Received: 13 August 2021 | Revised: 27 January 2022 | Accepted: 20 February 2022

DOI: 10.4218/etrij.2021-0239

ORIGINAL ARTICLE

ETRI Journal WILEY

Identifying the leaders and main conspirators of the attacks in terrorist networks

Abhay Kumar Rai[1] | **Sumit Kumar**[2]

[1]Department of Computer Science, Banasthali Vidyapith, Rajasthan, India

[2]Centre of Computer Education, IPS, University of Allahabad, Allahabad, India

Correspondence
Abhay Kumar Rai, Department of Computer Science, Banasthali Vidyapith, Rajasthan, India.
Email: abhay.jk87@gmail.com

Abstract

This study proposes a novel method for identifying the primary conspirators involved in terrorist activities. To map the information related to terrorist activities, we gathered information from different sources of real cases involving terrorist attacks. We extracted useful information from available sources and then mapped them in the form of terrorist networks, and this mapping provided us with insights in these networks. Furthermore, we came up with a novel centrality measure for identifying the primary conspirators of a terrorist attack. Because the leaders of terrorist attacks usually direct conspirators to conduct terrorist activities, we designed a novel algorithm that can identify such leaders. This algorithm can identify terrorist attack leaders even if they have less connectivity in networks. We tested the effectiveness of the proposed algorithms on four real-world datasets and conducted an experimental evaluation, and the proposed algorithms could correctly identify the primary conspirators and leaders of the attacks in the four cases. To summarize, this work may provide information support for security agencies and can be helpful during the trials of the cases related to terrorist attacks.

KEYWORDS

counter terrorism, network analysis, structure of terrorist networks, terrorism, terrorist networks

1 | INTRODUCTION

In the last few decades, multiple terrorist activities have been reported around the world. Any terrorist activity brings threats to human beings and damages the public property of a country. Thus, preventing terrorist attacks is among the most prominent goals related to the national security of any country. Across the whole world, most countries face the problem of terrorism and thus invest considerable amounts of money in their security agencies. Moreover, the ultimate aim of the security agencies of any country is to take preventive measures such that terrorist acts can be prevented.

One of the approaches of analyzing terrorist activities is to represent a complete terrorist activity in the form of a network. The actors involved in an attack (directly or indirectly) or those who are part of a conspiracy act as nodes, and the interactions or associations between these actors act as links.

Many centrality-based techniques have been previously designed for identifying the key actors involved in terrorist activities. We can broadly categorize key actors into two categories: main conspirators and attack leaders. The first category of key actors is the primary conspirators who have direct involvement in the planning and execution of an attack. Such actors can be identified using network theory-based techniques. In general, centrality-based methods are most suitable for identifying such actors because they measure the influence of each node present in a network. The second category of actors, the leaders, who do not have direct involvement in the attacks, are weakly connected to the network, and they only provide instructions for their subordinates to perform terrorist activities. Therefore, in a network, they show little participation. Existing network theory-based techniques cannot identify such actors. To our knowledge, none of the existing methods can identify the leaders of a terrorist attack.

The formulation used in centrality-based techniques cannot capture the information related to the leaders of terrorist attacks. In most cases, leaders hire or influence other people to plan an attack. Then, the planners hire their subordinates to recruit attackers, provide technical support to the attackers, arrange trainers for the attackers, and arrange the arms and other logistics required for the execution of the attack. The people in terrorist networks demonstrate different behaviors from those of the people in social networks. Berzinji and others [1] used five centrality-based techniques to identify the key actors in terrorist networks. They took those nodes as key actors who have top-k centrality scores for most of the centrality measures. However, the leaders of terrorist attacks cannot be identified using such techniques. Another limitation with existing methods is that they do not determine the relative contribution of an individual in an overall conspiracy or attack. Therefore, a mechanism is required for identifying the primary conspirators and leaders of terrorist attacks and the share of each individual in the whole act.

In this study, we aimed to come up with a solution for identifying the primary conspirators and leaders of terrorist attacks. We created a ranking list for the people involved in terrorist activities such that the primary conspirators occupy the top positions of the list. Through this list, the role of each individual in an attack can be identified. Moreover, we designed a novel algorithm that can identify the leaders of terrorist attacks and then evaluated the effectiveness of the proposed method using four real-world terrorist network datasets. The experimental results indicated the effectiveness of the proposed method in identifying the primary conspirators and leaders over all the used datasets.

1.1 | Motivation

Many efforts have been made by researchers to address the global issue of terrorism, and in most of them, centrality-based measures were used to identify the key actors related to terrorist activities. However, in real-world terrorist networks, the existing network theory-based or centrality-based methods are insufficient for identifying each category of the key actors. The flow of information in such networks is different from that in other real-world networks such as social networks, biological networks, and citation networks.

In any terrorist network, the leaders do not actively participate in the planning and execution of an attack, and they only instruct their subordinates to perform attacks. However, in reality, they are the most responsible people for any terrorist attack. The second category of key actors, the main conspirators, plays active roles in the planning and execution of attacks, and they can be identified by applying existing network theory-based concepts such as centrality-based measures. This is because they have several associations within a network. Moreover, an adequate level of information flows through such actors. The leaders of terrorist attacks cannot be identified by existing network theory measures because they only have a few associations within the network. Moreover, little information flows through the leaders.

The contribution of each actor cannot be measured in an overall attack using the existing methods. One example is betweenness centrality, which gives zero scores for many actors even if they actively participate in the planning and execution of attacks. This is practically demonstrated later in Section 5.1. To cope with these limitations, we have been motivated to provide solutions to these limitations. The proposed solutions in this study can identify both categories of the key actors and identify their shares in overall terrorist activities.

In this study, we used four real-world cases to prepare our datasets. Furthermore, we defined a centrality-based measure to identify the key conspirators directly involved in terrorist attacks. This measure can determine the share of each actor in an overall terrorist activity. Moreover, we designed an algorithm for identifying the leaders of terrorist attacks, where the basic idea behind this algorithm is that the masterminds of terrorist attacks are only associated with the top conspirators.

Using the proposed method, we calculated centrality scores for identifying the primary conspirators and their relative contributions to terrorist attacks. We designed a separate algorithm for detecting the leaders who do not look active in terrorist networks. The performance of the proposed algorithms was examined on four real-world datasets. Unlike other methods, the proposed algorithms

could successfully identify both the primary conspirators and leaders of the attacks.

1.2 | Contributions

The contributions of this paper are as follows:

1. We prepared real-world datasets of terrorist networks using the proceedings and confessional statements of the accused people in four real-world cases.
2. We propose a novel centrality-based measure for identifying the main conspirators and their relative contributions to terrorist networks. This method incorporates the concept of the shortest path in identifying the primary conspirators.
3. We propose a novel algorithm for identifying the leaders of the terrorist attacks who are not directly visible in the terrorist network.
4. We performed an experimental evaluation of the proposed method using the prepared datasets.

