0

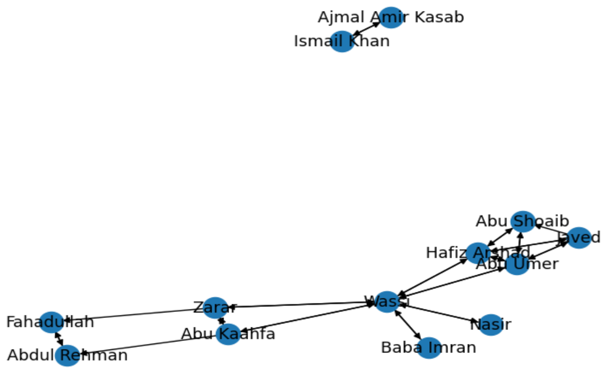

Fig. 4: Terrorist Network.

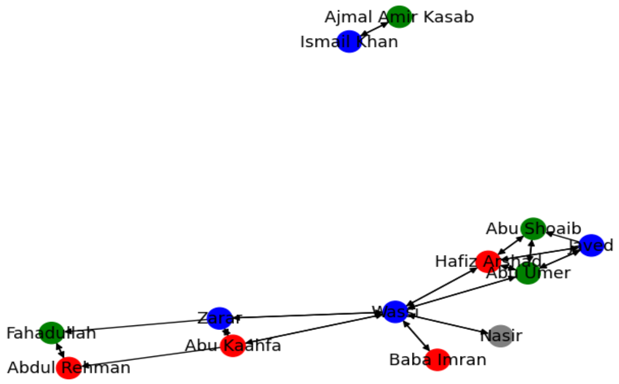

Fig. 5: Terrorist Network after Filtration and Grouping.

Table 2: Degree Centrality (D) and Average D

Rank	Agent	Degree Centrality (D)	Average D taken 4 at a time (Avg)
1	Abu Umer	8	8.25
2	Wassi	7	
3	Hafiz Arshad	8	
4	Abu Kaahfa	5	
5	Abu Shoaib	5	4.50
6	Javed	5	
7	Zarar	3	
8	Abdul Rehman	3	
9	Fahadullah	3	2.25
10	Ajmal Amir Kasab	2	
11	Baba Imran	2	
12	Ismail Khan	2	
13	Nasir	2	NA
Total average		4.77	

Out of the 13 nodes available, a total of 12 nodes are chosen as shown in Fig. 5, forming three distinct groups. The subsequent phase involves applying the genetic algorithm to this dataset. Various metrics, including Betweenness Centrality (BT), Page Rank (PR), and Closeness Centrality (CL), are computed, and based on these factors, the fitness function for each node is determined. The resultant values are presented in Table 3.

Table 3: Calculated Values of Betweenness, Closeness Centrality, Along with Page Rank and Fitness Function

Rank	Agent	Betweenness Centrality (CT)	Page Rank (PR)	Closeness Centrality (CL)	Fitness Function TN(x)
1	Wassi	54	0.198	0.016	270.61
2	Abu Umer	12.5	0.113	0.016	62.855
3	Hafiz Arshad	13	0.113	0.016	62.855
4	Abu Kaahfa	8	0.084	0.015	37.767
5	Abu Shoaib	0	0.06	0.014	0.194
6	Javed	0	0.076	0.014	0.242
7	Zarar	7.5	0.084	0.015	37.767
8	Abdul Rehman	0.5	0.02	0.019	2.579
9	Fahadullah	0.5	0.02	0.019	2.579
10	Ajmal Amir Kasab	0	0.077	0.007	0.238
11	Baba Imran	0	0.04	0.014	0.134
12	Ismail Khan	0	0.077	0.007	0.238

Table 4: Group I Fitness Function Values

Rank	Agent Group I	Individual TN()
1	Wassi	270.610
12	Ismail Khan	0.238
6	Javed	0.242
7	Zarar	37.767
Total TN()	308.857	

