I.J. Information Technology and Computer Science, **2013, 12, 21-30**
Published Online November 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2013.12.03

Efficient Algorithm for Destabilization of Terrorist Networks

Nisha Chaurasia
Department of CSE & IT, Madhav Institute of Technology and Science, Gwalior (M.P.), India
E-mail: chaurasianisha21@gmail.com

Akhilesh Tiwari
Department of CSE & IT, Madhav Institute of Technology and Science, Gwalior (M.P.), India
E-mail: atiwari.mits@gmail.com

Abstract— The advisory feasibility of Social Network Analysis (SNA) to study social networks have encouraged the law enforcement and security agencies to investigate the terrorist network and its behavior along with key players hidden in the web. The study of the terrorist network, utilizing SNA approach and Graph Theory where the network is visualized as a graph, is termed as Investigative Data Mining or in general Terrorist Network Mining. The SNA defined centrality measures have been successfully incorporated in the destabilization of terrorist network by deterring the dominating role(s) from the network. The destabilizing of the terrorist group involves uncovering of network behavior through the defined hierarchy of algorithms. This paper concerning the destabilization of terrorist network proposes a pioneer algorithm which seems to replace the already available hierarchy of algorithms. This paper also suggests use of the two influential centralities, PageRank Centrality and Katz Centrality, for effectively neutralizing of the network.

Index Terms— Data Mining, Social Network Analysis, Terrorist Network, Graph Theory

I. Introduction

The ever increasing availability of data has made data management and its significant retrieval troublesome manually hence the importance of mining of data for easy retrieval was felt and was made possible by introducing the eminent data mining concept. The data mining demonstrated its successful application for mining different kind data on the web. It grants the human ability to auspiciously mine interesting patterns according to the requirement without much labor. Not only limiting to mine useful information, data mining techniques are also beneficially used for classifying data, finding association among them, grouping them on the basis of similar characteristics and for uncovering the outliers. In addition to these techniques, data mining has established itself as the demanding field for studying social networks on web by applying one of its feasible techniques named Social Network Analysis (SNA).

Social Network Analysis is a data mining technique which usually analyzes the various social networks present on web. The technique is profitably used for studying the social behaviors of the networks. Thus social network analysis, from a data mining perspective, is also called link analysis or link mining [1]. The SNA uses a concept of centrality measures pointing out who is the central node(s) in the network. It is because of this that SNA is utmost utilized technique by the law-enforcement agencies for studying trends of hidden terrorist networks.

The web has unintentionally served these inhuman people for fulfilling their inhuman motives by allowing them to plan their strategy, convey messages, exchange documents, etc. As a result, it increases security concerns of security agencies on web too. Hence to diminish their existence their network patterns are studied and then network is neutralized in order to discontinue further communications within the network and prohibit the network members to plan their covert strategies.

In this context, when the SNA is applied for investigating of terrorist networks on web then it is acknowledged as Investigative Data Mining (IDM), also known as Terrorist Network Mining. Terrorist Network Mining is a technique defined for the analysis of hidden terrorist network that uses SNA and Graph Theory for the investigation. The technique discovers the most promising node(s) within the network and the goal is to remove this node(s) from the network in order to neutralize the network activities.

For the analysis, the terrorist network is considered as a graph and users are considered as its nodes. Using the SNA centrality measures i.e. degree and eigenvector, various roles are estimated from the graph. Making use of these measures and a third measure described for calculated dependency among nodes,

named as dependency centrality, a hierarchy is constructed in the form of a tree utilizing the two algorithms defined for destabilization of terrorist network.

The paper suggests replacing the two algorithms which were conventionally used for destabilization, by a proposed novel algorithm that performs the same task as done by the two algorithms. Also the paper urge to use the two other centrality measures i.e. PageRank and Katz centralities rather than degree and eigenvector respectively. The use of two measures would aid in an effective estimation of hierarchy followed by the terrorist networks.

The succeeding sections of this paper are organized as follows: Section 2 throws light on Social Network Analysis. Section 3 studies about Terrorist Network Mining. Section 4 describes about the Destabilization of Terrorist Network. Section 5 covers the Flaws noticed in the presently used Hierarchy of Algorithms. Section 6 explains Proposed Methodology. Section 7 presents the Experimental Results. Conclusion and Future Work are given in the final section.

II. Social Network Analysis

Social Network Analysis (SNA) is an analysis technique of social networks on web. The SNA technique defines the roles and interaction among the actors within the social network [2]. Social network analysis in general studies the behavior of the individual at the micro level, the pattern of relationships (network structure) at the macro level, and the interactions between the two [3]. A social network is usually represented by a graph, in which the set of vertices corresponds to the "actors" in a social network and the edges correspond to the "ties" between them [4]. SNA has been extensively preferred as the analysis technique because of its powerful estimation methodology known as centrality measures. The centrality measures are the network properties which serve as the essentialities of the SNA technique. It is because of the centralities, SNA helps in deciding the key nodes within a network. The centrality measures defined for estimating the node roles within a network are:

1) Degree defines the leader or the hub of the network.
2) Betweenness finds the extent to which a particular node lies between other nodes in a network.
3) Closeness, unlikely to betweenness, estimates the extent of farness of a node with respect to other nodes in a network.
4) Eigenvector defines the influence of a node on its neighbouring nodes.

