A New Fuzzy based Approach for Destabilization of Terrorist Network

Suraksha Tiwari
Research Scholar, Computer Science Dept.
Vikrant Institute of Technology & Management
Gwalior, India

Shilky Shrivastava
Asst. Professor, Computer Science Dept.
Vikrant Institute of Technology & Management
Gwalior, India

Manish Gupta
Asst. Professor, Computer Science Dept.
Vikrant Institute of Technology & Management
Gwalior, India

ABSTRACT
The wide scope of Social network analysis has led the law require agencies to study the performance of social network. The main objective of this study is to identify the key nodes (suspicious nodes) present in the network. Recently, Terrorist Network Mining (special branch of Social Network Analysis) has gained considerable prominence in the data mining community because of its relevance to the real scenario situation and need. This paper proposes a new Fuzzy based optimization mechanism. The proposed optimization mechanism is appropriate for operative optimization of big social network holding non terrorist and terrorist nodes. At the time of the optimization procedure elimination of non-terrorist nodes from the network has been performed and the optimization resultant represents only the reduced / optimized graph holding only the collection of potential nodes. Fuzzy Rule based system for the security of the cyber is a system that contains a rule depository and a mechanism for the accessing and also running the rules. The depository is generally created with a group of the related rule sets. The goal of this study is to progress of a fuzzy rule based practical indicator for the security of cyber with the use of an skillful method which is named System of the Fuzzy Rule Based Cyber Expert. Rule based systems employ fuzzy rule to the automate complex procedures. A common cyber threats expected for the cyber specialists are used as linguistic variables in this paper. However, these algorithm results in fruitful outcomes, there is a need to propose a typical algorithm for destabilization. In consideration to this, the present paper proposes a novel algorithm for destabilization of terrorist network revealing the hidden hierarchy followed by the network.

Keywords
Social Network Analysis, Terrorist Network Mining, Fuzzy Rules,Investigative Data Mining

1. INTRODUCTION
Security of the global security came into the limelight after 9/11 attacks. The problem faced by the law enforcement agencies is the largest crime 'raw' data volumes and the absence of the sophisticated network tools and methods to apply the data efficiently and competently. Likewise, the web traffic produces a huge quantity of data from which only a minor portion is important to the intelligence[18].

Data mining (sometimes known as data or knowledge discovery) is analyzing of data procedure from different perspectives and summarizing it into valuable knowledge-knowledge that can be used to the growth revenue, cut costs, or both [2]. Data mining software is one of the no. of the analytical tools for examining data. It permits users to study data from numerous various dimensions or angles, classify it, and summarize the relationships identified [1].

Terrorist network mining has emerged as the novel field of the study often applied to the investigation of systematized crimes. Relationship among terrorists/ criminals form the basis for the prepared crimes and are vital for smooth process of a terrorists/ criminals group which can be observed as a network where nodes represents terrorists and links signify relationships or associations between terrorists [3].

Classicaly, study of the terrorist network was a manual procedure consuming much time and effort because of knowledge overload and thus failed to produce valuable knowledge on time, hence real methods are of essence to amend the knowledge overload problematic. This paper defines the methods that produce patterns distinguishing between legitimate and threat groups and helps law enforcement agencies to select which networks to put under the scrutiny.

2. DATA MINING
Data mining, also popularly referred to as the KDD (knowledge discovery from data), is automated or the convenient method for finding patterns that were previously unknown, signifying the knowledge implicitly stored or captured in great databases, data warehouses, the Web, other massive knowledge repositories, or data streams [9]. In other words, data mining refers to extracting or "mining" knowledge from large amounts of data.

Data mining is being successfully implemented in various fields likewise marketing, financial affair, business organizations and many more. Data Mining also perform a projecting role in the data study by removing valuable knowledge from ever growing great quantity of the data. Hence, because of this feature of dominating data mining discovered its significance in discovery of covert users secreted on the web by its valuable methods.

