Research Articles

A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis

by Sarita Azad and Arvind Gupta

Abstract

This paper analyses, the terror attacks in Mumbai on November 26, 2008, popularly known as 26/11 terror attacks, as per a mathematical technique known as Social Network Analysis (SNA). This analysis of the behaviour of the ten attackers and their telephonic communications with their handlers in Pakistan even as the attacks were in progress is based on the open source information. Using the SNA technique, we identify the key members, sub-groups, and the interaction among the various members of the group. The analysis gives useful insights into the modus operandi of the terrorists. We have found that a star-type structure of hierarchy prevailed during the attack which means terrorists were well connected through a central node.

Key words: social network analysis, terrorism, mathematical models, 26/11 Mumbai attack.

1. Introduction

Over the past few decades, terrorism has become a major threat to international security [1]. In recent years, there have been frequent terrorist attacks around the world. One of the most high profile terror attacks executed by the cadres of the terror group Lashkar-e-Taiba (LeT) on November 26, 2008 in Mumbai, (India), was meticulously planned. It began on November 26th and ended on November 29th after an intense operation lasting over sixty hours. The attack was carried out by 10 militants armed with advanced weapons at five prime locations in Mumbai, India's financial capital. Nearly 260 persons, from ten countries, were killed in the attack. The modus operandi of this attack is explicitly described in various reports [2-4], and in the report shared by the Indian government [5] with the government of Pakistan. According to the analysis by Raman (2009) [6], the Mumbai terror attack had an anti-India, anti-Israel, anti-Jewish, anti-US and anti-NATO agenda.

A terrorist organisation can be represented as a network using a technique known as Social Network Analysis (SNA) which studies social relationships amongst nodes and ties. In case of a terrorist network, the members are considered as the nodes, and the ties describe the interactive

or collaborative relationships between the pairs of node. There was an increasing interest in the application of SNA for the study of terrorism shortly after the 9/11 attacks on the World Trade Center twin towers in New York [7, 8]. In the past few years the techniques of SNA have brought about a paradigm shift in counter terrorism planning and strategies [9,10]. The descriptive and visualisation potential of SNA helps to explain group activities, target selection and motives. Also, new analytical techniques and innovative means to conjoin available data in the network make it a powerful tool for research and ultimately to give inputs for policy makers.

Network analysis is an efficient tool for unravelling the complexities of systems that comprise many interacting elements. SNA helps to answer the following questions [11]:

- Who is central node in the network?

- What sub-groups exist in the network?

- What are the patterns of interaction between sub-groups?

- What is the overall structure of the network?

- How does information flow in the network?

The objective of this paper is to present a mathematical assessment of the 26/11 Mumbai terror attack using SNA technique. The paper relies on the information provided by the government of India in their report [5]. The paper is organised as follows: Section 2 gives the background of Mumbai terror attack. Section 3 describes the various social networks that are generally used for terrorism analysis. Also, a description of the parameters of social network analysis is provided. Section 4 discusses the terrorist networking during the Mumbai attack at different levels of occurrence and the information available at the time of incident. The structural organisation of the Mumbai terror attack and the details of planners and trainers behind the attack are given. We use graphical software UCINET to obtain a network for the attack. Section 5 is a summary of the conclusions

2. The Mumbai Terror Attack: A Brief History

The Mumbai terror attack was executed by the Lashkar-e-Taiba (LeT), a terrorist group based in Pakistan. The LeT was founded in 1987 with the express aim of helping the Mujahideen in Afghanistan and liberating Kashmir from India. The attack was planned well in advance and a Pakistani American David Headley was employed to gather critical information about Mumbai - which was later confirmed by Headley's confession in the Chicago case. It has now been revealed that Headley had played a central role in preparing the operation. He visited India many times to scout out targets. Based on the connections we have found in the report [16], the

Headley confession is an authentic source of information as to how the plan was conceptualised by both serving and retired officials of Pakistan's Inter Service Intelligence (ISI) along with the leaders and commandoes of the LeT, Hafiz Saeed (LeT chief), Lakhvi, Sajid Majeedid and Waasi.

10 militants carried out the Mumbai terror attack. Each member of the team was given rigorous training. They entered Mumbai clandestinely using a stolen boat, travelling all the way from Karachi by sea. They were equipped with sophisticated weapons and navigation equipment like Global Positioning Systems (GPS) and satellite phones. After reaching the territorial waters of Mumbai, they divided themselves into five groups and captured the high profile five stars Taj Mahal Hotel, on the Gateway of India, the Oberoi Trident Hotel, Café Leopold, Chhatrapati Shivaji Terminus and the Nariman (Chabad) house Jewish community centre. The various locations of the attack are shown in the Figure 2.

