IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

Social Network Analysis as Counter Terrorism Tool

A. Srivastava[1*], A. Pillai[2], D. J. Gupta[3]

[1]Department of Computer Engineering, Pranveer Singh Institute of Technology, Kanpur, India
[2]Department of Computer Engineering, YMCA University of Science & Technology, Faridabad, India
[3]Dean Research & Development, Poornima University, Jaipur, India

Available online at: www.ijcseonline.org

Accepted: 20/Sept/2018, Published: 30/Sept/2018

Abstract— Social network analysis is no more only bound to studying the relationship between the actors to discover the hidden trends and find scope in them but there is a darker side as well. The deep ocean of network has allowed people to counter attack on different countries via acting from various locations by issuing fake identities. The cycle of events that take place with the evil intentions to disrupt and cause fear not only physically but mentally too is referred to terrorism. SNA allows this act to counter prevent and associate the links by identifying the intentions and working of the actors. Various studies have been conducted after 9/11 attack and people all over the world are monitored so as to track the status and if any conviction is predicted, the complete network is examined. The sole purpose of these studies is to prevent thwarting and prepare oneself to counter terrorism. This paper outlines certain methods that recognize the terrorist activities which need to be monitored so as to detect the pre-event occurrence and counter attack on their planning.

Keywords— Social Network Analysis, Counter Terrorism, Information Analysis, Intelligence analysis.

I. INTRODUCTION

Social network is a connection of various nodes associated with each other based on interactions and personal relationship. These nodes communicate with one another through comments, messages, images information sharing by posting over the sites. The sites have a major actor associated with it. This actor is the identification of oneself for the entire world over the network. Social network analysis has many applications in various fields including data mining [1], email communication [2], information retrieving [3], criminology [4] etc. The social networks are studied by representing them into graphs and these graphs are further evaluated for covering the hidden complexity in the network and describe the entire organization associated with the graph structure [5]. The structures of the social network offer insight internal patterns of communication and connectivity [6]. These networks are represented as nodes and edges where the former are the individuals and the latter is the link associated or established between different former. The social network initially began its research theoretically and gained the pace with applications with time. The network has now become wide and distributed; which with the advancement now has also developed cons that need to be closely monitored as they are terror related which is likely to harm every aspect of living. The terrorism is the act where the political interceptions of individual or group of people are likely involved in the violent activity which causes the mental, physical, social riots in the society and individual. Thus to review these actions involved in criminal offences such as trafficking of arms, smuggling of drugs, disposal of toxic waste, nuclear weapons implementations and exporting, human trafficking, sexual harassment and trafficking, trading of illegal weapons and endangered species etc., SNA is a key tool for keeping a check and recordings of the activities of people i.e. the social network enables people to connect with each other thus a slight link could give the idea of what is the intention of an actor if network communication is involved.

With the advent in time there has been myriad regarding terrorism and a lot of people have been traced using the network linkups. The most terrific experience which people faced in 9/11 lead to loss of many lives and property. This loss built fear amongst the people and scholars got a new trend in research field using information gathering and analysis. The social network was highly effective in learning the culprit behind the attack and with joining the complete network the whole group was tracked and traced with the plan been discussed long before the attack. Thus, counter terrorism became one of the key areas from the perspective of research using information analysis and solving the puzzled links and connections vulnerabilities are explored with specific measures to fight back are defined. The detection and disruption of the pre terror attacks are not at all easy task but involves a lot of assessment and understanding the organizations involved in it. The criminal acts are always covert and exploring them might be dangerous as people involved in it have a insane mindset and causing harm is their ultimate motive. Counter terrorism is carried with intelligence analysis covering a flow of data which is reconstructed establishing the movement and interest of communication held between individuals or group of similar liking people. The process is highly complex and iterative with usage of intelligence searching, inference and intuition. Various agencies are associated with finding and working for the counter terrorism.

There are certain limitations associated with tracking of the counter terrorism such as analyses of the boundary conditions, their specifications, guarding the hindrances and unwarranted counterparts. These limitations were managed and overlooked with methods that are used to counter terrorism and this paper outlines few of those methods and their working principles.
The paper is categorized with different sections where section 2 explains the social network and its applications with detailing the counter terrorism. Section 3 includes the methods which analyses counter terrorism and section 4 concludes the paper.