Data mining tasks involve discrimination and also characterization, association rule mining, clustering, classification and regression, outlier analysis and social network analysis.

Following subsections gives the description of each of the mentioned data mining tasks:

Characterization and Discrimination
The characterization is a summarization of the common characteristics or features of the mark class of data while Discrimination is an association of the common features of the mark class data objects beside the common features of the objects from one or more contrasting mark class [9].

Association Rule Mining
Association Rule Mining is the discovery of association rules showing attribute-value conditions that occur frequently together in a given set of data. It is the rule defined for the purpose of discovering the association between two or more various frequent items within item set. Frequent items are those which happen a no. of time higher or the equivalent to support count (a threshold).

Clustering
Cluster analysis or simply clustering is the process of partitioning a set of data objects (or observations) into subsets. Each subset is a cluster, such that objects in a cluster are similar to one another, yet dissimilar to objects in other clusters. The set of clusters resulting from a cluster analysis can be referred to as clustering [9].

Classification and Regression
Classification predicts class or category to which the item would belong to the whole in the Regression is a function that predicts a number. An effort is prepared to the model relationship between the attributes previously recognized and predictor attributes (what is predicted).

Outlier/Anomaly Analysis
Certain objects do not reflect to the share some properties of single group rather reflect properties belonging to the more than one group. Such objects are well-known as outliers and the procedure of the finding the outliers are termed as outlier analysis.

Data mining tasks can be utilized for analyzing social networks on the web and is generally known as Social Network Analysis (SNA). Following Section gives the overview of SNA in brief.

2.1 Investigative Data Mining (Idm)
Terrorist have a large spread network worldwide in order to fulfill their inhuman goals. The terrorist networks (generally referred as horizontal networks) sustain among the legitimate users (or vertical networks). As a result of this, the data associated with, the terrorist activities also get mixed with that of genuine users. However, the criminals/terrorists have certain patterns followed in order to hide their unlawful motive and achieve smooth communication.

Since criminal are secreted among the genuine users, illegal intelligence examination, therefore requires the capability to the integrate knowledge from multiple crime occurrences or even multiple sources and also regular patterns, discover about the construction, organization, process and knowledge flow in criminal networks[7].

In order to aid the law enforcement agencies and uncover the terrorist behavior N.Memon et al. [10] Defined a concept for studying terrorist networks, named as Investigative Data Mining. Investigative Data Mining (IDM) is defined as "the method which models data to the predict organization of a non-hierarchical network, conclude associations and also help in terrorist networks destabilizing" [16].

Investigative Data Mining (IDM) uses modern methods that originate from research in algorithms and artificial intelligence with the quest for interesting and understandable patterns. There are three main levels of interest: the element, group and network. The central effort of Investigative Data Mining method is to recognize important actors, crucial links, subcategories, roles, network features and so on, to solution practical questions about the terrorist organization structures [12]. The ultimate goal of the IDM is to investigate terrorist networks in order to find out who the suspicious people are and who is capable of the carrying out terrorist actions and how to destabilize them. The strength of IDM is to assist analysts and investigators [16]. Investigators or analysts use this technique to construct a network that illustrates the criminal's roles, the flow of tangible and intangible goods and information and associations among these entities. This makes IDM as an interesting study for handling covert networks. Investigative Data mining and automated data analysis techniques, hence are powerful tools for intelligence and law enforcement officials fighting against such networks [12].

IDM borrows ideas from social network analysis and the graph theory methods in the order to connect the nodes and assist law enforcement agencies to the terrorist networks disconnect [17]. In this context, social network study can offer significant knowledge of the unique characteristics of terrorist organizations, ranging from subjects of selection of terrorist nodes, network formation and flow of inhuman ideas; while the graph theory gives a number of the ideas and techniques that goals to the detect maximal subgraphs in the graph (or network) that have a various property and looses this the property by adding the another point and its relationships of subgraph [16].