Table 5: Group II Fitness Function Values

Rank	Agent Group II	Individual TN()
5	Abu Shoaib	0.194
2	Abu Umer	62.855
9	Fahadullah	2.579
10	Ajmal Amir Kasab	0.238
Total TN()	103.335	

Table 6: Group III Fitness Function Values

Rank	Agent Group I	Individual TN()
8	Baba Imran	0.134
2	Abdul Rehman	2579
9	Hafiz Arshad	62.855
10	Abu Kaahfa	37.767
Total TN()	103.335	

4.1. Application of genetic algorithm

4.1.1. Random pairing

The filtered nodes are randomly paired in groups of 4 members each. As previously mentioned, 3 groups are formed and, for each group, the total Fitness function value is calculated:
Total Group Fitness Function = Sum of 4 nodes' fitness function. Tables 4, 5, and 6 show the result of this step.

4.1.2. Crossover

The next steps involve crossover and mutation to achieve the desired optimal result. The crossover process comprises two distinct steps, depicted in Figures 6 and 7 below, with the corresponding changes in fitness value per crossover shown in Figure 8.

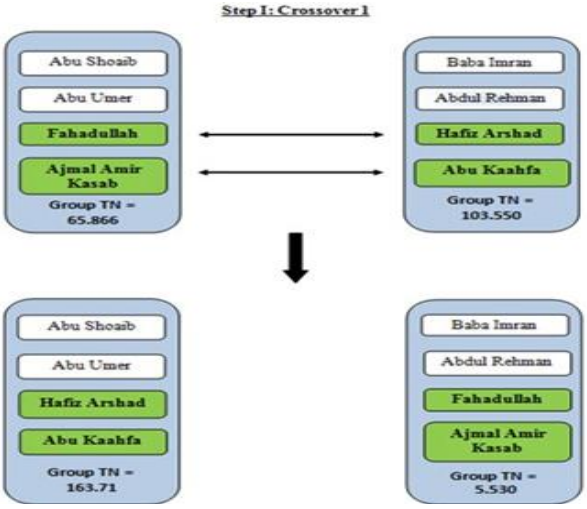

Fig. 6: Crossover Between Initial 2 Groups.

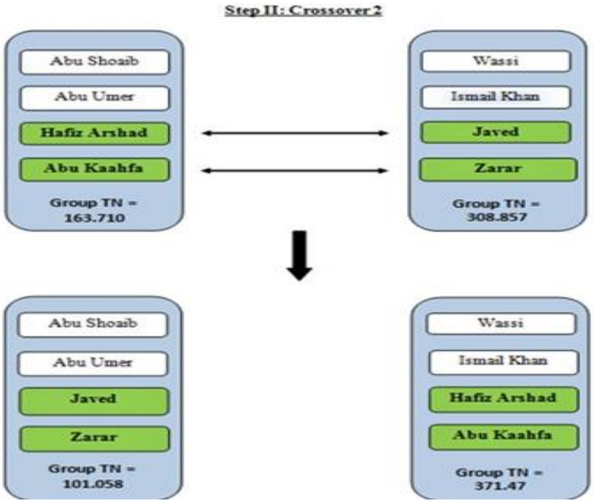

Fig. 7: Crossover between Generated as Well as Original.

In the first step of the crossover, as illustrated in Figure 6, the last two elements of both groups are swapped with each other. The resultant group with the higher fitness function then swaps its elements with the third group. This crossover aims to form a group with members whose individual fitness function values contribute maximally to the group's overall fitness.