Figure 2: Locations of 26/11 Mumbai terror attacks (source, Wikipedia)

Ismail Khan was the leader of the group. During the period of the attack the terrorists were in constant touch with their handlers in Pakistan. The Indian intelligence agencies were able to intercept their conversations on mobile and satellite phones as the attacks were in progress. While the contents of the intercepts are not known, the government of India has revealed the details of who was talking to whom. The attackers killed nearly 260 persons including several foreigners. While the Indian security forces killed 9 out of the 10 attackers, one by the name of

Ajmal Amir Kasab was taken alive and is now awaiting death sentence in a Mumbai jail. His testimony and that of Pakistani American David Headley in the US have been extremely valuable in reconstructing the entire sequence of events and have revealed now just how well planned the attack was. It turns out that the mastermind of the attack, LeT commander Lakhvi, was in Pakistan. During the entire operation lasting over 60 hours, the attackers were in touch with their handlers in Pakistan. Lakhvi and others are being tried in Pakistani courts.

3. Background of the different kinds of networks

Terrorist network analysis is a difficult undertaking because of the clandestine nature of terrorist groups [12]. These are covert networks where secrecy is the prime concern during the operation. Such networks are structured in such a way as to ensure efficient communication between members without being detected. Explicit theoretical studies have been undertaken on the predictive structure of the covert networks [13-15]. These networks are reported to have different formations such as ring, star and path in which the degree of covertness and communication efficiency depend on the connections between the nodes (Fig. 1). The star graph (Fig. 1b) is known as centralised network where all the nodes are connected only through one central node. On the other hand, the path graph (Fig.1a) is a network with one to one connections. The network shown in Fig 1 (c) is a complete network where all-to-all communication exists. It has maximum density and hence 100 per cent connectivity. The theoretical studies reveal that the path type is optimum in the lower order while star type network is best for balancing efficiency and covertness.
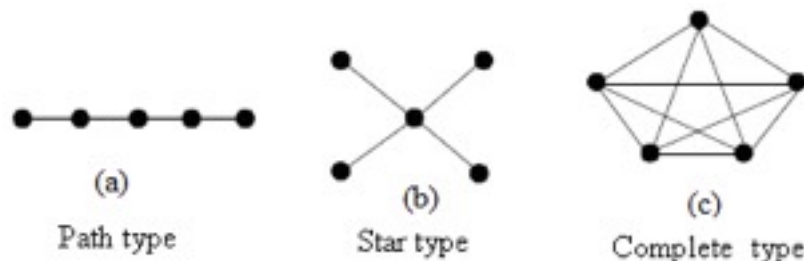

Figure 1. Types of networks.

The network for the 9/11 attack was structured using social network analysis [8]. The network was drawn based on information gathered about the 19 hijackers and yields a number of interesting properties. Using measures of centrality, Krebs elucidated the dynamics of the network. The 9/11 network has a path-like structure (Fig. 1a), which is an open and most decentralised network. Interestingly, this is an Al-Qaeda modus operandi, which was confirmed from a Bin Laden video.

3.1 Quantitative Parameters of Social Network Analysis

3.1.1 An adjacency matrix

The adjacency matrix $\{a_{ij}\}$ in social network analysis is a square matrix with as many rows and columns as there are nodes in the data set. The "elements" or scores in the cells of the matrix record information about the ties between each pair of nodes. If a "tie" is present, i.e. if one node can talk to the other, '1' is entered in a cell; if there is no tie, a zero is entered. The matrix contains the information about the existence or non-existence of a link. Therefore, the adjacency matrix can be defined as a set of numbers,

$$
A_{ij} =
\begin{array}{c|c|c|c|c}
 & a1 & a2 & a3 & a4 \\
\hline
a1 & & 1 & 0 & 1 \\
\hline
a2 & 1 & & 1 & 0 \\
\hline
a3 & 1 & 1 & & 1 \\
\hline
a4 & 0 & 0 & 1 & \\
\end{array}
$$

where we assume that there are four nodes in the network and the ties between them are binary numbers. Note that there are no diagonal entries in the matrix as the tie of a node from itself is not considerable.