II. UNDERSTANDING SOCIAL NETWORK AND COUNTER TERRORISM

A network is represented as a set of connecting nodes with the established link between them. These structures could be a flock formed by common interest sharing, interaction for a purpose, chatting, blogosphere, folksonomy. Social network analysis has become significant in the area of research dealing with criminology as they are able to better measure the social network structure and their influence than the methods used traditionally for evaluation. SNA has the basic utility to understand the dynamics associated within the networks which are formed by the combination of influential contents linked by ties such as friendship, membership, kinship, relationship etc. Knoke et al.[7] suggests in their research that social network study where people are closely connected gives the idea as of their behavior which plays a vital role in studying the primary attributes including age, gender, socio-economic status.

A. SOCIAL NETWORK AND ITS ANALYSIS

Network have a structure formed by sharing common attributes that influences people to attach to nodes and forms groups performing similar type of function. There are different topology that represents how a network is attached and up to what level the nodes are densely populated. For example a structure shaped as a star has its central effect on one node while if the structure is found to be chained then each node might be forming various chained where nodes are connected to certain other nodes depicting a chain as shown in figure 1.

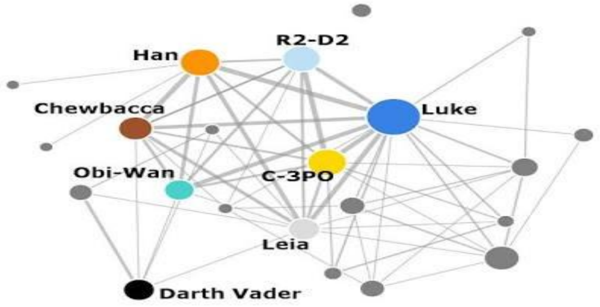

Figure 1 Network showing various nodes with different topology

When the network is found to be centralized outlining as a star the data and information are easily reachable travelling long distances and this is referred to as small world theory. The networks another point of consideration includes density which is given as the ratio of the ties visibly connected to the total number of possible available ties. The experimental results proposed by various authors exhibit that increased density bring about to increased resilience as even if one node is removed from the network there remains a network in itself which can be studied further [8,9,10]. The removal of one node from a network and still the remaining nodes are in tacked together into a complete network structure and this removal of nodes concept is said to be fragmentation.

SNA deals with centrality analysis where the actors connected to each other are evaluated based on how much strong the bond is and what factors are associated in making this bond exist. The centrality in terrorist network helps in knowing the importance and position of the actors situated at different locations. Degree Centrality is defined as the number of those nodes which are connected to each other directly where nodes having higher value of degree are depicted to be active users as more numbers of nodes are attached to it. Betweenness centrality is referred to the count of nodes crossing the shortest path of the number. The higher the value the node becomes the influential one who is responsible for the information interchange and those nodes are called brokers [11].

SNA has interdisciplinary inherent from various other fields including psychology, statistics, graph theory. It has become a major paradigm in sociology which combines complex network and becomes part of the network sciences. The data that is been built up through networks are evaluated on the traits and behavior which leads to the exact characteristics and attributes of individual. Before proceeding to understand the relevance of social network and terrorism there are various network ties that are often vulnerable to get attacked and influenced to join terrorism. Various authors through their surveys have concluded in their theories that weak bonds are prone to social influence and are somehow forced, manipulated and attracted towards these acts. Granovetter

[12] gave the theory based on the strength of weakly connected links that strongly put forth weak bonds uses less time and adapt themselves over the small portion of manipulated statements. These bonds connect themselves to get establishment with different groups and later make others join the group. This is the process as to how innocent people are deceived and made part of dark networks. Burt [13] in his paper worked on the concept of structural holes. The structural holes are the brokers who have the complete hold on the flow of information and these are further used in connecting with other groups available in the network. The small world theory is the major common network used in terrorist research which states that the connecting links are densely attached to each other and are reachable via six degrees of separation [14]. The ties with shorter length can easily access other nodes near to them and pass the information faster. The small world theory has been greatly expanded with different concepts by various authors and the researchers conducted through this cover a large portion of limitations associated with terrorism [9, 15, 16, 17]. Similar concepts were used by bichler et al. [11] to further conduct study and prove that nodes with higher degrees tend to connect other clusters in the network strongly and which can be used to associate large population with the dark network.