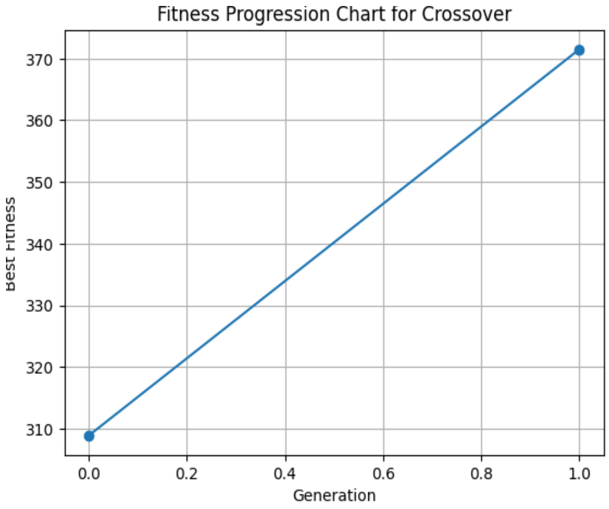

Fig. 8: Fitness Progression Chart for Crossover.

4.1.3. Mutation

Mutation occurs after the crossover when it becomes necessary to switch individual node elements. The steps involved in this process for the sample data are shown in Figures 9 and 10, and the changes in fitness value over each mutation are depicted in Figure 11.

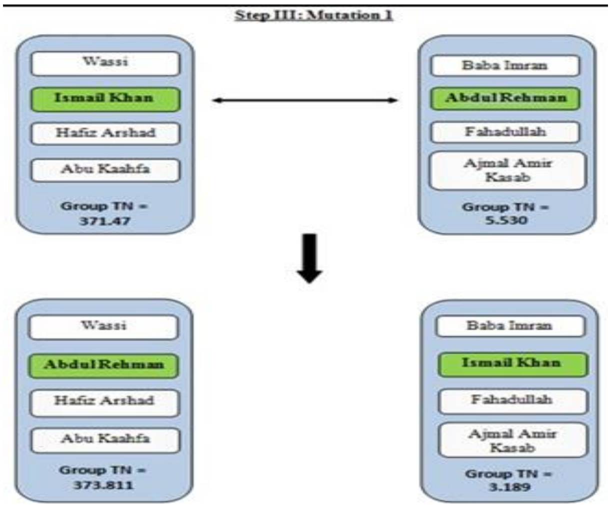

Fig. 9: Mutation Step 1.

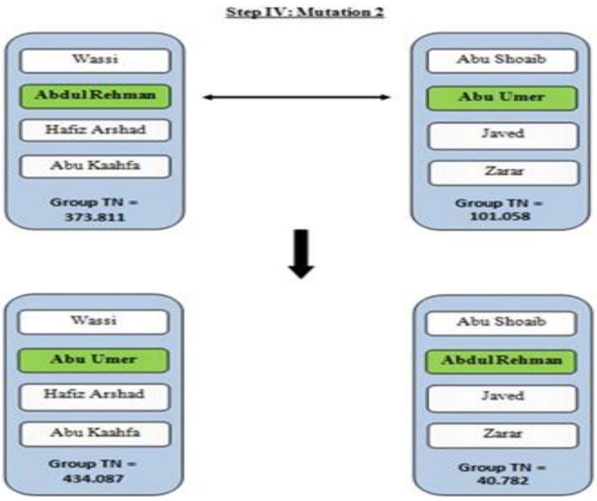

Fig. 10: Mutation Step 2.

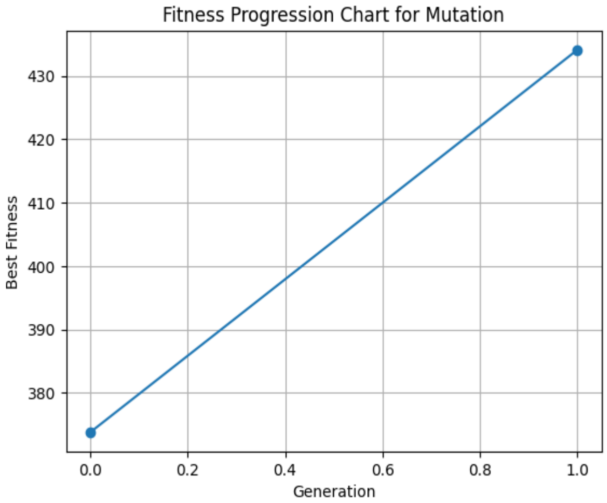

Fig. 11: Fitness Progression Chart for Mutation.