Using the SNA technique and graph theory, IDM considers the network as an adjacency matrix of size n x n, where n represents the number of vertices in the network. An adjacency matrix, A is defined as the matrix with value 1 if two nodes are connected otherwise with value 0, written as:

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

Also the matrix is a symmetric matrix i.e.$A_{ij} = A_{ji}$.

3. SOCIAL NETWORKING ANALYSIS
Social Network Analysis (SNA) is a data mining technique which usually analyses the various social networks present on the web. The method is beneficially used for learning the social networks behaviors. Thus, social network study, from a data mining perspective, is also known as link analysis or link mining [4].

The Social Network Analysis uses a idea of the import measures pointing out who is central node(s) in network. It is because of this that Social Network Analysis is greatest developed method by law-enforcement agencies for the learning trends of the hidden terrorist network.

In this context, when the Social Network Analysis is applied for studying of the terrorist networks on the web then it is acknowledged as IDM (Investigative Data Mining), also known as Terrorist Network Mining. The ultimate goal of the IDM is to investigate terrorist networks in order to find out who the suspicious people are and who is capable of carrying out terrorist activities and how to destabilize them [5]. It is a technique well-defined for study of the terrorist network which is hidden that uses Social Network Analysis and Graph Theory for study. IDM offers the capability to track the criminal network more effectively and also to analyze the interaction patterns within the network. The method discovers

the greatest promising node(s) within network and the aim is to eliminate this node(s) from the network in the order to the neutralize the network activities.

IDM is recognized as a grouping of the mining and subject-based automated data analysis methods where data mining serves as a method which uses predictive method for discovering patterns in the dataset and also subject-based automated data study regulate models to the data for predicting the behavior, determine associations, access risk, or achieve other kinds of analysis. IDM goals to connect the dots between the individuals and map and measure complex, covert, human groups, and also organizations [6].

Because of the magnificent applicability of Social Network Analysis for analyzing network behaviour has attracted the numerous law-enforcement agencies to the use of the technique for analyzing various hidden terrorist group on the web and enforce appropriate remedies for their neutralization.

4. ANALYSIS OF TERRORIST NETWORK

For the analysis of the terrorist network, the network is discovered from the web by using approaches such as content-based detection of terrorists on the web. Whenever a terrorist network is detected, the network influential roles and the network hierarchy are uncovered using Investigative Data Mining scheme.

One way to notice terrorist action on the Web is to eavesdrop on all traffic of the Web sites associated with terrorist organizations in order to identify the accessing users based on the their IP address [9]. But the solution was not much convincing as these users do not use fixed IP addresses or URLs. Hence the law enforcement agencies tried to detect the terrorists by monitoring all ISPs traffic.
After traffic analysis, the network is preliminary studied using social network analysis (SNA) approaching. The detected terrorist network is then studied for estimating promising roles. The analysis of each node (user) is done in the network and the centrality measures are calculated respectively for each node. The main centrality measures are degrees (number of direct connections that a node has), betweenness (the ability of an individual to link to important constituencies) and closeness (a position's ability to monitor the information flow and to "see" what is happening in the network) [8].

5. DESTABILIZATION OF TERRORIST NETWORK

To understand the dynamics of covert networks, and indeed any, network we need to understand the basic processes by which networks evolve. Hence in consideration to this, terrorist network roles are discovered and accordingly destabilization is achieved.

The destabilization is attempted by execution role analysis within network. This is done generally by evaluating the efficacy of the network, serious components of the network, a suggested measure "Position Role Index" (PRI) and dependence centrality.

- Efficiency of the network, to enumerate how competently the knowledge is replaced amongst the nodes in the network.
- Critical components of a network, for discovery the measure of centrality of a node, by which the drop in the network effectiveness is estimated when that node is disabled from network.
- PRI (Position Role Index), highlighted a clear distinction between gatekeepers and followers (It is the fact that the leaders may act as a gatekeepers) [10] and depends on the efficiency of the network.
- Dependence Centrality, for discovery the node dependency on the other nodes of the network and discovery the gatekeepers/leader.