SNA has relevance with terrorism getting to initiate the trending of combining SNA with data mining, spatial analysis, designs of the network helpful in terrorist research.

B. SNA AND TERRORISM

Terrorism has different meaning to various people as for terrorist to one might be the freedom fighter for other. Thus terrorism is a kind of situation created by political disruption which leads to violence, anxiety, stress that harms the mental and physical peace. The pre concept of terrorism was through the military power where security over the borders was breached and soldiers or people fought for their rights and freedom. Terrorist networks are examined carefully with each attached links to closely monitor and expand the relations and kinships associated to it. The network is represented as hierarchal model which is represented as their working stages and ranks. The hierarchal network is not flexible and is bounded at every stage because many nodes don’t know about their members and they were only orders of people at higher powers and positions. The communication involves the information sharing and fund transferring. The funds are transferred depending upon the purpose including weapons purchasing, bombs creation, drugs buying, kidnapping and planning to destroy whatever is a cause for terrorist mental peace. The psychology of those people is made up in a manner to create havoc and destruction. A single individual is not made the in charge of taking the entire decisions rather groups of people are distributed their jobs and dispersion techniques are used to execute the plan around the coverage. This is referred to decentralized technique of the terrorist network. Magouirk et al. [18] worked on the JI network and illustrated the network structure hierarchy where different individuals were handed over the leadership and the process execution was followed. After 9/11 the network was made to be decentralized and internet became the medium for the communication and the loosely connected nodes were targeted. The weak links are easy to stay covert and information is culled from different medium and similar environment is adapted amongst them. This made the decentralized network to become compartmentalized and an increase in the dark network activities was laid on.

US government was able to clearly connect every link to reach the cells associated in 9/11 using the SNA applications. Initially the public data was manually checked and following every link and connection the entire network was mapped. The process used was linking the contact list to the available sources and working on finding the related data and transfer of information with the money details. This clue helped them to recreate the pseudo-event and manage to get through people who could be involved in the event. As to find the complete network on a single go was difficult. Like the people around the world uses internet for sharing details similarly the terrorist group work upon its functioning. Information gathering is the most important activity that is followed by the intelligence agencies and the terrorist groups because without relevant information nobody is able to execute its proceedings. Various databases are created that stores the needful data for examining and keeping the records updated for pre-evaluation of the event to take place. There have been anti-terrorist groups made who remain hidden in a way that their work does not get disrupted and mysterious groups could be easily focused. Since data has become dynamic with the increasing population the data is analyzed for finding the nature of the network, identifying its influential node, its surrounding and neighboring environment, impact on various activities of interests. The limitation in terrorist network is in identification of the doubtful surroundings and comparing it with the cases. Once an event occurs it becomes difficult to know what effects were already existed in the network and were clean in one’s perspective while in other’s perspective it was a danger to other network.

III. SNA BASED COUNTER TERRORISM FRAMEWORKS

A. ARGUMENT DRIVEN HYPOTHESES MODEL

Dynamic social network has become vast with the passing years thus studying every node and creating its hierarchy is too complex and challenging. To eliminate this limitation several analytical models were implemented. These analytical models were created to generate the dependencies in a relationship between nodes. The dependencies depicted the nodes and their importance in the network. Hussain’s [19] novel approach states finding the main leads representing the terrorist groups where removing the path from the network may reduce the repercussions and make the network weak.

The paper deals with two stage framework; in the first stage an uncertain weighted index to each node is determined wherein the second stage the assumptions to the argument driven hypotheses are worked. The proposed paper concentrates on the middle age groups as they are more vulnerable to becoming part of these events. Thus people of these age groups status and identities are collected and studied. When applying it to the framework the weights of each node are evaluated. Once the weights are determined the next motive is to find the most influential or active path in the network. Finding the active or influential lead in the network makes easier for the hypotheses to work upon as if the influential node or the path is removed then the network could not be reached and entire network become destabilize.