4.1.4. Genetic algorithm application result

After executing the genetic algorithm and evaluating the final terrorist nodes, the group containing Wassi, Abu Umer, Hafiz Arshad, and Abu Kaahfa exhibited the highest fitness function value, identifying them as the chief members of the network. These values are presented in Table 7, with a pictorial representation in Figure 14.

Figures 12 and 13 effectively illustrate the progression of the optimal group through successive generations of the genetic algorithm, highlighting the concurrent increase in its fitness value throughout the optimization process.

Figure 12 (Generation Plot) provides a clear visual representation of member selection across four generations. Blue dots indicate selected members in each generation, while gray X marks show non-selected members. The progression reveals critical insights:

- Wassi remains consistently selected across all generations, confirming his central importance in the network
- Higher-value members like Abu Kaahfa and Hafiz Arshad are incorporated by generation 2 and remain stable

- Lower-fitness members like Javed and Zarar from generation 1 are systematically replaced
- By generation 4, the algorithm converges on the optimal group (Wassi, Abu Kaahfa, Hafiz Arshad, Abu Umer)

Figure 13 (Overall Fitness Progression Chart) complements this by quantitatively tracking the fitness function increase with each generation, demonstrating how the algorithm's selection choices progressively improved the group's collective importance score. The chart shows significant jumps in fitness value during early optimization phases, followed by more incremental improvements as the algorithm fine-tunes the selection in later generations.

Together, these visualizations effectively demonstrate both the qualitative composition changes and quantitative fitness improvements achieved through the genetic algorithm's optimization process, providing compelling evidence for the identification of the network's most critical members.

4.1.5. Optimisation of given nodes

In any organisation, a hierarchical structure determines the importance of individuals, with those at the top being more significant than those below them. The head of a department typically communicates tasks through intermediaries, such as managers, rather than directly to beginners. Similarly, in a terrorist network, the importance of each node is influenced by its neighbors.

To detect the leader or essential member of the terrorist network, nodes are arranged in decreasing order of their Page Rank. Page Rank helps to rank nodes based on the importance of their neighbors, effectively identifying the most influential members within the network.

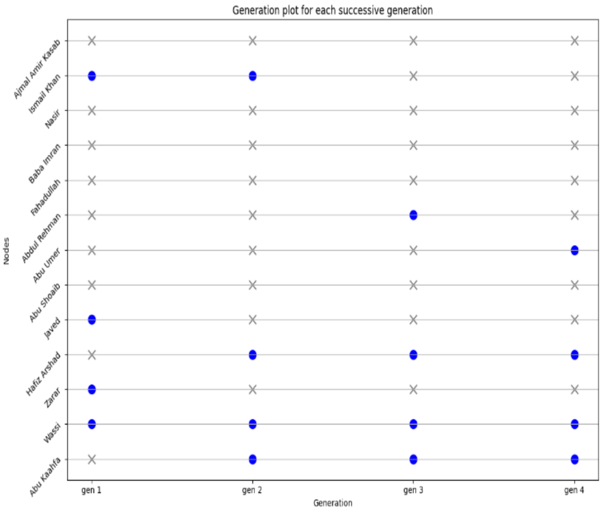

Fig. 12: Generation Plot for Each Successive Generation.