Because of the magnificent applicability of SNA for analysing network behaviour has attracted the various law-enforcement agencies to use the technique for the analysing various hidden terrorist groups on web and enforce suitable remedies for their neutralization. Hence the technique when utilized with respective to determination of terrorist network present behind several legitimate networks on web is called as investigative analysis based on SNA or Investigative Data Mining (IDM).

III. Terrorist Network Mining/ Investigative Data Mining

Since criminals are hidden among the genuine users, criminal intelligence analysis therefore requires the ability to integrate information from multiple crime incidents or even multiple sources and discover regular patterns about the structure, organization, operation, and information flow in criminal networks [5]. Hence IDM is understood as an intelligent network analysis tool. Investigative Data Mining (IDM) is defined as "the technique which models data to predict the structure of a non-hierarchical network, determine associations and help in destabilizing the terrorist networks" [6]. IDM is a SNA technique used for studying associations and predicting the behavior of terrorist networks in order to identify key nodes for the purpose of destabilizing of the network. SNA is considered well suited for mining large volume of association data to discover hidden structural patterns in terrorist networks. Social Network Analysis (SNA) provides a set of measures and approaches for the investigation of terrorist networks [7].Hence IDM is supposed as the combination of data mining and subject-oriented automated data analysis techniques. Data mining serves as an approach which uses predictive approach for discovering patterns in dataset and subject-based automated data analysis regulate models to data for predicting the behavior, access risk, determine associations, or perform other types of analysis. IDM aims to connect the dots between individuals and map and measure complex, covert, human groups, and organizations [8].The main focus of IDM approach is to identify important actors, crucial links, subgroups, roles, network characteristics, and so on, to answer substantive questions about terrorist organizational structures [7].

IDM borrows ideas from social network analysis (SNA) and graph theory techniques in order to connect the dots and assist law enforcement agencies to disconnect the terrorist networks [9]. Social Network Analysis applies various SNA techniques that help in assessment of the key roles in network users as leader or gatekeeper. Graph theory gives a number of concepts and procedures that aims to detect maximal subgraphs in a graph (or network) that have a certain property and looses this property by adding another point and its relationships to the subgraph [6].

Using the graph theory, the terrorist network under investigation is considered as an undirected and unweighted graph with users as the nodes and their relationship as links among them. The graph in mathematical form is represented as an adjacency matrix, A_{ij} such that

$$A_{ij} = \begin{cases} 1, & if\ i\ and\ j\ are\ connected \\ 0, & else \end{cases}$$

following the property of symmetric matrix, i.e. $A_{ij} = A_{ji}$.

Taking the adjacency matrix obtained into account, the two sophisticated centrality measures, degree and eigenvector are calculated that are significantly used for determining the central member in the network. A central member may play a key role in a network by acting as leader who issues commands and provides steering mechanisms or serving as gatekeeper who ensures that information or goods flows effectively among different components of the networks [10]. These measures are illustrated as:

3.1 Degree:

The Degree of a vertex in a network is the number of edges attached to it [11]. It is calculated as the sum of all directly linked nodes connected to a node for which degree is measured. It reveals the hub or the leader node(s) in the graph. Hence degree, Di calculated for a node i, is mathematically represented as:

$$D_i = \sum_{j=1}^{n} A_{ij} \tag{1}$$

3.2 Eigenvector:

Eigenvector centrality (EC) of a node in a network is defined to be proportional to the sum of the centralities of the node's neighbors, so that a node can acquire high centrality either by being connected to a lot of others (as with simple degree centrality) or by being connected to others that themselves are highly central [12]. It assumes that not all connections are equal as connections to terrorists who are themselves influential will lend a terrorist more influence than connections to less influential terrorists. Mathematically, EC is formulated as the average of centralities of the neighboring nodes of vertex i:

$$EC_i = \frac{1}{\lambda} \sum_{i=1}^{n} A_{ij} EC_j \tag{2}$$

where, ECi is the centrality of vertex i, λ is a constant called Eigenvalue. These centralities are represented in vector form as EC = (EC1, EC2, EC3 …) and the above equation is rewritten as:

$$\lambda EC = A.EC \tag{3}$$

Hence, EC is the eigenvector for the matrix Aij along with Eigenvalue λ. Assuming that we wish the centralities to be non-negative, it can be shown that λ must be the largest Eigen value of the adjacency matrix and x the corresponding Eigenvector [13].