2 | RELATED WORK

Many methods for analyzing terrorist networks have been designed in the past few decades [2–11]. Certain good survey papers and studies on terrorist networks are available in existing literature [12–20]. In most cases, centrality-based measures were used to identify the primary conspirators in terrorist networks. Out of many, we discuss here some of the most known cases. Sparrow [10] used six centrality-based measures, three concepts related to equivalence and a concept of weak ties, to examine their relevance so as to analyze terrorist networks. He efficiently presented a method of applying these concepts to terrorist networks so as to extract useful information from them. The extracted information can be used by law enforcement agencies to take preventive measures against terrorism.

Berzinji and others [1] used some centrality-based measures for identifying the key actors involved in terrorist activities. They computed the centrality scores corresponding to all the nodes present in a terrorist network using different centrality-based measures and determined the nodes as the key actors with the maximum scores in the majority of cases. Gialampoukidis and others [5] presented a novel centrality-based measure named mapping entropy betweenness (MEB) for identifying the key players present in terrorist networks, and they tested the effectiveness of their method on a dataset prepared using terrorism-related user accounts on Twitter.

Burcher and Whelan [14] gathered information related to criminal networks from the qualitative interviews of two criminal intelligence analysts belonging to Australian state law enforcement agencies. They applied certain existing measures available in the network theory to analyze the gathered information, which helped in understanding the structural characteristics of criminal networks. Bright and others [2] applied certain social network analysis measures to Australian-based jihadist groups to analyze them, and the purpose of the analysis was to identify the hidden connections among the groups. Some of them looked to be separate in the used network; however, they facilitated the work of other groups by providing information and resources. The method of Bright and others could identify the actors who acted as bridges among the groups present at different locations.

Su and others [19] presented a link prediction-based approach for disintegrating terrorist networks, and they designed a link prediction-based method for identifying the critical nodes present in terrorist networks. To illustrate their work, they used the 9–11 hijackers network, and their approach identified missing relationships among the members of the terrorist organization involved in the 9–11 attack. Mitzias and others [7] presented a unified semantic infrastructure for identifying the contents related to the terrorist activities available on the web. Their method uses ontology and the concept of adaptable semantic reasoning to understand the behaviors of terrorist networks.

In their work, Gregori and Merlone [15] used the following popular measures available in the network theory with the aim of analyzing 10 terrorist networks including three Islamic State of Iraq and Syria-affiliated networks: centralization [21], density [22], mean nodal degree [22], clustering coefficient [23], average path length [22], average efficiency [24], global efficiency [24], betweenness [25], and closeness [22]. In their work, they investigated all the networks to understand their structural characteristics and measured the impact of an attack conducted by terrorists using information extracted from the structural characteristics of the networks. Singh and others [9] presented a method named gray relational analysis (GRA) to organize and analyze terrorist networks, and this method is under the category of structural-based methods. They applied their method to a dataset based on the 26/11 Mumbai attack to test its effectiveness. In addition to these methods, the following interesting methods were proposed in recent years: other studies [26–38]. Most of these methods are based on community detection approaches, where they use time-series features and other network theory concepts to analyze terrorist networks. The basic idea behind these approaches is to

divide terrorist organizations into communities and attack them to reduce the possibility of joint resistance.

The above discussion shows that the existing methods mostly used centrality-based measures for identifying the key actors in terrorist networks. Centrality-based approaches capture the information flow corresponding to the different nodes present in a network. Based on this information, they rank the persons involved in a terrorist activity and identify those who occupy the top positions in the list as the key actors, which can be either primary conspirators or leaders. However, in reality, leaders only have indirect involvement in terrorist attacks and even look as persons with little involvement in the attacks. Therefore, information flow through such nodes is low. Thus, an alternative method is required to identify the leaders of terrorist attacks.

In addition to centrality-based measures, some researchers proposed learning-based methods [11,39–43] in recent years to identify the key actors in terrorist networks. Johnston and Weiss [39] designed an approach that can automatically identify the related web pages and text content to Sunni extremist propaganda on social media, where a deep neural network-based model is used to classify propaganda content from other social media content. The model can classify text written in multiple languages. Tutun and others [11] presented a framework that uses the information related to the patterns of suicide attacks for analyzing the activity patterns and relations in terrorist networks. The analysis results can be used to understand the behaviors and movements of terrorists. In particular, they proposed a logistic regression-based model for selecting features for the similarity function and used this model in analyzing terrorist networks. Moussaoui and others [40] presented a probabilistic-based clustering algorithm for identifying the potential communities involved in terrorist activities on Twitter. The overall approach works in three steps: extraction of tweets, semantic processing, and classification of the nodes forming a community of terrorists. They classified the people on Twitter into three groups: terrorists, people who support them, and those who do not have any involvement in terrorist activities. Accordingly, they could identify a community of terrorists.

Rasheed and others [41] designed a machine learning-based method for identifying the key actors in terrorist networks. As a preprocessing step, the *k*-core concept is used in removing the passive or unwanted nodes from given networks. In the next step, a hybrid classifier that utilizes multiple features is used to identify the key actors in the network. Wang and Li [43] presented a behavior-aware network embedding approach named outlier spotting with behavior-aware network embedding (OSNE) to identify the terrorists belonging to different terrorist organizations. The basic idea behind their method is to gather information from the high-order relation paths among the members of terrorist groups.

Then, this information is used for network embedding to identify the potential entities in a network. To our knowledge, the most recent learning-based method was proposed by Uddin and others [42]. They used certain deep neural network-based models to understand the behaviors of the people involved in terrorist activities. Using five learning-based models, they tried to answer some questions. For example, (i) depending on the planning level, is a particular attack successful or not? (ii) Are the attackers ready to commit suicide or not? (iii) What can be the probable place of an attack? (iv) What weapon types are going to be used in an attack? (v) What are the possible targets of an attack (e.g., people, buildings, and public property)? Because none of the abovementioned approaches can identify the leaders of terrorist attacks because of their indirect involvement in attacks, a novel method for identifying the leaders of terrorist attacks is necessary.

The novelty of the proposed approach compared with other existing methods in identifying key actors is as follows. (i) Unlike other existing methods, our method can identify the leaders in terrorist networks even if they do not look active in a network. (ii) The proposed method enables us to identify the key conspirators who get instructions from leaders to conduct terrorist activities. (iii) Through the proposed method, the persons involved in a terrorist activity can be ranked based on their relative contributions to the whole activity. (iv) We prepared four datasets using proceedings and confessional statements made by certain accused persons corresponding to four real-world cases. The proposed algorithms can identify all the key actors and whether they have direct or indirect involvements in attacks in the four cases.

3 | PROPOSED METHOD

The proposed method works in two steps. In the first step, we apply the proposed proximity-based centrality measure to compute the proximity of each node present in a terrorist network. The top conspirators of an attack can be determined based on the proximity scores calculated using the proposed centrality measure. In the second step, we apply the proposed algorithm for identifying the leaders of terrorist networks. We demonstrated a brief overview of the proposed method using the flow chart in Figure 1.