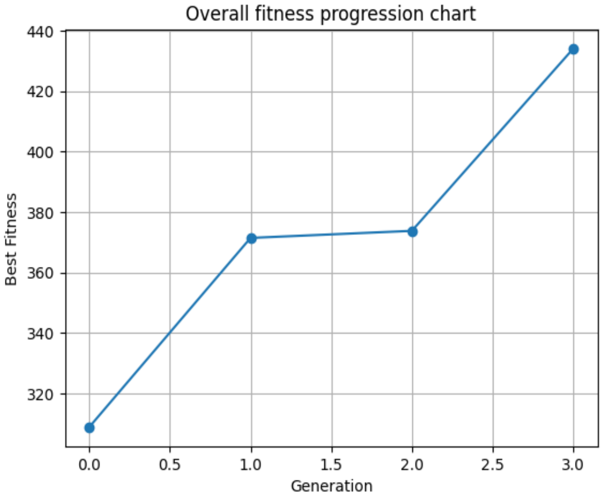

Fig. 13: Overall Fitness Progression Chart.

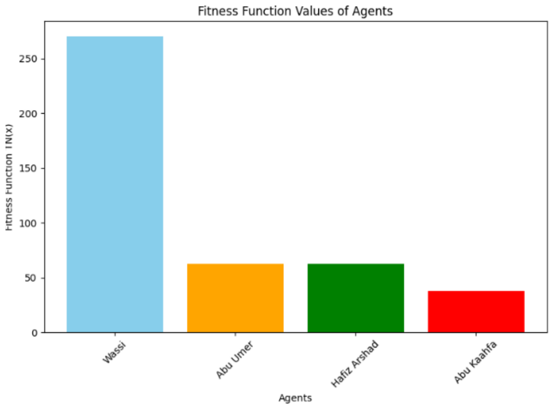

Fig. 14: Bar Chart Representing Fitness Function of the 4 Resultant Nodes.

Optimised Result
As shown in Table 8, Wassi has the highest Page Rank, indicating that he is the most important member of the network. By using the algorithm, the desired result can be achieved efficiently, both in terms of time and computational resources.

5. Analysis & validation against 26/11 mumbai attack

The data considered for visualisation was for the 26/11 Mumbai terror attack, and the data was obtained from reports obtained from the Government of India. Measurement analysis shows that Wassi was the most central, leading, and controlling node, which is in alignment with the report obtained from the government. This suggests that the proposed methodology can be used to develop a counter-terrorism strategy which concentrates on the key node identification and its ego network to obtain maximum network disruption Mumbai terrorist attack [20].

6. Comparison of previous work & the proposed model

Numerous approaches have been proposed to identify significant members within terrorist networks. Most of these rely on traditional centrality measures such as Degree, Betweenness, Closeness, and PageRank, or use decision-support models like ELECTRE or FANP. While effective to a degree, such models often focus solely on individual node scores, neglecting interdependencies, group behaviour, or scalable optimisation techniques.

The proposed model addresses these limitations through a novel Genetic Algorithm (GA)-based three-phase framework. This approach differentiates itself in the following ways:

- Weighted Multi-Centrality Fitness Function: Rather than averaging centrality values or using them individually, the proposed model creates a composite fitness function that weights Betweenness, PageRank, and Closeness centralities based on their relative importance, enhancing the precision of key node identification.
- Degree-Based Network Pruning: An initial filtration step based on Degree Centrality ensures reduced computational complexity and focuses only on highly connected nodes for further processing.
- Group-Based Evolutionary Optimization: Unlike prior models that assess nodes in isolation, this approach groups nodes (in sets of four) and evolves them using Genetic Algorithm operators—random selection, crossover, and mutation—leading to more holistic insights into network dynamics.
- Ego Network Awareness via PageRank: After GA convergence, results are refined using PageRank to capture the influence of a node's neighbors, an aspect often underrepresented in earlier work.
- Validated with Real-World Data: The model is validated using the 26/11 Mumbai attack dataset, correctly identifying “Wassi” as the most central figure, aligning with official reports. This confirms both its reliability and practical relevance.