3.1. 2 Centrality

Centrality deals with the role of individuals in a network. Several measures of centrality such as 'degree', 'betweenness', 'closeness', and 'eigenvector' can suggest the importance of a node in a network. The degree of a particular node is its number of links; its betweenness is the number of 'geodesics' (shortest paths between any two nodes) passing through it; and its 'closeness' is the sum of all the geodesics between the particular node and every other node in the network. An individual with a high 'degree', for instance, may imply that he is a leader; whereas an individual

with a high 'betweenness' may be a gatekeeper in the network. An eigenvector centrality is the measure of how much a participant interacts with the other "connected" or highly interactive members of the group. This can be useful in providing a snapshot of how group members interact, as the eigenvector scores of different members or subgroups may indicate the degree to which they have formed strong relationships with other influential or active members in the group.

4.1 Analysing the Mumbai Attack using Social Network Analysis

It is now known, from various reports available, that 10 ten terrorists were present at the time of incident, whereas three others were simultaneously handling the operation from Pakistan. The names and the locations of these attackers and the handlers are listed in Table 1 and 2.

Table 1: LeT handlers who operated from Pakistan (P).

S. No.	Handler's Names	Place of Operation
1	Abu Kaahfa	Pakistan
2	Wassi	Pakistan
3	Zarar	Pakistan

Table 2: Attackers who operated in Mumbai.

S. No.	Attacker's Names	Place of Operation	Abbreviations
1	Hafiz Arshad	Leopold Café and Bar	LC
2	Javed	Taj Mahal Hotel	TMH
3	Abu Shoaib	Taj Mahal Hotel	TMH
4	Abu Umer	Leopold Café and Bar	LC
5	Abdul Rehman	The Oberoi-Trident Hotel	OTH
6	Fahadullah	The Oberoi-Trident Hotel	OTH
7	Baba Imran	Nariman House	NH
8	Nasir	Nariman House	NH

9	Ismail Khan	Chhatrapati Shivaji Terminus	CST
10	Ajmal Amir Kasab	Chhatrapati Shivaji Terminus	CST

As mentioned earlier, techniques like SNA can help in the visualisation of a network by using a two-dimension graph, which helps to understand the overall structure of the network. The software we use for the construction of 26/11 network is UCINET which represents, analyses, visualises, and simulates nodes (attackers) and ties (relationships) from the input data. The network thus obtained can help to better understand the whole incident and can shed light on the pattern of interaction.

To start with, we first form the adjacency matrix as defined in section 3.1. From the government of India's report [5], we found that the attackers reportedly used satellite phones and were in frequent contact with their handlers in Pakistan. They received calls from the handlers during the siege to discuss their plans and routes. The phone conversations between these attackers and remote handlers in Pakistan were intercepted by Indian government and are given in the report [5]. The adjacency matrix in Table 3 represents the binary relationships between the attackers and the handlers determined through the contextual background. If we find a conversation was established between the two people, value one is assigned in the matrix, for no conversation the value remains zero (Table 3).

Table 3: Connections established between attackers and handlers at the time of incident.

	Abu Kaahfa	Wassi	Zarar	Hafiz Arshad	Javed	Abu Shoaib	Abu Umer	Abdul Rehman	Fahadullah	Baba Imran	Nasir	Ismail Khan	Ajmal Amir Kasab
Abu Kaahfa		1	1	0	0	0	0	0	0	0	0	0	0
Wassi	1		1	1	0	0	1	0	0		1	1	
Zarar	1	1		0	0	0	0	0	0	0	0	0	0
Hafiz Arshad	0	1	0		1	1	1	0	0	0	0	0	0
Javed	0	0	0	1		0	1	0	0	0	0	0	0
Abu Shoaib				1	1		1	0	0	0	0	0	0
Abu Umer	0	1	0	1	1	1		0	0	0	0	0	0
Abdul Rehman	1								1				
Fahadullah	0	0	1	0	0	0	0	1		0	0	0	0
Baba Imran	0	1	0	0	0	0	0	0	0		0	0	0
Nasir	0	1	0	0	0	0	0	0	0	0		0	0
Ismail Khan	0	0	0	0	0	0	0	0	0	0	0		1
Ajmal Amir Kasab	0	0	0	0	0	0	0	0	0	0	0	1	

Source: Adapted from information provided by Government of India in Dossier, 2008[5].