This paper deals with 18 attributes which assemble the entire characteristics of the network and its attributes. The history of individual attached to the network is recorded and a weighted index is assigned to it. The empirical value is evaluated and with this the higher efficiency node to become influential in a network is seen. Further the argument driven hypotheses suggests the real potential in any node to become vulnerable. Different comparative levels are conducted and entire resource is computed carefully which is in itself a tough task as permutations of an individual with its entire history are to be maintained.

The real scenario suggests that a single node does not hamper the network rather it needs a quantity of key members to disrupt the network by their removing or killing.
Different networks are taken up in this paper to depict and conclude that destabilizing or disrupting any network which is harmful needs technical expertise and a quality in its information flow. If 25% of the data members who play significant roles in the terrorist network are found and removed from the network then the complete activity can be exposed and rendered.

B. SIMULATION AND COMPUTATIONAL MODELS

On the bases of simulation and predictive analysis Carley [20, 21] complex modelling tools were used for research in terrorism. The tool used was DyNet in which the textual data was analysed and was converted to the pictorial network where then the destabilizing of the network was proceeded. Various software were used for representation of the terrorist groups or network including Automap [20], NETEST [22]. These software works for the analysis of the network study wherein the social media became associated during the Mumbai attack. Several case studies have been later conducted to find the status and programming after the event. The 9/11 attack on the world trade tower lead to high loss of lives and property. The entire structure as to how hijackers took lead over the situation and their whereabouts of which passport were used to enter the country were culled. Though it took more time in getting through every link and facing the culprits but the every suspicious information was coiled. Figure 2 shows the mapping of the terrorist involved in 9/11 attack.

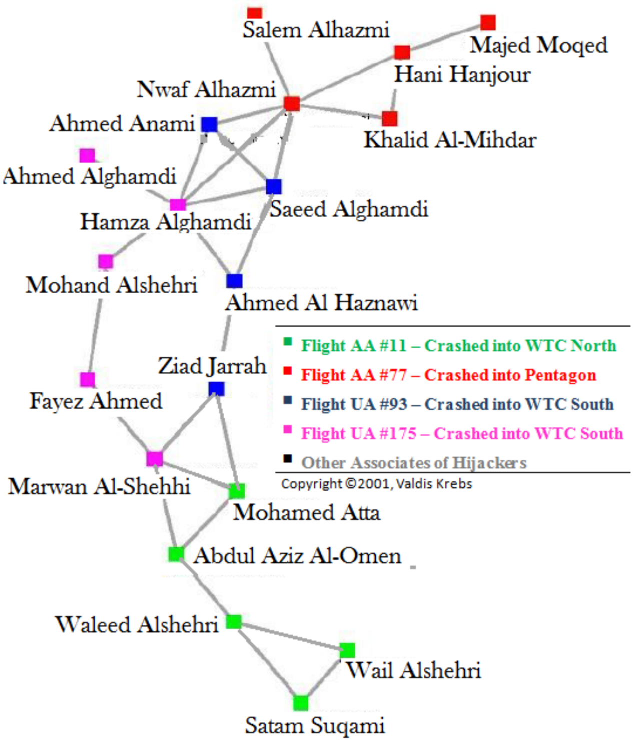

Figure 2 The network mapping of the 19 hijackers involved in 9/11 attack.

The links in the network associated with the terrorism are not the real links but those are formed by association which can be measured by their co-occurrences. The frequency of the co-occurrences of organization gives the idea of strong ties and strength of the bond. On knowing the co-occurrences the adjacency matrix is formed where the clustered nodes and network are studied.

C. COUNTER TERROR SNA AND INTENT RECOGNITION

Weinstein et al. [24] gave the counter terror SNA and intent recognition approach which works upon exploration of the dynamic network tools used for tracking and detection of the terrorist network. The modeling and simulation over the real attacks are done based on which the novel approach that uses Terror Attack descriptive Language which is helpful in generating the real attack scenarios to view and understand the transactions held. Social network analysis is used to filter the nodes that are outliers and identify the actors which combine to form a community. These communities can be formed using different algorithms defined by various authors to find best possible approach for representation of the network and classify them into certain groups based on their interests and behavior. The traffic including the nodes which cause hindrance in the network are examined and their modelling needs to be done as well because these help in separating the suspicious event or activities from the harmless one.