To summarize the advancements of this model, the following table compares it with notable existing methods:

Table 7: Comparative Analysis of the Proposed Model with Prior Works

Aspect	Alzahrani & Horadam (2014)	Sachan (2012)	S. Singh et al. (2020)	Proposed Model (This Paper)
Centrality Measures Used	Degree Centrality (graph decomposition)	Weighted Degree Centrality	Multiple centralities via ELECTRE	Degree, Betweenness, Closeness, PageRank (weighted)
Optimization Technique	None	Partial (genetic-based filtering)	Multi-criteria decision-making	Full Genetic Algorithm with selection, crossover, and mutation
Network Reduction Approach	Component-based segmentation	Removal of non-terrorist nodes	Not specified	Degree Centrality–based pruning via average threshold
Focus on Node Groups	No	No	No	Yes – optimises nodes in groups of four
Use of Fitness Function	No	Implicit	No	Yes – TN(x) = BT×5 + PR×3 + CL
Ego Network Influence	Limited	No	No	Yes – Post-GA ranking using PageRank
Validation Dataset	Simulated bipartite networks	Synthetic networks	26/11 dataset	26/11 dataset with real adjacency matrix
Real-World Alignment	Conceptual	Partial	Aligned (Wassi identified)	Strong – Wassi identified, matching the government report
Scalability	Moderate	Moderate	Low	High – due to filtration and GA efficiency

The integration of multi-layered centrality analysis, group-based evolutionary optimisation, and real-world data validation ensures that the proposed model not only identifies the most influential individuals but also captures the group dynamics critical to an effective counter-terrorism strategy. This approach offers a significant improvement in terms of accuracy, scalability, and actionable insight compared to existing methods.

7. Conclusion and future work

The successful application of the Genetic Algorithm-based framework to the 26/11 case study highlights its potential for broader adoption in counter-terrorism efforts. By leveraging communication patterns and network structures, this approach can unveil the hidden hierarchies and command chains within terrorist organisations, enabling a targeted and impactful response.

Future research can explore the integration of additional data sources, such as financial transactions, travel patterns, and online activity, to further enhance the framework's predictive capabilities. Additionally, adapting the model to evolving terrorist tactics and communication methods will be crucial in maintaining its relevance and efficacy in the ever-changing security landscape.

Overall, the proposed methodology's ability to accurately identify the key influencers in the 26/11 attacks serves as a testament to its potential in supporting counter-terrorism operations, fostering a safer and more secure global environment.

This research also opens up opportunities for interdisciplinary collaboration. Incorporating criminological theories, such as the study of radicalisation, organisational behaviour, and cell formation, could enhance the model's sociological validity. Furthermore, addressing data privacy challenges by embedding anonymisation and ethical data handling techniques will be essential for deploying such frameworks responsibly in operational environments. The proposed methodology's ability to accurately identify key influencers in the 26/11 attacks serves as a testament to its potential in supporting counter-terrorism operations and fostering a safer global environment.

8. Ethical considerations

The application of advanced algorithms and data-driven techniques in counter-terrorism research raises significant ethical issues, particularly regarding the use of sensitive personal information. While the proposed Genetic Algorithm-based framework has demonstrated its effectiveness in identifying key influencers within terrorist networks, the methods employed must ensure the privacy and security of individuals' data.

- Data Privacy and Security: Given that the framework utilizes communication patterns, travel data, financial transactions, and online behavior, it is crucial to implement robust data anonymization and encryption techniques. Personal information must be protected to prevent misuse, and the framework should comply with international data protection standards such as the General Data Protection Regulation (GDPR) or similar regulations.
- Informed Consent and Transparency: If the framework is to be deployed in real-world operational environments, it is important to ensure transparency regarding the types of data being collected and analyzed. If feasible, gaining informed consent from individuals whose data may be utilized should be considered, ensuring that participants understand the scope and implications of their data being part of the analysis.
- Bias and Fairness: Data used in such frameworks may be inherently biased, potentially leading to misidentification or disproportionate focus on specific communities. Researchers should be mindful of such biases and strive to ensure fairness in the analysis, preventing the misuse of the technology for profiling or unjust surveillance.
- Accountability and Oversight: Ethical oversight is vital when developing and deploying technologies that can have significant societal impacts. Independent review bodies should be established to ensure that counter-terrorism frameworks are used in compliance with ethical standards and human rights principles.
- Balancing Security and Privacy: While the need for security is paramount, it is essential to strike a balance with the right to privacy. Counter-terrorism strategies should focus on maximizing public safety without compromising individuals' fundamental rights to privacy and freedom of expression.