Removal of top leadership caused problems initially, but in network structures, the network is able to recover quickly and become more efficient [14]. The idea of destabilization is thought to find the most effective node(s) and then removing that node(s) in order to neutralize their activities. To gain better destabilization, a third centrality was defines named as Dependency Centrality for finding the level of dependency of a node on other nodes in a network.

3.3 Dependence Centrality (DC):

The basic purpose of the DC is in the network destabilization process where the nodal dependency is estimated for determining the most influential node(s) in a network. Memon et al [11] defined the dependence centrality of a node as how much that node is depending on any other node in the network. In mathematical structure, DC is calculated as:

$$DC_{ij} = \sum_{i \neq k, k \in G} \frac{d_{ij}}{N_k} + \Omega \tag{4}$$

Where, DC_{ij} is the dependence centrality being calculated for node i depending on node j, dij is the geodesic path from i to j, and N_k is the number of shortest paths being traversed by node i to node j through the third node k. If the graph is connected, the value for Ω is assumed as 1 otherwise 0.

The three centralities finally after estimation for each network node is incorporated for finding the hidden hierarchy of the terrorist network which is done using the two hierarchical algorithms defined for destabilizing terrorist networks.

IV. Destabilization of Terrorist Network

The concept of destabilizing a terrorist network was introduced by N.Memom et. al [9] in 2006. The destabilization was attempted by performing role analysis within the network. Role analysis is performed to find out who is in a network. This is done usually by evaluating the efficiency of the network, critical components of a network, a proposed measure "Position Role Index" (PRI) and dependence centrality.

4.1 Efficiency of the Network E(G)

Efficiency of the network E(G), to quantify how efficiently the information is exchanged among the nodes in the network. For efficiency calculation of the graph G, the shortest (d_{ij}) among the two nodes, i and j is found. It is supposed that the nodes send information through their edges. The efficiency ε_{ij} in the communication between vertex i and j is inversely proportional to the shortest distance: $\varepsilon_{ij} = 1/ d_{ij}$ for all i, j; when there is no path in the graph between i and j, we get $d_{ij} = +\infty$ and consistently $\varepsilon_{ij} = 0$ [3]. Hence, efficiency of the graph, E(G) is calculated as:

$$E(G) = \frac{\sum_{i \neq j \in G} \varepsilon_{ij}}{N(N-1)} = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}} \qquad (5)$$

Where, N denotes size of the graph or the number of nodes in the graph. The value of E practically normalized, lies between [0, 1] but it can vary in the range [0, ∞].

4.2 Critical Components of a Network

Critical components of a network is used for finding the measure of the centrality of a node, using which the drop in the network efficiency is evaluated when that node is deactivated from the network.

The method is mainly used to determine the critical nodes in the graph. The importance (I) of a node i in the graph G, is calculated as:

$$\begin{aligned} I(node\,i) &= \mathrm{V}E \\ &= E(G) - E(G - node\,i); \\ i &= 1, \ldots, N \end{aligned} \qquad (6)$$

Where, E(G-node i) is the efficiency of the network (G-node i), obtained by deactivating the node i from the graph G. The node with highest value of ΔE is the critical or the important node.

4.3 Position Role Index (PRI)

Position Role Index (PRI), highlighted a clear distinction between followers and gatekeepers (It is a fact that leaders may act as gatekeepers) [3]. The presence of the followers results in low efficiency as compared to their absence. When a graph is plot along x-y plane, the plots below the x-axis are followers, while the nodes higher than remaining nodes with higher values on positive y axis are the gatekeepers. While the nodes which are on the x-axis usually central nodes, which can easily bear the loss of any node. The leaders tend to hide on x-axis there [3].

4.4 Dependence Centrality

Dependence Centrality as discussed earlier is used for finding the node dependency on other nodes of the network and finding the leader/gatekeepers.

With respect to the role analysis, hierarchy of the terrorist network is determined. Discovering hierarchy in a terrorist network is a process of comparing different centrality values of different nodes to identify which node is more powerful, influential or worthy to neutralize than others [12]. Hence, two algorithms were defined to uncover network hierarchy such that destabilization is achieved in a promising manner. The objective of the first algorithm was to convert the network's undirected graph obtained by SNA approach into a directed graph utilizing the degree and eigenvector centrality measures. Meanwhile the second algorithm works specifically for destabilization by constructing a tree from the graph, by calculating the dependency of each node to other nodes in the network. The later algorithm involved dependence centrality (DC). The nodes with less DC are predicted as the key player (leader or the gateway) nodes as they are the nodes with highest number of direct links to other nodes and do not depend on any other nodes in the network for communication. The intelligence agencies can easily detect who are potential leaders/gatekeepers and even peripheries by using these new algorithms [10].