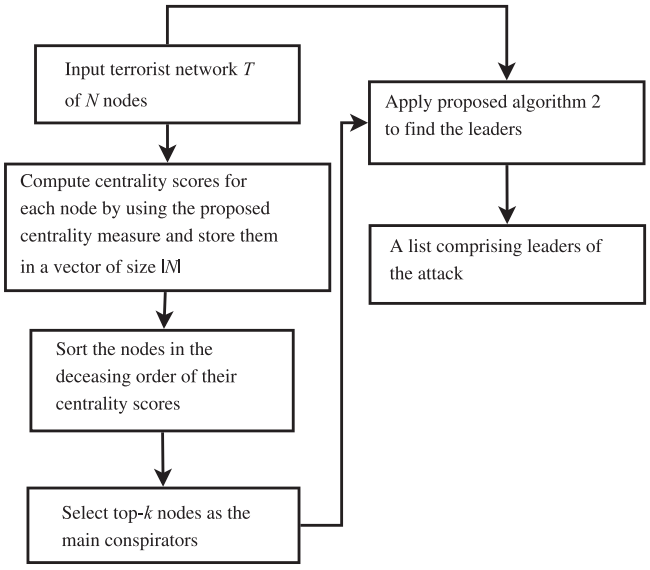

FIGURE 1 Flow chart of the proposed method

3.1 | Defining the proposed centrality measure

In a terrorist network, let $T = (N, L)$, where N represents the set of persons contributing to terrorist activities and L represents the set of links or associations among the people involved in terrorist activities. Here, we considered T as a simple undirected, unweighted, and connected network. The proposed centrality measure is based on the shortest path algorithm [44,45]. According to Sabidussi [46], the centrality of a node can be measured by adding the shortest distances from that node to all the other nodes in a network. This quantity measures how closely a node is to all the other nodes in the network. Furthermore, to measure the overall centrality of the network, we summed the centrality scores for all the nodes present in the network. If the overall centrality is divided by the centrality score of an individual node, it yields the relative centrality of that node compared with the other nodes present in the network. Therefore, the proposed centrality measure determines how close a node is to all the other nodes in a network and what is its relative closeness compared with the other nodes.

The formal definition of the proposed centrality measure is given as follows. The proximity centrality of a node (v) present in a terrorist network (T) is given as follows:

$$P_T^c(v) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}|\text{spath}_{i,j}|}{\sum_{i=1}^{n}|\text{spath}_{v_i}|}$$

where n is the number of nodes present in the network, $|\text{spath}_{i,j}|$ is the length of the shortest path between the nodes i and j, and $|\text{spath}_{v_i}|$ is the length of the shortest path from node v to i.

3.2 | Proposed algorithms for identifying the primary conspirators and leaders

Here, we present two algorithms for two purposes. The first algorithm identifies the list of persons directly involved in terrorist activities such as recruiting attackers, recruiting people who provide support systems to the attackers, arranging training camps for the attackers, and arranging sophisticated weapons for conducting the attacks. We utilized the concept of the shortest path algorithm to design this algorithm. This concept considers a terrorist network as the input and produces a list of primary conspirators as the output.

In particular, the algorithm takes a terrorist network as an input and computes the proximity score for each node using the proposed proximity-based centrality measure. Then, it sorts all the nodes in the decreasing order of their centrality scores. In the final step of the algorithm, the top-k nodes with the highest scores are selected as the primary conspirators of the attack. Identifying the value of k is an important issue because the number of main conspirators may vary for different terrorist networks. Here, we considered all the main conspirators with the top-3 centrality scores. The outline of the proximity-based centrality measure is given in Algorithm 1.

Algorithm 1 Proximity-based centrality measure

Input: Terrorist network $T(N, L)$
Output: Accused list
Begin
netGraph ← Read network data from file
for each vertex $v \in$ *netGraph* **do**
  shPath ← shortest path from v to other vertices
  pLength ← length of each shortest path
  sumofpLength ← *sumofpLength* + *pLength*
  totalScore ← *totalScore* + *sumofpLength*
end for
for each vertex $v \in$ *netGraph* **do**
  proxCentrality ← *totalScore* / *sumofpLength* for v
end for
accList ← List of top 3 v according to *proxCentrality*
Print *accList*
End

The second algorithm identifies the leaders or masterminds, who are usually not directly involved in terrorist attacks but provide directions to the primary conspirators. The basic idea behind the proposed algorithm for identifying these leaders is simple, as it is based on the observation that the leaders only interact with the primary conspirators and nobody else. The outline for identifying the leaders of the terrorist attacks corresponding to given terrorist networks is given in Algorithm 2.

Algorithm 2 Finding leaders of the terrorist attacks

Input: *netGraph* and *accList*
Output: Leader list
Begin
nAccList ← Set difference of *netGraph* and *accList*
neList ← Calculate neighbors for each *v* in *netGraph*
for each vertex $v \in nAccList$ **do**
  len ← length of set difference of *neList* of *v* and *accList*
  if *len* = 0 **then**
    Add to *leaderList*
  end if
end for
Print *leaderList*
End

4 | EVALUATION STRATEGY

We considered four real-world cases and prepared four datasets corresponding to these cases to evaluate the proposed algorithms. We run Algorithm 1 on each of these datasets and obtained the output in the form of centrality scores corresponding to each node present in a particular dataset. We maintained the centrality scores temporarily in a vector and sorted the vector of the centrality scores in a decreasing order. Then, we predicted the top-*k* nodes with the highest centrality scores as the primary conspirators. Furthermore, we run Algorithm 2 to identify the attack leaders corresponding to the given datasets. The algorithm takes a vector containing centrality scores as the input and produces a list of the comprising leaders of an attack as an output.

4.1 | Data gathering and dataset preparation

Gathering information related to terrorist networks from social media or through other means of communication is extremely difficult because of the covert nature of such networks [47]. We considered four real-world cases related to terrorist attacks from India to prepare the used datasets: 1991 Rajiv Gandhi assassination case [48,49], 2001 Indian Parliament attack case [50–52], 26/11 Mumbai attack (2008) case [53–55], and 1993 Bombay bomb blast case [56,57].

First, we extensively examined and analyzed all four cases to prepare the datasets. Based on this study, we discussed certain facts related to all the cases one by one. Sivarasan, Subha, and Santhan played central roles in the Rajiv Gandhi assassination case. Sivarasan arranged everything for the conduct of the assassination, and Shubha and Santhan accompanied Sivarasan everywhere, even after the assassination. Prabhakaran and Pottu Amman were the leaders because they formulated the attack plan and directed the primary conspirators to plan and execute the attack. As for the Indian parliament attack case, Afzal Guru, Mohammad, and Tariq were the main conspirators, and Afzal Guru played a central role in the attack as he planned the attack on the Indian parliament in collaboration with Mohammad and Tariq. Mohammad is another main conspirator who came to Delhi to make proper arrangements, gather necessary information, and arrange other logistics for the attack. Tariq is a main conspirator because he introduced Afzal Guru to Ghazibaba and he was involved in managing the necessary funds and attackers to perform the attack. As the leader of the operation, Ghazibaba directed the top conspirators to attack the Indian parliament.