This paper deals with the multimedia data which is excessive in quantity and is raw for its purpose. The R & D is conducted on the raw data to extract the exploited data resource but only R &D does not solve the significant purpose. There needs to be automation tools which could analyze and trace the threats which are harmful and are dark network. The data is passed onto various levels of processing when the complete network is explored and its threats are predicted. Figure 3 shows the complete working of the CT-SNAIR.

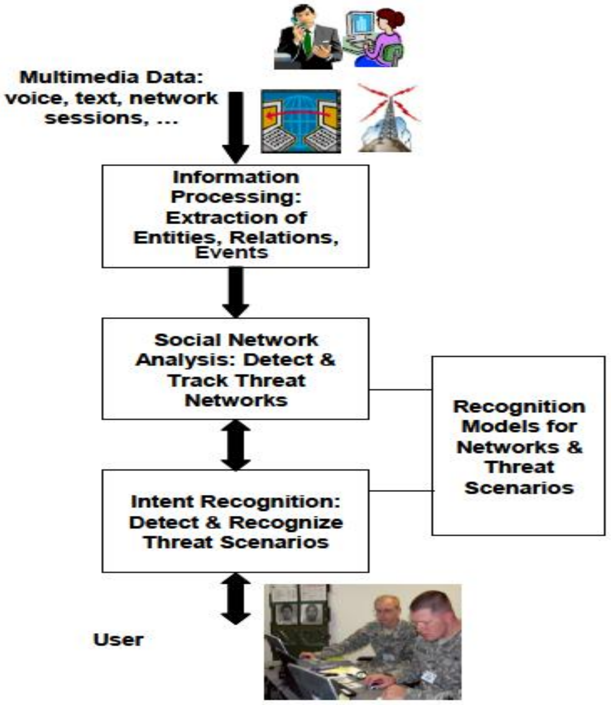

Figure 3 Data flow representing the CT-SNAIR approach.

The network attacks are formally analysed using the simulation and modelling framework which uses intelligence methods for its understanding of the network and perception. To understand the transactions held in the network author uses techniques that could identify the addressing of the actors in the network. The HMM modelling method focuses on finding the connection between the actors through the connecting links and possibility of recognizing one another through any of the 4 attributes used. The method limit where the network becomes multi connected and few of which could not be layered through anywhere thus needs to be left out. There are various levels in the simulation and modelling of the data extracted from multimedia and then the simulated data is used for its intent recognition as shown in figure 4 and 5.

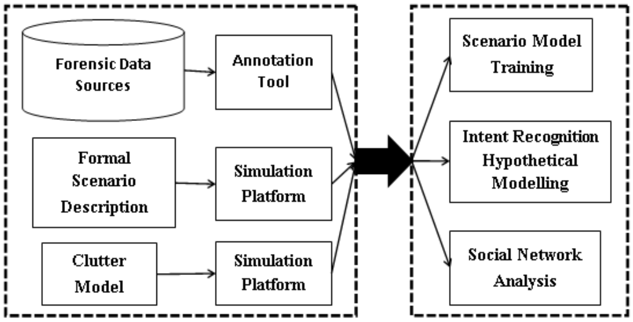

Figure 4 The Various levels of Simulation and modeling for CT-SNAIR.

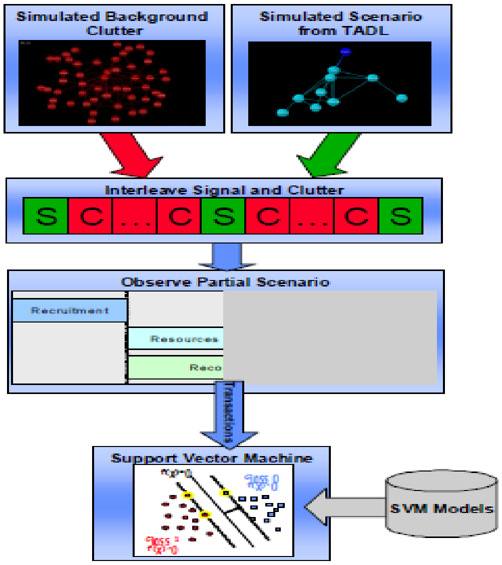

Figure 5 Simulated Data used for intent recognition.