By addressing these ethical considerations, the proposed methodology can be deployed in a responsible and accountable manner, fostering both security and respect for civil liberties.

References

[1] Alzahrani, T., & Horadam, K. J. (2014). Analysis of two crime-related networks derived from bipartite social networks. 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014), 890–897. https://doi.org/10.1109/ASONAM.2014.6921691.

[2] Dawoud, K., Alhajj, R., & Rokne, J. (2010). A Global Measure for Estimating the Degree of Organization of Terrorist Networks. 2010 International Conference on Advances in Social Networks Analysis and Mining, 421–427. https://doi.org/10.1109/ASONAM.2010.84.

[3] Wiil, U. K., Gniadek, J., & Memon, N. (2010). Measuring Link Importance in Terrorist Networks. 2010 International Conference on Advances in Social Networks Analysis and Mining, 225–232. https://doi.org/10.1109/ASONAM.2010.29.

[4] Kaati, L., Omer, E., Prucha, N., & Shrestha, A. (2015). Detecting Multipliers of Jihadism on Twitter. 2015 IEEE International Conference on Data Mining Workshop (ICDMW), 954–960. https://doi.org/10.1109/ICDMW.2015.9.

[5] Singh, S., Verma, S. K., & Tiwari, A. (2020). A novel approach for finding crucial node using ELECTRE method. International Journal of Modern Physics B, 34(09), 2050076. https://doi.org/10.1142/S0217979220500769.

[6] Duo-Yong, S., Shu-Quan, G., Hai, Z., & Ben-Xian, L. (2011). Study on covert networks of terroristic organizations based on text analysis. Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, 373–378. https://doi.org/10.1109/ISI.2011.5984117.

[7] Maheshwari, S., & Tiwari, A. (2015). A Novel Genetic Based Framework for the Detection and Destabilization of Influencing Nodes in Terrorist Network. In L. C. Jain, H. S. Behera, J. K. Mandal, & D. P. Mohapatra (Eds.), Computational Intelligence in Data Mining—Volume 1 (Vol. 31, pp. 573–582). Springer India. https://doi.org/10.1007/978-81-322-2205-7_53.

[8] Petersen, R. R., Rhodes, C. J., & Wiil, U. K. (2011). Node Removal in Criminal Networks. 2011 European Intelligence and Security Informatics Conference, 360–365. https://doi.org/10.1109/EISIC.2011.57.

[9] Ranjan, P., & Vaish, A. (2014). Apriori Viterbi Model for Prior Detection of Socio-Technical Attacks in a Social Network. 2014 International Conference on Engineering and Telecommunication, 97–101. https://doi.org/10.1109/EnT.2014.11.

[10] Sachan, A. (2012). Countering terrorism through dark web analysis. 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), 1–5. https://doi.org/10.1109/ICCCNT.2012.6396055.

[11] Sakharova, I. (2011). Al Qaeda terrorist financing and technologies to track the finance network. Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, 20–25. https://doi.org/10.1109/ISI.2011.5984044.

[12] Spezzano, F., Subrahmanian, V. S., & Mannes, A. (2013). STONE: Shaping terrorist organizational network efficiency. Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 348–355. https://doi.org/10.1145/2492517.2492626.

[13] Xuning Tang, & Yang, C. C. (2010). Generalizing terrorist social networks with K-nearest neighbor and edge betweeness for social network integration and privacy preservation. 2010 IEEE International Conference on Intelligence and Security Informatics, 49–54. https://doi.org/10.1109/ISI.2010.5484776.