Abu Kafa, Hafiz Sayeed, and Zaki-ur-Rehman Lakhvi played central roles in the 26/11 Mumbai attack case. Abu Kafa was involved in organizing training camps for the attackers and made all the necessary arrangements for them. Hafiz Sayeed and Zaki-ur-Rehman Lakhvi were primarily involved in the planning of the attack. Major General Saab, as a leader, formulated a plan with the primary conspirators to conduct terrorist attacks on big Indian cities, and he was continuously in touch with the main conspirators. In the 1993 Bombay bomb blast case, Tiger Memon, Phanasmiyan, and Yakub Memon were the main conspirators. Tiger Memon and Phanasmiyan played central roles in the attack plan from the moment of its inception, and they received the arms and ammunition used in the attack with their men from the sea coasts of Mumbai. Yakub Memon assisted Tiger Memon in the acquisition, transportation, and storage of the used arms and explosives. Moreover, Yakub actively participated in all the meetings held in Bombay and arranged funds through Hawala. Dawood Ibrahim was the leader because he directed the two primary conspirators to plan the attack.

We prepared four datasets after thoroughly studying the four cases, and we collected information from many

sources to prepare these datasets. The information sources include certain judgments of the Supreme Court of India, certain articles published in newspapers, and certain confessional statements made by some of the accused terrorists. The summary statistics of the input graphs related to the prepared datasets are given in Table 1.

4.2 | Experimental setup

We used the R programming language to implement all the centrality-based measures. More specifically, we executed all the algorithms on R version 3.6.3 and R-Studio version 1.2.5042. We took all the observations on a 64-bit computer system with an Intel(R) Core(TM) i5-8265U CPU @1.60 GHz 1.80-GHz processor coupled with 8 GB of primary memory.

5 | EXPERIMENTAL EVALUATION

First, we discussed the proposed method using a case study to understand how it works. Then, we evaluated the performance of the proposed method against other existing methods considering the used four real-world datasets.

5.1 | Case study

There are many challenges when dealing with terrorist networks using social network analysis techniques. These challenges include the noncompleteness of data, difficulty in data gathering, and the covert nature of certain key actors. We designed a novel approach comprising a centrality measure and an algorithm to cope with these challenges. We used the Indian Parliament Attack case of 2001 as a case study to explain our methodology for identifying the primary conspirators and leaders of the attack. Two terrorist organizations, Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM), were involved in the planning and execution of the attack. LeT is one of the largest terrorist organizations in South Asia. Hafiz Saeed, Zafar Iqbal, and Abdullah Azzam established this group in 1987. LeT was involved in many terrorist attacks in India. Moreover, India, the United Nations, and many countries around the world have labeled LeT as a terrorist organization. JeM is another terrorist group that was involved in several terrorist attacks in India. Most countries and organizations around the world have labeled JeM as a terrorist group.

Terrorists from these two groups were involved in the planning and execution of the Indian Parliament attack. As discussed earlier in Section 4.1, first, we prepared a dataset corresponding to this case.

Based on the extracted information, as shown in Figure 2, we showed the people involved in the planning

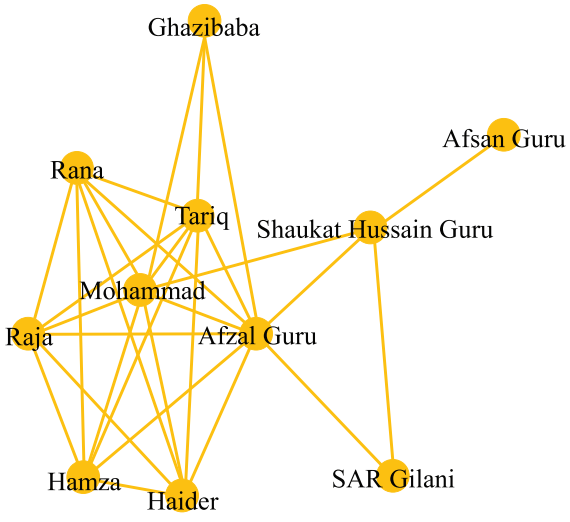

FIGURE 2 Example of a terrorist network corresponding to the Indian parliament attack case. The nodes in the network represent the terrorists who contributed to the planning and execution of the attack, and the links between the nodes represent the associations among the people involved in the attack

TABLE 1 Dataset summary statistics

Name	Type	Nodes	Edges	Description
Indian parliament attack	Undirected	11	29	Network of a terrorist group involved in the Indian parliament attack (private)
26/11 Mumbai attack	Undirected	36	139	Network of a terrorist group involved in the 26/11 Mumbai attack (private)
Rajiv Gandhi assassination	Undirected	46	155	Network of a terrorist group involved in the assassination of Rajiv Gandhi (private)
1993 Bombay bomb blast	Undirected	143	1085	Network of a terrorist group involved in the 1993 Bombay Bomb Blast (private)

and execution of the attack and their associations. We ran the proposed centrality measure and other existing centrality-based measures on the prepared dataset. The centrality scores corresponding to all the methods are shown in Table 2. Here, it can be seen that the actors with high centrality scores were more involved in the conspiracy than the others, whereas the actors with low centrality scores were less involved.

The above observations show that according to the proposed methods of flow-betweenness centrality [58] and degree centrality [5], the top three actors/conspirators of the parliament attack case are Afzal Guru, Mohammad, and Tariq. However, according to the betweenness centrality measure [15], Afzal Guru, Shaukat Hussain Guru, and Mohammad are the top three conspirators of the attack in decreasing order. The analysis in Section 4.1 justifies the results obtained by the proposed method for the parliament attack case. The names of the primary conspirators are present in the proceedings of the case.

To identify the leader, we applied Algorithm 2 to the results of Algorithm 1. The algorithm identified Ghazibaba as the leader who directed the conspirators to plan and execute the attack on the Indian Parliament. It is important to note that none of the centrality measures had the highest centrality score for Ghazibaba, and their results indicate that Ghazibaba was not very much involved in the attack. The reason for this result is that Ghazibaba was not directly involved in the attack, as he only directed the top conspirators to conduct the attack. However, the proposed algorithm successfully identified him as the mastermind behind the attack.

5.2 | Performance of the proposed method against the other methods

We evaluated the performance of the proposed method with regard to the accuracy of finding the main conspirators and leaders of terrorist attacks. We used centrality measures for the performance analyses, as they can assign a numerical value to each node of a network as per its influence on the other nodes. A higher centrality score represents more influence. Therefore, a person (node) with a high centrality score is most properly more involved in an attack than others. We used different centrality measures to measure the influences of the nodes in a network from different perspectives. For example, the proposed centrality measure determines how close a node is to all the other nodes in a network. Betweenness centrality determines how much information flows through a node. The nodes that frequently lie on the shortest paths between other nodes have high betweenness centrality scores. The flow-betweenness centrality determines the total maximum flow mediated by a node v, and the degree centrality determines how many neighbors a node has. Here, we compared the proposed centrality measure with the betweenness centrality, flow-betweenness centrality, and degree centrality. Then, we applied all the methods to each dataset to find the centrality scores of each node. Subsequently, we recorded the five persons with the highest centrality scores, as shown in Tables 3–6.