The purpose of proposing the hierarchy of algorithms is to solve the dilemma that occurred during the estimation of influential nodes considering the hierarchy in form of a tree. The dilemma constituted two concerns:

1) The first dilemma was that sometimes there are chances where centrality measures for more than one nodes holds the same value hence creating difficulty in identifying which node will be parent and which will be a child.
2) The second dilemma was to judge which node would be parent and which would be a child in the hierarchy, if more than two nodes qualify as powerful nodes over another particular node.

The dilemma was familiarized as ABC problem as it becomes very tedious to decide where to place node C as a child, if nodes A and B being promising nodes are nominees of its parent node. The dilemma was tackled by introducing dependency centrality of a node. After resolving the dilemma, hidden hierarchy was detecting using the two algorithms. The algorithms worked as following:

1) The first algorithm was to covert an undirected network graph into a directed graph using degree and eigenvector centralities. The node with higher degree emerges link to a node with less degree value. If value of degree for two nodes is same then the same judgment is followed for eigenvector value for those nodes. And even then also if the value for nodes is

same in case of eigenvector, the link among nodes is ignored.

2) The second algorithm intakes the directed graph obtained from the first algorithm constructs the hierarchy of parent and child nodes in form of a tree structure. In case if two nodes qualifies for being parent of a particular node then the node with maximum neighbors is considered as parent for that particular node. This represents the fact that the true leader, with respect to a node, is more influential on its neighborhood [12].

After constructing the hierarchy, the hierarchical relationship among the parents of a node is discovered. Finally, the most promising parent is detected from possible parents using dependence centrality.

The two algorithms can be illustrated as [10]:

Algorithm 1: Converting undirected graph G into directed graph

1) Take any node "n" of graph G, and find its neighbors "N".

2) Take a node "s" such that s € N (N is set of neighbors of n.). Compare Degree Centrality of s to Degree Centrality of n,

•if Degree Centrality of s > Degree Centrality of n, Mark a directed edge from s to n.

•if Degree Centrality of s < Degree Centrality of n, Mark a directed edge from n to s.

•if Degree Centrality of s = Degree Centrality of n Compare Eigen-Vector Centrality of s to Eigen-Vector Centrality of n,

•If Eigen-Vector Centrality of s > Eigen-Vector Centrality of n, Mark a directed edge from s to n.

• If Eigen-Vector Centrality of s < Eigen-Vector Centrality of n, Mark a directed edge from s to n.

•If Eigen-Vector Centrality of s = Eigen-Vector Centrality of n, Ignore the link.

3) Repeat Step 2 for every member of N.

4) Repeat Step 1 for every node of graph G.

Algorithm 2: To make Tree T from Directed Graph D:

1) Take any node "n" of directed Graph "D", and find all the nodes "N(n)" adjacent to edges originating from node n. and mark them as Children of n. Here N(n) is neighbors N of node n.

2) Find all the nodes (parents) "P" adjacent to edges pointing to node n and mark them as Parents of n.

3) Repeat step 1 and 2 for all nodes of Directed Graph D.

4) Again take any node "n" of directed Graph "D",

5) If number of elements in P (where P is the set of Parents of n) is 0, then add "root "of Tree "T" as its parent and mark node n as children of "root".

6) If number of elements in P > 1, Remove all the nodes except "p1" from P, such that (N (p1) ∩ N (n)) is maximum (Where N (p1) is the set of Neighbors of p1). Also mark n as Children of p1.

7) If number of elements in P is still > 1, remove all the nodes from P except the node p1, for which the n has highest Dependence Centrality. Also mark n as children of p1.

8) If number of elements in P is still > 1, Remove all of its parents and then add "root" of Tree T as its parent and also mark node n as children of "root".

9) Repeat Step 4 to 8, for all nodes of directed graph D.

10) Draw Tree T.

V. Flaws Noticed in the Presently Used Hierarchy of Algorithms

Though the present hierarchy of algorithms is quite capable of determining the hidden hierarchy of the terrorist network, there are certain up-gradations are required with the view for improving the efficiency of the algorithm. Also the algorithms needs to be executed in hierarchy in order to obtained the desired results. This section involves discussion about the shortcomings that makes the presently available hierarchy of algorithms for destabilization. These flaws are as follows:

1) One needs to run the two algorithms separately in order to uncover the hidden hierarchy.

2) The first algorithm i.e. algorithm for converting an undirected graph to a directed graph was only utilized for generating children and parent set for the second algorithm.

3) The number of steps for calculating the neighbor set, parent and children set required separate execution instead they can be calculated altogether.

4) Some nodes that do not require consideration i.e. the nodes with least centrality values should be taken into account during execution.