From the collected information it is found that during the attack, 13 terrorists played the major role (as listed in Table 1, 2). Their network is drawn on the basis of their telephonic conversations using software UCINET and depicted in Fig.3. Such graphs are commonly used to visualise which nodes (terrorists) are highly connected. Terrorists are located at equal distances, and nodes that are highly connected are very easy to locate because of the density of lines. The

overall structure looks like a centralised star-type network (Fig. 1b) where Wassi, a handler from Pakistan is the most centrally placed terrorist. The attackers Ismail Khan and Ajmal Kasab are isolated in the network. The density of the network, which is an indicator of connectedness of the network, is found to be 0.22. The limiting value of density is one when all the nodes are connected with each other and zero when all nodes are not connected. In the present study, the value for density is 0.2 attributed to the open structure of this terrorist network. Further, this network (Fig. 3) is divided into three sub-groups, which are coloured to identify which terrorist is a member of which group.
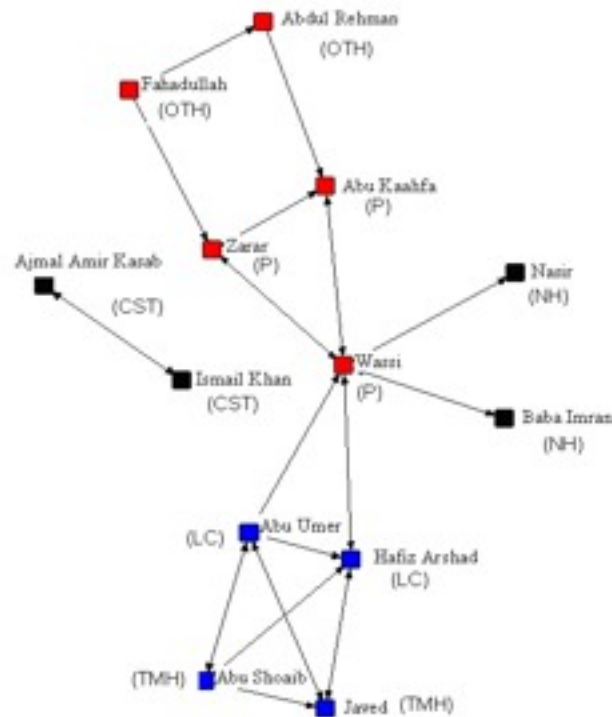

Fig.3: Terrorist network for 26/11 attack based on intercepted phone calls.

Our network analysis reveals that the following sub-groups operated at the time of incident:

1. The terrorists divided themselves into five subgroups in charge of five locations.

2. Fahadullah and Abdul Rehman took charge of the Oberoi-Trident Hotel; Ismail Khan and Ajmal Amir Kasab went to the Chhatrapati Shivaji rail terminus; Nazir & Baba Imran attacked the Israeli chabad at Nariman House; Abu Umer and Hafiz

Arshad took possession of Leopold Café and Abu Shoaib & Javed went to the Taj Mahal hotel. It appears that Abu Umer and Hafiz Arshad joined the two terrorists at the Taj hotel after they finished with Café Leopold.

3. Each sub-group, with the exception of the one at the CST, was in touch with a handler in Pakistan. Wassi in Pakistan turns out to be the key handler. He directed the attack at Oberoi-Trident Hotel through Zarar and Abu Kaahfa. Wassi personally directed the attacks at Nariman House, Café Leopold and the Taj Mahal Hotel.

4. Although Ismail Khan was reportedly the leader of the entire group, he got killed at CST and his partner was taken into custody.

To further study the interaction between individuals, degree, closeness, betweenness and eigenvector are evaluated and given in Table 4. These indices are a measure of the centrality of the network and indicate hierarchal prestige, importance and power of individuals. It reveals patterns of interactions and associations and can be helpful for revealing the overall structure of terrorist networks under study. It is found that Wassi with highest value of eigenvector, betweenness , closeness, and degree can be identified to be the most important person in Pakistan who was handling the entire operation. Other important persons were Abu Umer, Hafiz Arshad, Abu Shoaib and Javed.

Table 4: Various networks' parameters for all the terrorists understudy

S.No.	Terrorist Names	Abbreviations	Degree	Closeness	Betweenness	Eigenvector
1	Abu Kaahfa	P	25.000	26.667	11.364	29.191
2	Wassi	P	50.000	30.000	50.000	62.844
3	Zarar	P	25.000	26.667	11.364	29.191
4	Hafiz Arshad	LC	33.333	27.273	10.606	64.497
5	Javed	TMH	25.000	23.529	0.000	50.672
6	Abu Shoaib	TMH	25.000	23.529	0.000	50.672
7	Abu Umer	LC	33.333	27.273	10.606	64.497
8	Abdul Rehman	OTH	16.667	23.077	0.758	11.467
9	Fahadullah	OTH	16.667	23.077	0.758	11.467
10	Baba Imran	NH	8.333	24.490	0.000	17.724
11	Nasir	NH	8.333	24.490	0.000	17.724
12	Ismail Khan	CST	8.333	8.333	0.000	-0.000
13	Ajmal Amir Kasab	CST	8.333	8.333	0.000	-0.000