In the Indian parliament attack case [50–52], the names of the primary conspirators are Afzal Guru, Mohammad, and Tariq. Afzal Guru is on the primary conspirator list because he played a central role in the attack.

TABLE 2 Actors and their centrality scores based on different centrality measures for the dataset of the Indian parliament attack case

Node ID	Actor	Proximity centrality	Betweenness centrality	Flow-betweenness centrality	Degree centrality
1	Mohammad	14.500000	7.333333	56	0.8
2	Afzal Guru	15.818182	13.833333	86	0.9
3	Shaukat Hussain Guru	10.875000	9.500000	36	0.4
4	SAR Gilani	9.666667	0	16	0.2
5	Afsan Guru	6.960000	0	0	0.1
6	Ghazibaba	9.666667	0	6	0.3
7	Raja	11.600000	0	30	0.6
8	Haider	11.600000	0	30	0.6
9	Rana	11.600000	0	30	0.6
10	Hamza	11.600000	0	30	0.6
11	Tariq	12.428571	1.333333	44	0.7

TABLE 3 Top five actors by different centrality measures in the attack case dataset of the Indian parliament

Proximity centrality		Betweenness centrality		Flow-betweenness centrality		Degree centrality	
Name	**Score**	**Name**	**Score**	**Name**	**Score**	**Name**	**Score**
Afzal Guru	15.818	Afzal Guru	13.833	Afzal Guru	86	Afzal Guru	0.900
Mohammad	14.500	Shaukat Hussain Guru	9.500	Mohammad	56	Mohammad	0.800
Tariq	12.429	Mohammad	7.333	Tariq	44	Tariq	0.700
Raja	11.600	Tariq	1.333	Shaukat Hussain Guru	36	Raja	0.600
Haider	11.600	SAR Gilani	0.000	Raja	30	Haider	0.600

TABLE 4 Top five actors based on different centrality measures for the dataset of the 26/11 Mumbai attack case

Proximity centrality		Betweenness centrality		Flow-betweenness centrality		Degree centrality	
Name	**Score**	**Name**	**Score**	**Name**	**Score**	**Name**	**Score**
Abu Kafa	56.735	Kasab	218.955	Kasab	630	Abu Kafa	0.686
Hafiz Sayeed	52.453	Hakim Saab	110.286	Hafiz Sayeed	564	Hafiz Sayeed	0.657
Zaki-ur-Rehman Lakhvi	52.453	Abu Kafa	108.440	Abu Kafa	552	Zaki-ur-Rehman Lakhvi	0.657
Kasab	48.772	Abu Abdul Rehman	96.000	Zaki-ur-Rehman Lakhvi	542	Zarar Shah	0.514
Zarar Shah	47.931	Hafiz Sayeed	79.319	Hakim Saab	388	Abu Hamza	0.486

TABLE 5 Top five actors based on different centrality measures for the dataset of the Rajiv Gandhi assassination case

Proximity centrality		Betweenness centrality		Flow-betweenness centrality		Degree centrality	
Name	**Score**	**Name**	**Score**	**Name**	**Score**	**Name**	**Score**
Sivarasan	78.421	Sivarasan	454.163	Sivarasan	1326	Sivarasan	0.733
Subha	62.958	Santhan	149.205	Santhan	742	Santhan	0.467
Santhan	62.083	Subha	109.108	Subha	594	Subha	0.444
Murugan	56.582	Murugan	65.302	Murugan	446	Murugan	0.333
Arivu	55.875	Jayakumar	54.803	Jayakumar	378	Jayakumar	0.289

TABLE 6 Top five actors based on different centrality measures for the dataset of the 1993 Bombay bomb blast case

Proximity centrality		Betweenness centrality		Flow-betweenness centrality		Degree centrality	
Name	**Score**	**Name**	**Score**	**Name**	**Score**	**Name**	**Score**
Tiger Memon	228.957	Tiger Memon	3103.552	Tiger Memon	18 126	Tiger Memon	0.521
Phanasmiyan	210.929	Phanasmiyan	2773.779	Phanasmiyan	13 402	Phanasmiyan	0.366
Yakub Memon	194.821	Sultan Sayyed	1575.832	Sultan Sayyed	8276	Shahnawaz Qureshi	0.359
Nasir Dakhla	194.115	Sharif Parkar	770.968	Sharif Parkar	6538	Zakir Hussain Noor	0.345
Parvez Mohammed	192.719	Sanjay Dutt	552.000	Mohammed Ali Khan	3536	Farooq Mohammed Yusuf	0.324

As for Ghazibaba, who is a top-ranking commander of Jaish-e-Mohammed and a deputy commander of the terrorist group Harkat-ul-Ansar, he planned the attack on the Indian parliament in collaboration with Mohammad and Tariq. Afzal arranged the houses in which the terrorists stayed and provided other logistics required for the attack. Mohammad is another primary conspirator who came to Delhi before the other terrorists to make proper arrangements, gather necessary information, and arrange other necessary materials for the attack. In the

main conspirator list, we put the name of Tariq. He introduced Afzal Guru to Ghazibaba and worked as a messenger of Ghazibaba during the planning and execution processes of the attack. Moreover, he arranged the necessary funds and attackers. The above discussion indicates that Ghazibaba is the leader of the attack; he directed the top conspirators to attack the Indian parliament.

Table 3 shows that Afzal Guru, Mohammad, and Tariq are the top three conspirators corresponding to the proposed centrality measure, flow-betweenness centrality, and degree centrality. According to the betweenness centrality, Afzal Guru, Shaukat Hussain Guru, and Mohammad are the top three conspirators. The discussion in the last paragraph justifies the efficiency of the proposed centrality measure. Hence, the proposed centrality measure performed well for the dataset of the Indian parliament attack case.

In the 26/11 Mumbai attack case [53–55], the names of the main conspirators are Abu Kafa, Hafiz Sayeed, and Zaki-ur-Rehman Lakhvi. Abu Kafa is present in the main conspirator list because he played a central role in the attack together with Hafiz Sayeed and Zaki-ur-Rehman Lakhvi. He was involved in organizing training camps and marine training for the attackers. Moreover, he showed some places to be attacked using Google Earth and made all the necessary arrangements needed for the attackers (e.g., sophisticated weapons and other logistics). Moreover, he saw the attackers off and gave them the final instructions related to the attack. Hafiz Sayeed, the cofounder of Lashkar-e-Taiba (LeT) and the chief of Jama'at-ud-Da'wah (JuD), is present in the main conspirator list. He was present everywhere during the planning of the attack and instructed the attackers from time to time during their training. Furthermore, he arranged funds, support staff for training, support staff for technical support, sophisticated weapons, and all the other necessary logistics. Zaki-ur-Rehman Lakhvi, an Islamist, operational commander and top leader of the militant group Lashkar-e-Taiba, is part of the main conspirator list, as he actively participated in the planning of the Mumbai attack. He gave speeches and other instructions to the attackers from time to time and attended all the meetings with Major General Saab, a Pakistani army officer, Abu Kafa, and Hafiz Sayeed. Major General Saab was the leader because he directed the conspirators to plan attacks on big Indian cities. Furthermore, he arranged trainers from the Pakistani army, visited training camps many times, and monitored the progress of trainees. Moreover, he was continuously in touch with the main conspirators.