VI. Proposed Methodology

The proposed methodology includes two subsections: Recommended Centrality Measures and The Proposed Algorithm for Destabilization. The former section recommends making use of PageRank and Katz

centrality measures rather than using Degree and Eigenvector traditionally for discovering the hidden hierarchy of the terrorist network. The two measures PageRank and Katz helps to overcome the conflict to judge two nodes with same centralities that arises during the application of destabilization algorithms. The two measures almost every time results in two different values for each node henceforth removing the conflict to a greater extent. Apart from these two measures, the later section defines the new destabilization algorithm that would consume lesser time and space complexity in comparison to already defined hierarchy of algorithms.

6.1 Recommended Centrality Measures

6.1.1 Katz Centrality

Katz centrality measures the extent of influence of a node in a network i.e. it counts the number of walks starting from a node or ending on a node, providing penalties to longer walks. Katz is assumed as a variation of the previously discussed eigenvector centrality. It finds the influence by taking into consideration the total number of walks among a pair of nodes in a network. Katz evaluates this relative influence of a node by measuring the number of the immediate neighboring nodes and the nodes that are connected to the node through these neighboring nodes. As the connection between nodes is estimated through the walk or length for the pair of node, hence length is inversely related to the strength of connection (strong or weak). In mathematical form,

$$x_i = \alpha \sum_j A_{ij} x_j + \beta \tag{7}$$

where, α and β are the constants referred as normal eigenvector centrality and free centrality respectively, x_i and x_j is the pair of node for which Katz centrality is being calculated. Since the series need to be converged, hence α must be smaller than the reciprocal value of the maximum eigenvalue $\lambda_{max}(A)$ of the adjacency matrix A.

β is generally assumed to be 1 due to negligence of absolute values typically. Expecting the value as 1 because even if α tends to 0, the constant term β remains while for the eigenvector, term disappears. The β is a positive penalty constant to control the weight on the walks of different length [15].

The same equation may be represented in matrix form:

$$x = \alpha Ax + \beta.1 \tag{8}$$

or,

$$x = \beta(I - \alpha A)^{-1}1 \tag{9}$$

Katz here involves an identity matrix which indicates a connection of each actor with itself as strongest connection. Katz centrality does not bother about the direction of the link thus it is supposed profitable to determine the influence for a symmetric matrix.

6.1.2 PageRank Centrality

PageRank Centrality is a way to measure network centrality similar to degree centrality. It is considered as an enhance version of in-degree centrality used to measure the influence on other nodes in the network. PageRank is Google's patented algorithm for examining the entire link structure of the web and determine which pages are most important.

One of the problems with Katz centrality is that a high centrality is gained by other nodes those who were pointed by any high centrality node in the network. This problem was tackled using the PageRank centrality. The PageRank in place of assigning whole of centrality of a high centrality node, just assigns a fraction of the node's centrality to its neighboring nodes.

$$x_i = \alpha \sum_j A_{ij} \frac{x_j}{K_j^{out}} + \beta \tag{10}$$

, where, x_i and x_j is the node pair for which centrality is to be calculated; α and β are the constants similar to that of Katz centrality. The value for α is usually assumed as 0.85 (as Google uses this value as its empirical choice) but it is expected to be less than inverse of the largest eigenvalue of AD^{-1} while β again is set to 1 as a positive penalty constant.

K_j^{out} is the out degree centrality of node j. K_j^{out} is set to 1 if $K_j^{out} = 0$ as $A_{ij} = 0$ and the role of non out-degree nodes remains zero. Hence relation of the PageRank centrality with out-degree can be viewed as the centrality derived from a node neighbors is proportional to their centrality divided by their out-degree.

Again the PageRank centrality in matrix form is written as:

$$x = \alpha AD^{-1}x + \beta.1 \tag{11}$$

or,

$$x = \alpha AD^{-1}x + 1 \tag{12}$$

again,

$$x = (I - \alpha AD^{-1})^{-1}.1 = D(D - \alpha A)^{-1}.1 \tag{13}$$

where, D is the diagonal matrix having $D_{ii} = \max(k_i^{out}; 1)$ elements and I is the identity matrix of A_{ij}.

6.2 Proposed Algorithm for Destabilization

The proposed algorithm works out better when compared with the two present algorithms. The algorithm not only provides the desirable outcomes but also removes the shortcomings that were noticed while using the two algorithms.

The framework of the proposed algorithm is as follows:

1) Take any node n of graph G and find its neighhbors N

2) Take a node m such that m€N

3) Compare PageRank Centrality of m to PageRank centrality of n

- *if (PageRank centrality of m > PageRank Centrality of n)*

  add node m to Parent set of n

- *else if (PageRank centrality of m < PageRank Centrality of n)*

  add node m to Children set of n

- *else*

  - *if (Katz centrality of m > Katz Centrality of n)*

    add node m to Parent set of n

  - *else if (Katz centrality of m < Katz Centrality of n)*

    add node m to Children set of n

  - *else*

    ignore the link

4) Repeat step 3 for all nodes

5) If number of elements in Parent set is 0, add "root" of tree T as its parent and mark n as children of "root".