The scenarios defined in the paper needs to be generalized as to include the social network analysis in combination with entity and attributes. Few of the data is illustrated in the paper using the scenarios defined and fruitful results are estimated. The framework works for the large data source where the clutter model is automatically found.

D. DynNetSim

This approach focuses on enhancing the counter terrorism using the intelligence analysis, protection measures for the infrastructure, pre planning and preparedness in case of the attack. Dynamic network need to be exceptionally visualized through better decision support system. DynNetSim gives a better version of its displaying the network through modelling its structure, simulating the behavior. The scenario which is its representational unit gives the clear picture of real as well as hypothetical situations. The multi node structure is modelled depicting the trends, causalities, events, behavior of the actors, variations and transactions associated in the network. DynNetSim is a layered processing model which specifies its domain initially and represents them using different framework on further it has platform to work upon various modes of attributes. This method reduces the risk factor and enables the individual to get prepared for any situation that might occur in situation caused by terrorism. The approach creates those scenarios which could make one understand the environment conditions when severe actions for the safety needs to be taken and thus consequences must be fought with confidence. The modelling adapts the environment conditions and gives the possible situation to be handled thus making the planning to be done with excellent decision making skills.

E.MULTI-FACTOR ANALYSIS OF TERRORIST ACTIVITIES

This paper proposed the six element analysis approach for the terrorist network detection. The six elements include individual, organization, time, location, method and event. Sub networks are managed to be drawn from the complete network through correlation analysis. The research claims to be better than the previous researches as it has better decision making concepts involved and early signs of the terrorist activities are made to be detected. This paper deals with the characteristics along with the people and organization getting to illustrate the entire network strategy and working. The East Turkistan terrorist activities are examined and 420 pages over the web are considered to show case the network assessment and their vulnerability. The multi view terrorist activities were monitored and understood. The sub network was analyzed with the attributes including various techniques and the revelation of the complete network management was presented.

CONCLUSION

This paper reviews few of the methods used for counter terrorism using the social network analysis. Terrorism has caused life threatening conditions at times and it is better to understand and be aware of the situations for dealing with people and for people. The above discussion establishes the fact that social network analysis has potential application in counter terrorism. It is evident from the literature that most of the terrorist activities are organized crimes. People involved in terrorist activities communicate among each other and they also want to influence other people for new recruit. They disguise behind unanimous profiles and interact. SNA helps in finding these disguised profiles by identifying the patterns of communication and by studying structural patters on the network they form. It has been investigated that that SNA has potential application in counter terrorism.

REFERENCES

[1] D.Charabarti and C. Faloutsos. “Graph Mining: Laws, Generators, and Algorithms.” ACM Computing Surveys 38:1(2006) p.4.

[2] J.R.Tyler, D.M.Wilkinson, and B.A. Huberman. “Email as Spectroscopy: Automated discovery of community structure within organizations.” In Communities And Technologies (2003) pp. 81- 96.

[3] J.G. Augustson and J.Minker. “An Analysis Of Some Graph Theoretical Cluster Techniques.” Journal of ACM 17:4 (1970) pp. 571-588.

[4] A. Calvo-Armengol and Y. Zenou. “Social networks and crime decisions: The Role Of Social Structure In Faciliating Delinquent Behaviour.” CEPR Discussion papers (2003) 3966.

[5] A.L. Barabasi. “Linked: The New Science ofNetworks”. Cambridge, MA: Perseus Publishing, 2002.

[6] R. Cross and A. Parker. “The Hidden Power ofSocial Networks.” Cambridge, MA, Harvard Business School Press, 2004.

[7] D. Knoke and S. Yang. ” Social network analysis (Quantitative applications in the social sciences).” New York: Sage Publications. (2008)

[8] S. Koschade. (2006). “A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence”. Studies in Conflict and Terrorism, 29(6), 559–575.