[14] Collins, B., Hoang, D. T., Nguyen, N. T., & Hwang, D. (2022). A New Model for Predicting and Dismantling a Complex Terrorist Network. IEEE Access, 10, 126466–126478. https://doi.org/10.1109/ACCESS.2022.3224603.

[15] Shafi, I., Din, S., Hussain, Z., Ashraf, I., & Choi, G. S. (2021). Adaptable Reduced Complexity Approach Based on State Vector Machine for Identification of Criminal Activists on Social Media. IEEE Access, 9, 95456–95468. https://doi.org/10.1109/ACCESS.2021.3094532.

[16] Singh, S., Indurkhya, D., & Tiwari, A. (2018). An avant-garde approach for detection of key individuals with leader hierarchy determination using FIMAX Model (Anti—Terrorism approach). 2018 International Conference on Information Management and Processing (ICIMP),89–99. https://doi.org/10.1109/ICIMP1.2018.8325847.

[17] Li, G., Hu, J., Song, Y., Yang, Y., & Li, H.-J. (2019). Analysis of the Terrorist Organization Alliance Network Based on Complex Network Theory. IEEE Access, 7, 103854–103862. https://doi.org/10.1109/ACCESS.2019.2929798.

[18] Singh, saurabh kumar. (2024). 26/11 Mumbai Terror Network Communication Dataset (Version 1.0) [Dataset]. Zenodo.

[19] Li, Z., Sun, D., Guo, S., & Li, B. (2014). Detecting key individuals in terrorist network based on FANP model. 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014), 724–727. https://doi.org/10.1109/ASONAM.2014.6921666.

[20] Report on “Mumbai Terrorist Attacks (Nov.26-29, 2008)” https://zenodo.org/records/14887023.

[21] Singh, Saurabh, Shashikant Verma, and Akhilesh Tiwari. "Identification of Pivotal node in Terrorist Network using TOPSIS Method."(14) Avaliable Online.

[22] Landherr, Andrea, Bettina Friedl, and Julia Heidemann. "A critical review of centrality measures in social networks." Business & Information Systems Engineering 2 (2010): 371-385. (21) https://doi.org/10.1007/s12599-010-0127-3.

[23] Berzinji, Ala, Lisa Kaati, and Ahmed Rezine. "Detecting key players in terrorist networks." In 2012 European Intelligence and Security Informatics Conference, pp. 297-302. IEEE, 2012.(15) https://ieeexplore.ieee.org/abstract/document/6298852. https://doi.org/10.1109/EISIC.2012.13.

[24] Campedelli, Gian Maria, Iain Cruickshank, and Kathleen M Carley. "A complex networks approach to find latent clusters of terrorist groups." Applied Network Science 4, no. 1 (2019): 1-22. (16) https://doi.org/10.1007/s41109-019-0184-6.

[25] Yusof, Norazah, and Azizah Abdul Rahman. "Students' interactions in online asynchronous discussion forum: A Social Network Analysis." In 2009 International Conference on Education Technology and Computer, pp. 25-29. IEEE, 2009.(17) https://ieeexplore.ieee.org/abstract/document/5169446. https://doi.org/10.1109/ICETC.2009.48.

[26] Jiang D, Wu J, Ding F, Ide T, Scheffran J, Helman D, Zhang S, Qian Y, Fu J, Chen S, Xie X, Ma T, Hao M, Ge Q. An integrated deep-learning and multi-level framework for understanding the behavior of terrorist groups. Heliyon. 2023 Aug 6;9(8):e18895. PMID: 37636372; PMCID: PMC10457427. https://doi.org/10.1016/j.heliyon.2023.e18895.

[27] Anwar, R., Hussain, I., & Chen, Z. (2022). A hybrid deep learning-based framework for predicting future terrorist activities. Egyptian Informatics Journal, 23(3), 437–446. https://doi.org/10.1016/j.eij.2022.04.001.

Appendices

Appendix1:
https://zenodo.org/records/14887023.