6) If number of element in Parent set is 1, mark the node as the parent of n

7) If number of elements in Parent set >1, remove all nodes from Parent set except the node P1 such that

[N(P1)∩N(n)] is maximum (where N(P1) is the set of neighbors of P1); and mark n as children of P1.

If N(P1)∩N(n) = 0, ignore the node

VII. Experimental Results

The performance of the proposed algorithm is assessed through the 26/11 attacks dataset. The dataset involved thirteen terrorists who were responsible for the disaster. Among the 13 terrorists, Wassi is expected as the most crucial node in the network as it led multiple communications through it with highest number of direct connections with other nodes in the network. The following table1 lists the name of the thirteen terrorists and a number assigned to them respectively for the ease of experiment.

Table 1: Names of terrorists of 26/11 attacks

S. No.	Name of Terrorist
0	Abu Kaahfa
1	Wassi
2	Zarar
3	Hafiz Arshad
4	Javed
5	Abu Shoaib
6	Abu Umer
7	Abdul Rehman
8	Fahadullah
9	Baba Imran
10	Nasir
11	Ismail Khan
12	Ajmal Amir Kasab

The graph constructed for the 26/11 attackers is as follows:

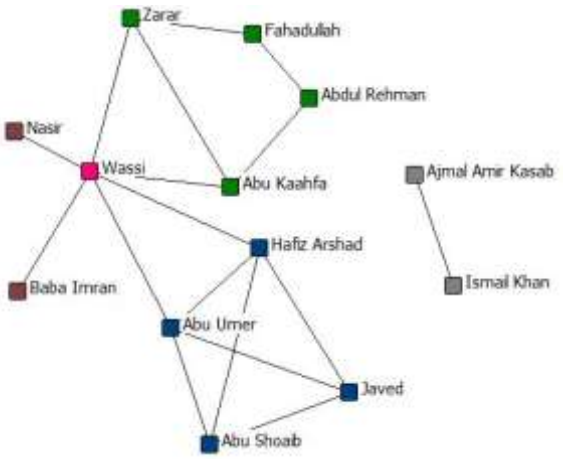

Fig. 1: 26/11 Terrorist Network

The software used for the construction of 26/11 network is UCINET which represents, analyzes, visualizes, and simulates nodes (attackers) and ties (relationships) from the input data [16]. UCINET is a social network analysis tool produced by Analytic Technologies [17]. All of the experimental analysis is performed using UCINET.

The values of centralities for each terrorist member obtained are calculated and are utilized in the algorithm for destabilization. The centralities values estimated are as follows:

Table 2: Centralities of Terrorists

Name of Terrorist	Degree	EC	DC	PgRank	Katz
Abu Kaahfa	3	0.206	1.160	0.074	1.087
Wassi	6	0.444	1.248	0.210	2.572
Zarar	3	0.206	1.164	0.074	1.087
H. Arshad	4	0.456	1.164	0.146	1.467
Javed	4	0.456	1.167	0.074	0.992
Abu Shoaib	3	0.358	1.167	0.109	0.773
Abu Umer	3	0.358	1.164	0.146	1.467
A. Rehman	2	0.081	1.123	0.069	0.260
Fahadullah	2	0.081	1.163	0.069	0.260
Baba Imran	1	0.125	1.190	0.039	0.514
Nasir	1	0.125	1.190	0.039	0.514
IsmailKhan	1	0.000	0.996	0.039	1.000
A.A. Kasab	1	0.000	0.996	0.039	1.000

While executing the dataset using Degree and Eigenvector Centralities values, the following results shown in table were obtained from the older hierarchy of algorithms.

Table 3: Parent and Children Set using Degree and Eigenvector for Hierarchy of Algorithms

Parent Set	Children Set
1,2	2,7
-	0, 2, 3, 6, 9, 10
0, 1	0, 8
1, 6	4, 5, 6
3, 5, 6	-
3, 6	4
1, 3	3, 4, 5
0, 8	8
2, 7	7
1	-
1	-
12	12
11	11

Similarly, on executing the proposed algorithm with Degree and Eigenvector centralities, the acquired outcomes are more accurate than the previous hierarchy of algorithms. It is very clear here that Wassi who is assigned number 1 acts as the parent for multiple nodes. Hence it is the node which needs to be taken into consideration. This can be viewed in Table 4:

Table 4: Parent and Children Set using Degree and Eigenvector for Proposed Algorithm

Parent Set	Children Set
1	-
-	0, 2, 3, 6, 9, 10
1	-
1	4, 5
3, 6	-
3, 6	-
1	4, 5
0	-
2	-
1	-
1	-
-	-
-	-

Finally, again when the proposed algorithm was executed using PageRank and Katz Centralities the promising outputs are obtained. These outcomes shows that the parent set accomplished consists of only selective nodes and does not considers the nodes that are undesirable usually during analysis. Subsequently, the acquired candidate or neighbor set offers selective child nodes for forming the hierarchy.