As shown in Table 4, Abu Kafa, Hafiz Sayeed, and Zaki-ur-Rehman Lakhvi are the three main conspirators according to the proposed centrality measure and degree centrality measure. As per the betweenness centrality, Kasab, Hakim Saab, and Abu Kafa are the three main conspirators. The flow-betweenness centrality identified Kasab, Hafiz Sayeed, and Abu Kafa as the three main conspirators. To summarize, the discussion in the last paragraph justifies the accuracy of the proposed centrality measure.

In the Rajiv Gandhi assassination case [48,49], the top conspirator is Sivarasan, who arranged everything for the assassination of Rajiv Gandhi. In the main conspirator list, the names of Subha and Santhan can be added after Sivarasan. Shubha is present in the main conspirator list because she accompanied Sivarasan everywhere, even after the assassination. She was present at the assassination location with Thanu, a suicide bomber who conducted the attack. Shubha successfully escaped alive from the assassination location after the attack. Because of the abovementioned reasons, she must be part of the main conspirator list. Santhan was present in the main conspirator list because he came to India with Sivarasan in the same batch of Thanu and Shubha. The other members came to India in groups on different dates. Santhan accompanied Sivarasan during the whole process, even after the attack, and he is a member of the intelligence wing of LTTE (a terrorist organization). Prabhakaran and Pottu Amman were the leaders of the whole conspiracy; they directed the conspirators to plan and execute the attack. Prabhakaran was the supreme leader of LTTE, and Pottu Amman was heading the intelligence wing of LTTE.

According to Table 5, Sivarasan, Subha, and Santhan are the three main conspirators according to the proposed centrality measure. According to the betweenness centrality, flow-betweenness centrality, and degree centrality, Sivarasan, Santhan, and Subha are the three main conspirators. Here, note that the order of Santhan and Subha is different for the betweenness centrality, flow-betweenness centrality, and degree centrality. However, the names of the top three main conspirators are the same for all the centrality measures. The discussion in the last paragraph justifies the correctness of the outcome corresponding to the proposed centrality measure.

In the 1993 Bombay bomb blast case, the names of the main conspirators are Tiger Memon, Phanasmiyan, and Yakub Memon. Tiger Memon and Phanasmiyan are present in the main conspirator list because they played a central role in the attack starting from its inception under the influence of Dawood Ibrahim. They were present in the first meeting, which was held in Dubai to formulate the terrorist attack plan in Bombay. The reason for this conspiracy was to take revenge for the demolition of the Babri Masjid in Ayodhya. Tiger Memon with his men received arms and ammunitions from the sea coasts of Bombay. He sent some of the accused terrorists to Pakistan via Dubai to be trained in handling arms and

arranged money for other logistics. Moreover, he headed all the meetings related to the attack. Phanasmiyan with his men received two landings of arms, detonators, hand grenades, and explosives. He arranged training programs for some of the accused persons and participated in the transportation and storage of the used arms and explosives. Yakub Memon was a part of the main conspirator list; he assisted Tiger Memon in landing, transporting, and storing the used arms and explosives. Yakub actively participated in all meetings held in Bombay and arranged funds through Hawala. Dawood Ibrahim was the leader of this conspiracy because he directed the two main conspirators to plan the attack. Furthermore, he arranged the training camps in Pakistan, sent arms and explosives to the main conspirators, and monitored the planning and execution of the attack.

As shown in Table 6, Tiger Memon, Phanasmiyan, and Yakub Memon are the three main conspirators according to the proposed centrality measure. According to the betweenness centrality and flow-betweenness centrality, Tiger Memon, Phanasmiyan, and Sultan Sayyed are the three main conspirators. The degree centrality identified Tiger Memon, Phanasmiyan, and Shahnawaz Qureshi as the three main conspirators. The discussion in the last paragraph justifies the accuracy of the proposed centrality measure.

The abovementioned analysis indicates that the proposed centrality measure provided the correct list of main conspirators in the four cases. The betweenness centrality measure did not result in accurate results in any of the four cases, and it only indicated the right conspirator names in the Rajiv Gandhi assassination case. However, even in this case, Santhan had a bigger score than Subha, which is incorrect because Subha contributed more to the attack plan than Santhan. The flow-betweenness centrality measure led to correct results only for the Indian parliament attack case, and for the Rajiv Gandhi assassination case, it resulted in the same list of the betweenness centrality measure. The degree centrality measure was only accurate for two cases: the Indian parliament attack case and the 26/11 Mumbai attack case, and for the Rajiv Gandhi assassination case, it afforded the same list of the betweenness centrality measure. Note that for the 26/11 Mumbai attack case, the betweenness and flow-betweenness centrality measures demonstrated that Kasab was the top conspirator. This was expected for these two centrality measures because the dataset of the 26/11 Mumbai attack is primarily based on the confessional statement of Kasab. However, the proposed centrality measure demonstrated that Kasab was not part of the main conspirator list and could correctly identify the top three conspirators. Moreover, it provided the correct order as per the involvement level of the main conspirators for the four cases.

TABLE 7 Leaders of the attacks

Dataset	Leader(s) of the attack
Indian parliament attack	Ghazibaba
26/11 Mumbai attack	Major General Saab
Rajiv Gandhi assassination	Prabhakaran, Pottu Amman
1993 Bombay bomb blast	Dawood Ibrahim

We could confirm the results of the proposed centrality measure from the proceedings of these cases. The names of the primary conspirators and leaders are present in these proceedings.

Furthermore, we applied the proposed Algorithm 2 to the results of Algorithm 1 to identify the leaders of the attacks based on all the used datasets in this study. Table 7 shows the leaders who directed the conspirators to plan and execute the four attacks. Note that none of the centrality measures had the highest centrality scores for the leaders of the attacks. Moreover, the results shown in Tables 3–6 show that these actors were not very much involved in the attacks because they were not even in the category of the top five actors. The reason for such results is that the leaders were not directly involved in the attacks and only directed the conspirators to plan and conduct the attacks. To solve this limitation, we designed Algorithm 2, which could successfully identify the leaders of the attacks corresponding to the four used datasets. We could confirm the outcomes of the proposed Algorithm 2 from the proceedings of these cases wherein the names of the leaders were present.

6 | CONCLUSION

In this study, we designed a centrality-based measure to identify the key conspirators of terrorist attacks and outlined an algorithm to identify the leaders who direct conspirators to plan and execute terrorist attacks. First, we considered four real-world terrorist attack cases from India and gathered information related to these cases to prepare four real-world datasets. Then, we applied the proposed method and other available methods to these datasets. The proposed method works in two steps. In the first step, the proposed centrality measure is used to compute the proximity of each node present in a terrorist network. We considered the top-k persons as the primary conspirators who have the top-k centrality scores. In the second step, the proposed algorithm is used to identify the leaders of terrorist attacks. We compared the proposed centrality-based measure with other baseline methods, and the obtained results demonstrated the effectiveness of the proposed centrality measure because

it could correctly identify all the conspirators of the attacks based on each of the datasets. Furthermore, only the proposed method could correctly identify the terrorist attack leaders based on the used datasets. To our knowledge, none of the existing approaches can correctly identify the leaders of terrorist attacks.