With respect to study about role, hierarchy of the determined the terrorist network. Determining hierarchy in a terrorist network is a procedure of comparing different centrality values of the various nodes to the recognize which node is more powerful, influential or the worthy to neutralize than others [11].

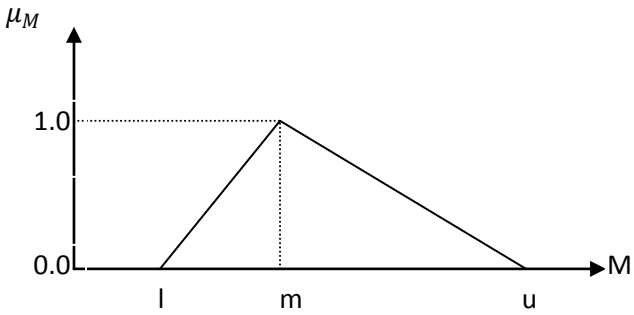
6. FUZZY SET

As one of the principal constituents of the soft computing, fuzzy logic is singing a key role in what might be called the high machine intelligence quotient (MIQ) methods. The two basic ideas within the fuzzy logic play a vital role in its applications. The first is a linguistic variable; that is, a variable whose values are sentences or words in a synthetic language or natural [12]. The other is the fuzzy if-then rule, in which the consequents and antecedent are propositions holding linguistic variables [12]. While variables in the mathematics generally take arithmetical values, in the fuzzy logic applications, the non-numeric linguistic variables are often used to the simplify expression of rules and facts [13]. For example, a simple temperature regulator that the uses a fan might look like this:

- IF temperature IS very cold THEN stop fan
- IF temperature IS cold THEN turn down fan

Fuzzy sets and fuzzy no. The theory of fuzzy set was presented by the Zadeh [14]. Fuzzy logic is multi-value logic which licenses of the intermediate values to be well-defined between the conventional ones like false / true, high / low, bad / good etc. In a standard set theory, an element may either not belong to set or belong. In fuzzy set theory, an component has a degree of membership. A degree of membership function can be defined as an interval [0, 1].

In this paper TFN (triangular fuzzy number) was used for the cyber threat computational effectiveness. A triangular fuzzy number is presented simply as (l, m, u). "l, m, u" parameter represents the minimum possible value (lower bound), mean value, the biggest possible value (upper bound) respectively [15]. μ_m is a membership function



$$\mu_M(x) = \begin{cases} 0 & x<1 \\ \frac{x-1}{m-1} & 1 \le x \le m \\ \frac{u-x}{u-m} & m \le x \le u \\ 0 & x>1 \end{cases}$$

Fuzzy Sets in Data Mining

The research in the knowledge discovery in the databases and also data mining has lead to a huge no.of proposals for a common model of process of the knowledge discovery. A recent suggestion for the such a model, which can be probable to have significant impact, since it is backed by the various big companies like DaimlerChrysler and NCR, is the CRoss Industry Standard Process for Data Mining model (CRISP-DM) [16]. The circle specifies that the data mining is essentially a circular procedure, in which the evaluation of the outcomes can trigger a re-execution of the data preparation and the model generation steps. In this procedure, fuzzy set approaches can beneficially be applied in numerous stages: The business considerate and data accepting stages are commonly strong human centered and only minute automation can be attained here. These stages serve mostly to describe the aims of the knowledge discovery scheme, to approximation its potential advantage, and to classify and assemble the necessary data. In calculation, background domain knowledge and also meta knowledge about the data is the collected. In these stages, fuzzy set approaches can be used to the formulate, for instance, the background domain knowledge in vague positions, but still in a form that can be used in the subsequent modeling stage. Furthermore, fuzzy database questions are valuable to discovery the data needed and to check whether it may be valuable to the take extra, related data into the account. In the data preparation stage, the collected data is cleaned, transformed and may be correctly scaled to create the input for the modeling methods. In this stage fuzzy approaches may, for illustration, be used to notice outliers, e.g., by fuzzy clustering the data [17, 18] and then discovery those data points that are extreme away from the cluster prototypes.