Table 5: Parent and Children Set using PageRank and Katz for Proposed Algorithm

Parent Set	Children Set
1	-
-	0, 2, 3, 6, 9, 10
0,1	-
1,6	4, 5
3, 6	-
3, 4, 6	-
1	3, 4, 5
0,8	-
0,7	-
1	-
1	-
-	-
-	-

Following are the figures respective to the tables of the tree hierarchy achieved after processing the algorithms:

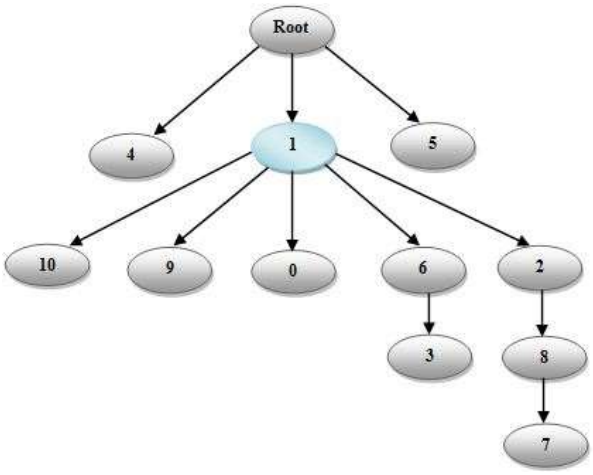

Fig. 2: Hierarchy graph for table1

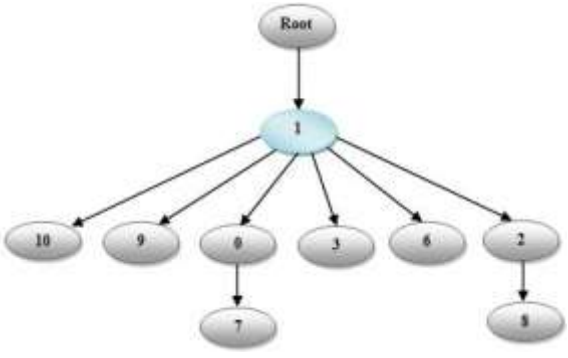

Fig. 3: Hierarchy graph for table2

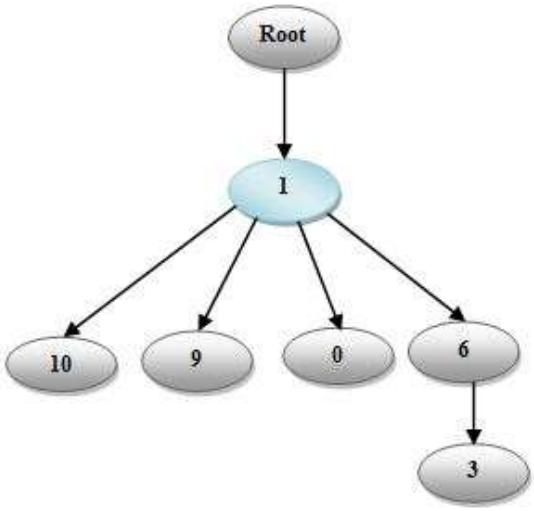

Fig. 4: Hierarchy graph for table3

VIII. Conclusion and Future Work

This paper presented a new destabilization algorithm for terrorist networks on web. The proposed algorithm along with less time and space complexity provides much appreciable outcomes. The previously known hierarchy of algorithms on execution, results in presenting every node in the outcome instead the n2ew algorithm making use of PageRank and Katz centralities, results in presenting selective nodes that are capable enough to indicate the most influential node in the network. It was notified that Wassi had the maximum influence in the 26/11 attacks dataset, thus needs to be deterred from the network in order to neutralize the network activities. Hence it may be assumed that the algorithm proposed will aid the law enforcement agencies to track the terrorist whose removal will result in disrupting the network on whole. In consideration to strong points discussed, the future scope would be to enhance the algorithm by limiting the nodes traversed during detection as the less active nodes which are not important for estimating the key node(s) and may be neglected for the ease of computation.

References

[1] Jiawei Han & Micheline Kamber: Data Mining: Concepts and Techniques, Second Edition, Morgan Kaufmann Publishers (2006).

[2] Nisha Chaurasia, Mradul Dhakar, Akhilesh Tiwari and R. K. Gupta: A Survey on Terrorist Network Mining: Current Trends and Opportunities, International Journal of Computer Science and Engineering Survey (IJCSES), 3(4), pp. 59 – 66 (2012).

[3] Nasrullah Memon, Henrik Legind Larsen: Structural Analysis and Destabilizing Terrorist

Networks, In: The First International Conference on Availability, Reliability and Security, 2006. ARES 2006, IEEE (2006).