To summarize, we believe that this work may provide some information support to security agencies worldwide such that they can understand the working strategies of terrorist organizations in a more meaningful way. Security agencies can take preventive measures by arresting the leaders and main conspirators of terrorist attacks after identifying them. They can take some other actions such as freezing the bank accounts of the main actors, issuing alerts against them, and banning the organizations to which they belong. Such actions can help in minimizing and preventing future attacks. The proposed method in this study can be helpful during the case trials related to terrorist attacks. Moreover, using the proposed centrality measure, terrorists can be ranked based on their involvement level in terrorist attacks and can be penalized based on their centrality scores.

CONFLICTS OF INTEREST

The authors declare that there are no conflicts of interest.

ORCID

Abhay Kumar Rai https://orcid.org/0000-0002-3009-9764

REFERENCES

1. A. Berzinji, L. Kaati, and A. Rezine, *Detecting key players in terrorist networks*, (Proceedings of the 2012 European Intelligence and Security Informatics Conference, Odense, Denmark), Aug. 2012. https://doi.org/10.1109/EISIC.2012.13
2. D. Bright, C. Whelan, and S. Harris-Hogan, *On the durability of terrorist networks: Revealing the hidden connections between jihadist cells*, Stud. Confl. Terrorism **43** (2020), no. 7, 638–656.
3. H. A. Eiselt, *Destabilization of terrorist networks*, Chaos Solitons Fractals **108** (2018), 111–118.
4. I. Gialampoukidis, G. Kalpakis, T. Tsikrika, S. Papadopoulos, S. Vrochidis, and I. Kompatsiaris, *Detection of terrorism-related twitter communities using centrality scores*, (Proceedings of the 2nd international workshop on multimedia forensics and security, Bucharest, Romania) 2017, pp. 21–25.
5. I. Gialampoukidis, G. Kalpakis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, *Key player identification in terrorism-related social media networks using centrality measures*, (European Intelligence and Security Informatics Conference, Uppsala, Sweden), Aug. 2016. https://doi.org/10.1109/EISIC.2016.029
6. H. Isah, D. Neagu, and P. Trundle, *Bipartite network model for inferring hidden ties in crime data*, (IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Paris, France), Aug. 2015. https://doi.org/10.1145/2808797.2808842
7. P. Mitzias, E. Kontopoulos, J. Staite, T. Day, G. Kalpakis, T. Tsikrika, H. Gibson, S. Vrochidis, B. Akhgar, and I. Kompatsiaris, *Deploying semantic web technologies for information fusion of terrorism-related content and threat detection on the web*, (IEEE/WIC/ACM International Conference on Web Intelligence-companion, Thessaloniki, Greece,) Oct. 2019, pp. 193–199.
8. R. Pelzer, *Policing of terrorism using data from social media*, Eur. J. Secur. Res. **3** (2018), no. 2, 163–179.
9. S. Singh, S. K. Verma, and A. Tiwari, *A novel method for destabilization of terrorist network*, Modern Phys. Lett. B **34** (2020), no. 27. https://doi.org/10.1142/S021798492050298X
10. M. K. Sparrow, *The application of network analysis to criminal intelligence: An assessment of the prospects*, Soc. Netw. **13** (1991), no. 3, 251–274.
11. S. Tutun, M. T. Khasawneh, and J. Zhuang, *New framework that uses patterns and relations to understand terrorist behaviors*, Expert Syst. Appl. **78** (2017), 358–375.
12. M. Almoqbel and S. Xu, *Computational mining of social media to curb terrorism*, ACM Comput. Surv. **52** (2019), no. 5, 1–25.
13. V. Behzadan, A. Nourmohammadi, M. Gunes, and M. Yuksel, *On fighting fire with fire: Strategic destabilization of terrorist networks*, (Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Sydney, Australia), July 2017, pp. 1120–1127.
14. M. Burcher and C. Whelan, *Social network analysis as a tool for criminal intelligence: Understanding its potential from the perspectives of intelligence analysts*, Trends Organized Crime. **21** (2018), no. 3, 278–294.
15. M. Gregori and U. Merlone, *Comparing operational terrorist networks*, Trends Organized Crime **23** (2020), no. 3, 263–288.
16. M. Lalou, M. A. Tahraoui, and H. Kheddouci, *The critical node detection problem in networks: A survey*, Comput. Sci. Rev. **28** (2018), 92–117.
17. F. Ozgul, *Analysis of topologies and key players in terrorist networks*, Socio-Econ. Plann. Sci. **56** (2016), 40–54.
18. F. Saidi, Z. Trabelsi, K. Salah, and H. B. Ghezala, *Approaches to analyze cyber terrorist communities: Survey and challenges*, Comput. Secur. **66** (2017), 66–80.
19. Z. Su, K. Ren, R. Zhang, and S. Y. Tan, *Disrupting terrorist networks based on link prediction: A case study of the 9–11 hijackers network*, IEEE Access **7** (2019), 61689–61696.
20. J. Xu and H. Chen, *The topology of dark networks*, Commun. ACM **51** (2008), no. 10, 58–65.
21. S. F. Everton and D. Cunningham, *Detecting significant changes in dark networks*, Behav. Sci. Terrorism Political Aggress. **5** (2013), no. 2, 94–114.
22. S. Wasserman and K. Faust, *Social network analysis: Methods and applications*, Cambridge University Press, 1994.
23. T. Opsahl and P. Panzarasa, *Clustering in weighted networks*, Soc. Netw. **31** (2009), no. 2, 155–163.
24. V. Latora and M. Marchiori, *Efficient behavior of small-world networks*, Phys. Rev. Lett. **87** (2001), no. 19, 198701.
25. L. C. Freeman, *Centrality in social networks conceptual clarification*, Soc. Netw. **1** (1978), no. 3, 215–239.
26. Y. Cui, X. Wang, and J. Li, *Detecting overlapping communities in networks using the maximal sub-graph and the clustering coefficient*, Phys. A: Stat. Mech. Appl. **405** (2014), 85–91.