[9] S.F. Everton. (2012). “Disrupting dark networks”. New York: Cambridge University Press.

[10] S.F. Everton & D. Cunningham. (2012). “Detecting significant changes in dark networks”. Behavioral Sciences of Terrorism and Political Aggression, 5(2), 94–114.

[11] G. Bichler & S. Bush. (2015). Networks in a nutshell. In G. Bichler & A. Malm (Eds.), Disrupting criminal networks: Network analysis in crime prevention (pp. 233–244). Boulder, CO: Lynne Reinner Publishers, Inc.

[12] M. Granovetter (1973). “The strength of weak ties.” American Journal of Sociology, 78(6), 1360–1380.

[13] R. Burt. (1992). “Structural holes: The social structure of competition.” Cambridge, MA: Harvard University Press.

[14] D.J. Watts. (2003). “Six degrees: The science of a connected age”. New York: W.W. Norton & Company.

[15] V.E. Krebs. (2001). “Mapping networks of terrorist cells”. Connections, 24(3), 43–52.

[16] M. Sageman. (2004). “Understanding terror networks.” Philadelphia, PA: University of Pennsylvania Press.

[17] J. Xu & H. Chen. (2008). “The topology of dark networks.” Communications of the ACM, 51(10), 58-65.

[18] J. Magouirk, S. Atran, & M. Sageman. (2008). Connecting terrorist networks. Studies in Conflict and Terrorism, 31(1), 1–16.

[19] D. M. Akbar Hussain. “Terrorist Networks Analysis through Argument Driven Hypotheses Model”. In Second International Conference on Availability, Reliability and Security (ARES'07). IEEE 0-7695-2775-2. 2007.

[20] Diesner, J., Carley, K.M.: Using network text analysis to detect the organizational structure of covert networks. In: Proceedings of the North American Association for Computational Social and Organizational Science (NAACSOS) Conference (2004)

[21] Tsvetovat, M., Carley, K.M.: On effectiveness of wiretap programs in mapping social networks. Computational and Mathematical Organization Theory 13(1), 63–87 (2006).

[22] NETEST: Estimating a Terrorist Network’s Structure. In: 11th European Intelligence and Security Informatics Conference (EISIC), Athens (2011).

[23] Aparna Basu. “Social Network Analysis: A Methodology for Studying Terrorism”. M. Panda, S. Dehuri, and G.-N. Wang (eds.), Social Networking Intelligent Systems Reference Library 65, Springer International Publishing Switzerland 10.1007/978-3-319-05164-2_9. (2014). pp.215-242.

[24] Clifford Weinstein, William Campbell, Brian Delaney, Gerald O’Leary.” Modeling and Detection Techniques for Counter-

Terror Social Network Analysis and Intent Recognition" IEEE. 978-1-4244-2622-5 (2009) . pp. 1-16.

[25] Richard M. Adler," A Dynamic Social Network Software Platform for Counter-Terrorism Decision Support" IEEE. 1-4244-1330-3. (2007). Pp. 47-54.

[26] Julei Fu and Jian Chai "Multi-factor analysis of terrorist activities based on social network" In Fifth International Conference on Business Intelligence and Financial Engineering, IEEE 978-0-7695-4750-3. (2012) pp. 476-480.

Authors Profile

Atul Srivastava received the B. Tech. degree in Information Technology from the UP Technical University, Lucknow, India, in 2008, and M.Tech. degree in Information Technology from YMCA University of Science and Technology, Faridabad, India in 2012. He is a research student of YMCA University of Science and Technology, Faridabad, India. He is currently Assistant Professor at Pranveer Singh Institute of Technology, Kanpur, India.

Dr. Anuradha Pillai has received her M. Tech and PhD in Computer Engineering from MD University Rohtak, in the years 2004 and 2011 respectively. She has published 30 research papers in various International journals and conferences. She has more than 13 years of teaching experience. Presently she is serving as Assistant Professor at YMCA University of Science & Technology, A State Govt. University, Faridabad Haryana. Her research interests include Web Mining, Data Structures and Algorithms, Databases. Research Papers listed in database.

Dr. Dimple Juneja Gupta is working as Dean Research & Development at Poornima University, Jaipur, Rajasthan India.