[4] Scott, J.: Social Network Analysis: A Handbook, 2 edn. Sage Publications, London 2000.

[5] Nasrullah Memon, Abdul Rasool Qureshi: Investigative Data Mining and its Application in Counterterrorism, In: Proceedings of the 5th WSEAS Int. Conf. on Applied Informatics and Communications, Malta, pp. 97-403 (2005).

[6] Nasrullah Memon, Kim C. Kristoffersen, David L. Hicks and Henrik Legind Larsen: Detecting Critical Regions in Covert Networks: A Case Study of 9/11 Terrorists Network, In: Second International Conference on Availability, Reliability and Security (ARES'07), IEEE (2007).

[7] Muhammad Akram Shaikh, Wang Jiaxin: Investigative Data Mining: Identifying Key Nodes in Terrorist Networks, Multitopic Conference, 2006. INMIC '06, pp. 201-207 IEEE IEEE (2006).

[8] Uffe Kock Wiil, Nasrullah Memon, and Panagiotis Karampelas: Detecting New Trends in Terrorist Networks: In: 2010 International Conference on Advances in Social Networks Analysis and Mining (2010).

[9] Nasrullah Memon, David L. Hicks and Henrik Legind Larsen: Harvesting Terrorists Information from Web, In: 11th International Conference Information Visualization (IV'07), IEEE (2007).

[10] Nasrullah Memon, Henrik Legind Larsen: Practical Approaches for Analysis, Visualization and Destabilizing Terrorist Networks, In: Proceedings of the First International Conference on Availability, Reliability and Security,ARES (2006).

[11] Nasrullah Memon, David L. Hicks, Dil Muhammad Akbar Hussain and Henrik Legind Larsen: Practical Algorithms And Mathematical Models For Destabilizing Terrorist Networks, In: Sharad Mehrotra, Daniel Dajun Zeng, Hsinchun Chen, Bhavani M. Thuraisingham, Fei-Yue Wang (Eds.): ISI 2006, LNCS 3975, pp. 389. Springer-Verlag Berlin Heidelberg (2006).

[12] Nasrullah Memon, Henrik Legind Larsen, David L. Hicks, and Nicholas Harkiolakis: Detecting Hidden Hierarchy in Terrorist Networks: Some Case Studies, In: Proceedings of Springer-Verlag Berlin Heidelberg 2008, ISI 2008 Workshops, LNCS 5075, pp. 477–489 (2008).

[13] Memon, N., Larsen H.L.: Investigative Data Mining Toolkit: A Software Prototype for Visualizing, Analyzing and Destabilizing Terrorist Networks. In: Visualizing Network Information, pp. 14-1 – 14-24 (2006).

[14] Carley, Kathleen M.; Reminga, Jeffrey; and Kamneva, Natasha: Destabilizing Terrorist Networks, In: Proceedings of the 8th International Command and Control Research and Technology Symposium (2003).

[15] U Kang, Spiros Papadimitriou, Jimeng Sun, Hanghang Tong: Centralities in Large Networks: Algorithms and Observations, In: SIAM International Conference on Data Mining (SDM'2011), Phoenix, U.S.A. (2011).

[16] Sarita Azad and Arvind Gupta: A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis, Journal of Terrorism Research, Volume 2, Issue 2 (2011).

[17] Borgatti,. S. P., Everett, M. G. and Freeman, L. C.: UCINET 6 for Windows, Analytic Technologies, Cambridge, MA: Harvard University Press (2002).

Authors' Profiles

Nisha Chaurasia: Nisha Chaurasia is M.Tech Scholar in Computer Science Engineering at Madhav Institute of Technology and Science (MITS), Gwalior, M.P. (India). She completed her Bachelor of Engineering in 2011 in Information Technology from MITS, Gwalior, M.P. (India). She is a member of IAENG and Journal of Terrorism Research.

Akhilesh Tiwari: He has received Ph.D. degree in Information Technology from Rajiv Gandhi Technological University, Bhopal, M.P. (India). He is currently working as Associate Professor in the Department of CSE & IT, Madhav Institute of Technology & Science (MITS), Gwalior, India. He has guided several theses at Master and Under Graduate level. His area of current research includes Knowledge Discovery in Databases and Data Mining, Wireless Networks. He has published more than 20 research papers in the journals and conferences of international repute. He is also acting as a reviewer & member in editorial board of various international journals. He is having the memberships of various Academic/ Scientific societies including IETE, CSI, GAMS, IACSIT and IAENG.

How to cite this paper: Nisha Chaurasia, Akhilesh Tiwari,"Efficient Algorithm for Destabilization of Terrorist Networks", International Journal of Information Technology and Computer Science(IJITCS), vol.5, no.12, pp.21-30, 2013. DOI: 10.5815/ijitcs.2013.12.03