27. D. Li, X. Wang, and P. Huang, *A fractal growth model: Exploring the connection pattern of hubs in complex networks*, Phys. A: Stat. Mech. Appl. **471** (2017), 200–211.
28. G. Li, J. Hu, Y. Song, Y. Yang, and H. J. Li, *Analysis of the terrorist organization alliance network based on complex network theory*, IEEE Access **7** (2019), 103,854–103,862.
29. H. J. Li, Z. Bu, Z. Wang, and J. Cao, *Dynamical clustering in electronic commerce systems via optimization and leadership expansion*, IEEE Trans. Ind. Informat. **16** (2019), no. 8, 5327–5334.
30. H. J. Li, Q. Wang, S. Liu, and J. Hu, *Exploring the trust management mechanism in self-organizing complex network based on game theory*, Phys. A: Stat. Mech. Appl. **542** (2020), 123514.
31. H. J. Li, Z. Wang, J. Pei, J. Cao, and Y. Shi, *Optimal estimation of low-rank factors via feature level data fusion of multiplex signal systems*, IEEE Trans. Knowl. Data Eng. **34** (2020), no. 6, 2860–2871.
32. J. Li, X. Wang, and J. Eustace, *Detecting overlapping communities by seed community in weighted complex networks*, Phys. A: Stat. Mech. Appl. **392** (2013), no. 23, 6125–6134.
33. F. Nian, C. Hu, S. Yao, L. Wang, and X. Wang, *An immunization based on node activity*, Chaos Solitons Fractals **107** (2018), 228–233.
34. F. Nian and X. Wang, *Efficient immunization strategies on complex networks*, J. Theor. Biol. **264** (2010), no. 1, 77–83.
35. H. H. Qiao, Z. H. Deng, H. J. Li, J. Hu, Q. Song, and L. Gao, *Research on historical phase division of terrorism: An analysis method by time series complex network*, Neurocomputing **420** (2021), 246–265.
36. X. Wang and J. Li, *Detecting communities by the core-vertex and intimate degree in complex networks*, Phys. A: Stat. Mech. Appl. **392** (2013), no. 10, 2555–2563.
37. X. Wang and T. Zhao, *Model for multi-messages spreading over complex networks considering the relationship between messages*, Commun. Nonlinear Sci. Numer. Simul. **48** (2017), 63–69.
38. X. Wang, T. Zhao, and X. Qin, *Model of epidemic control based on quarantine and message delivery*, Phys. A: Stat. Mech. Appl. **458** (2016), 168–178.
39. A. H. Johnston, and G. M. Weiss, *Identifying sunni extremist propaganda with deep learning*, (IEEE Symposium Series on Computational Intelligence, Honolulu, HI, USA), 2017. https://doi.org/10.1109/SSCI.2017.8280944
40. M. Moussaoui, M. Zaghdoud, and J. Akaichi, *A possibilistic framework for the detection of terrorism-related twitter communities in social media*, Concurr. Comput: Pract. Experience **31** (2019), no. 13, e5077.
41. J. Rasheed, U. Akram, and A. K. Malik, *Terrorist network analysis and identification of main actors using machine learning techniques*, (Proceedings of the 6th international conference on information technology: Iot and smart city, Hong Kong, China), 2018, pp. 7–12.
42. M. I. Uddin, N. Zada, F. Aziz, Y. Saeed, A. Zeb, S. A. Ali-Shah, M. A. Al-Khasawneh, and M. Mahmoud, *Prediction of future terrorist activities using deep neural networks*, Complexity **2020** (2020), 1373087. https://doi.org/10.1155/2020/1373087
43. P. C. Wang, and C. T. Li, *Spotting terrorists by learning behavior-aware heterogeneous network embedding*, (Proceedings of the 28th ACM International Conference on Information and Knowledge Management, New York, NY, USA), Nov. 2019, pp. 2097–2100.
44. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*, MIT Press, 2009.
45. D. B. Johnson, *A note on Dijkstra's shortest path algorithm*, J. ACM **20** (1973), no. 3, 385–388.
46. G. Sabidussi, *The centrality index of a graph*, Psychometrika **31** (1966), no. 4, 581–603.
47. A. Tundis, L. Böck, V. Stanilescu, and M. Mühlhäuser, *Limits in the data for detecting criminals on social media*, (Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK), Aug. 2019, pp. 1–8.
48. T. Hindu, Rajiv's death—A revisit, 2016. Available from: https://www.thehindu.com/in-school/rajivs-death-a-revisit/article5814423.ece [last accessed May 2021].
49. The Supreme Court of India, Death Reference Case No.1 of 1998, 1999. Available from: https://web.archive.org/web/20111102222525/http://cbi.nic.in/dop/judgements/thomas.pdf [last accessed May 2021].
50. T. Hindu, A perfect day for democracy, 2016. Available from: https://www.thehindu.com/opinion/lead/a-perfect-day-for-democracy/article4397705.ece [last accessed May 2021].
51. The Supreme Court of India, Appeal (criminal) 373-375 of 2004, 2005. Available from: https://main.sci.gov.in/jonew/judis/27092.pdf [last accessed May 2021].
52. A. Tak, Afzal Guru interview with Shams Tahir Khan, 2019. Available from: https://www.youtube.com/watch?v=Mat54XtiQgA [last accessed May 2021].
53. T. Hindu, Pak Army officers trained 26/11 terrorists, 2010. Available from: https://www.thehindu.com/news/national/lsquoPak-Army-officers-trained-2611-terroristsrsquo/article16550267.ece [last accessed May 2021].
54. The Supreme Court of India, Appeal (criminal) 1899-1900 of 2011, 2012. Available from: https://main.sci.gov.in/jonew/judis/39511.pdf [last accessed May 2021].
55. I. Today, Tutor of the 26/11 terrorists, 2020. Available from: https://www.indiatoday.in/india/north/story/26-11-mumbai-attacks-pakistan-isi-let-zabiuddin-ansari-107634-2012-07-01 [last accessed May 2021].
56. The Supreme Court of India, Criminal Appeal No. 1728 of 2007, 2013. Available from: https://main.sci.gov.in/jonew/judis/40190.pdf [last accessed December 2021].
57. Wikipedia, 1993 Bombay bombings, 2021. Available from: https://en.wikipedia.org/wiki/1993_Bombay_bombings [last accessed December 2021].
58. L. C. Freeman, S. P. Borgatti, and D. R. White, *Centrality in valued graphs: A measure of betweenness based on network flow*, Soc. Netw. **13** (1991), no. 2, 141–154.

AUTHOR BIOGRAPHIES

Abhay Kumar Rai received his MSc degree in Computer Science from the University of Allahabad, India, in 2008, and his MTech in Software Engineering from the MNNIT Allahabad, India. He received his PhD degree in Computer Science from the University of Allahabad, India, in 2015. From 2015 to

2018, he worked for the Centre of Computer Education, University of Allahabad, India. Since 2018, he has been with the Department of Computer Science, Banasthali Vidyapith, Rajasthan, India, where he is now an Assistant Professor. His research interests include heterogeneous network security, algorithm design, criminal intelligence analysis, and social network analysis.

Sumit Kumar received his BCA and MCA degrees in computer applications from the Centre of Computer Education, University of Allahabad, Allahabad, Uttar Pradesh, India, in 2015 and 2018, respectively. Since 2018, he has been working for Tata Consultancy Services, New Delhi, India, as a System Engineer. His work is to develop and design various modules to analyze network devices and their behaviors. His main research interests are criminal intelligence analysis and network behaviors.

How to cite this article: A. K. Rai and S. Kumar, *Identifying the leaders and main conspirators of the attacks in terrorist networks*, ETRI Journal **44** (2022), 977–990. https://doi.org/10.4218/etrij.2021-0239