5. Summary and Conclusions

SNA can be a powerful tool for understanding the complex nature of terrorist organisations. Even the limited information available from open sources has helped create a fairly clear picture of the details of the terrorist group and its sub-groups. The security agencies, which routinely intercept phone conversations, emails etc. can use SNA techniques to identify the nodes in a complex network and evaluate their importance in the hierarchy. The identification of type of terror networks would provide useful inputs to strengthen counter-terrorism efforts.

However, it must be mentioned that SNA alone would not suffice for unravelling the modus operandi of terrorist networks. Inputs from the traditional methods of analysing terror networks will be required. SNA can help in providing additional insights that may not be available from other methods.

Authors Biography

Dr. Arvind Gupta holds the Lal Bahadur Shastri Chair at the Institute for Defence Studies and Analyses, New Delhi, India, where he leads the Internal Security Cluster. A member of the Indian Foreign Service (IFS), he has wide ranging diplomatic experience. He has also served in India's National Security Council Secretariat (NSCS) and dealt with national and international security issues. He received a Ph.D in International Relations from the Jawaharlal Nehru University, New Delhi in 1993.

Email: lbscidsa@gmail.com

Dr Sarita Azad is a researcher at Institute for Defence Studies and Analyses, New Delhi, India, where she is employing mathematical and statistical techniques in various applications related to International Relations. She received her Masters (Mathematics) from the Indian Institute of Technology (IITD), Delhi, India, in 1999. She did her Ph.D (2008) in Applied Mathematics from Delhi University, India, under Professor Roddam Narasimha (FRS) from the Indian Institute of Science, Bangalore, India. She was visiting fellow at University of Cambridge, UK (2009).

Email: saritaazad@gmail.com

Notes:

[1] Fenstermacher L., Kuznar T. Rieger, and Speckhard A. (2010). "Protecting the Homeland from International and Domestic Terrorism Threats:.", *White Paper: Counter Terrorism,* 178.

[2] Acharya, A, Mandal, S and A. Mehta (2009). *Terrorist attacks in Mumbai: picking up the pieces.* International Centre for Political Violence and Terrorism Research S.Rajaratnam School for International Studies Nanyang Technological University, Singapore.

[3] Gunaratna, R. (2009). "Mumbai investigation: the operatives, masterminds and enduring threat." , *UNISCI Discussion Paper,* Nº 19: 142.

[4] Onook O, Agrawal M and R. Rao. (2010). "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter.", *Information System Frontiers* 13 (1): 33-43.

[5] A report on Mumbai attack (2009). "*Mumbai terrorist attack (Nov. 26-29, 2008),*" Govt. Of India.

[6] Raman B (2009). "*Mumbai 26/11 a day on infamy.*" Lancer Publishers, New Delhi.

[7] Carley, M.K, Ju-Sung, L. and D. Krackhardt (2002). "Destabilizing network." *Connections* 24(3): 79-92.

[8] Krebs, V.E. (2002). "Mapping networks of terrorist cells." *Connections* 24(3): 43-52.

[9] Sageman M. (2004). *"Understanding Terror Networks."* University of Pennsylvania Press.

[10] Wiil U.K., Memon N and P. Karampelas (2010). "Detecting new trends in terrorist networks." *International Conference on Advances in Social Networks Analysis and Mining* 435

[11] Xu J.J. and H. Chen. (2005). "CrimeNet explorer: a framework for criminal network knowledge discovery."*ACM Transactions on Information Systems* 23 (2): 201-226.

[12] Johnson, L.K. (2007). "*Strategic intelligence: covert action: Beyond the veils of secret foreign policy.*" Praeger Security International: Westport.

[13] Lindelauf R., Borm P.E.M. and H.J.M. Hamers (2008). "On heterogeneous covert networks." *Discussion Paper,* Tilburg University 46.

[14] Jackson. (2001). "*The Stability and efficiency of economic and social networks.*" Springer-Verlag: Heidelberg.

[15] Koschade. (2006). "A social network analysis of Jemaah Islamiyah: the applications to counterterrorism and intelligence." *Terrorism and Political Violence* 29: 559-575.

[16] Burke J. (2010). The Guardian report, http://www.guardian.co.uk/world/2010/oct/18/david-headley-mumbai-attacks-pakistan.