7. LITERATURE SURVEY

The very first innovative step utilizing SNA approach was put by Valdis Krebs in 2002 [2] after September 2001 attacks. Krebs used network analysis to provide an extensive analysis of the 9/11 Hijackers network. For the successful accomplishment of the study, Krebs has considered the following contributions from different researchers:

(i) Incompleteness - inevitability of the missing nodes and links that the investigators will be not uncover.

(ii) Fuzzy boundaries - regarding the decision of inclusion and exclusion of nodes in the network.

(iii) Dynamic – networks are not static but dynamic.

On the basis of the knowledge about the September 2001 attacks, Krebs framed a network consisting of terrorist nodes and evaluated the importance and the contribution of each node in the attacks. For this purpose Krebs has followed the facts and important explorations of the works of following authors

(i) Malcolm Sparrow (1991), examining the application of SNA to criminal activity.

(ii) Wayne Baker and Robert Faulker (1993), suggests looking at previously stored or known data to find the relationship data.

(iii) Bonnie Erickson (1981), explaining the importance of trusted prior contacts (that came in touch earlier) for the operative functioning of the secret society (such as terrorist groups).

Krebs during his study of terrorist networks evaluated the links in the network on the basis of their strength. The strength of the tie depends on the time spent by users together. He categorized the tie or strength on three scales:

(i) Strongest tie link reveals a cluster of network players or leaders of the group. The node pair with the strongest tie would largely be governing the group.

(ii) Moderate strength or medium thickness links reveals the nodes through which maximum transactions are done or information is forwarded.

(iii) Weak tie or the thinnest links reveal the nodes having a single transaction, or an occasional meeting and no other ties.

Using the SNA centrality measures viz. Degree, eigenvector, betweenness, closeness; Krebs evaluated the involvement of each node or used in the attacks. This beneficial step helped law enforcement agencies to detect terrorist networks more effectively. However the centrality measures are significant in the analysis, but these are the most sensitive to the little modifications in connectivity of the network [2]. After the successful analysis of the criminal network, Krebs discussed the shortcomings that were to be considered. He discussed about the difficulty faced in discovering links that may be the strongest ties, but because of their low frequency of activation, they may appear to be weak ties. The second consideration was about the network detection as the less active the network, the additional challenging it is to discover [2].

Subsequent to the study and the successful implementation of terrorist network by Krebs and discovering the importance of each node in the network, Philip Vos Fellman et al. [5] Put their efforts for the improvement of the analysis techniques. They appreciated the centrality measures to gain knowledge about the role of the nodes in the network and gave the idea about finding the important nodes in the network using social cohesion and adhesion.

They discussed that according to Moody and White, the structural cohesion would help in finding out the minimum number of nodes (actors), when removed from the group would result in disconnection of the network. Cohesion helped in determining of the subgroups in the network. Because the hub (subgroup) can become the entire group's fundamental structural weakness, the stability of the network depends upon the ability for keeping the hub hidden. Thus, cohesion is a developing property of relational pattern that contain a collection together [5].

In case of no lateral entries adhesion is applied. This is the term, whose strength shows the support of each node to hold the group together. It implies the many-to-one commitments of the individuals to the group itself or its leaders [5]. Hence a group is said to be adhesive if the members of the network are resistant from being forced to move apart as a pair of nodes. The third element of group robustness discussed was the redundancy of connections. [5].

The next beneficial and novel effort for terrorist group detection on the web was made by Y. Elovici et al. [6] In 2004. They as a group analyzed the behavior of terrorists on

the web using data mining techniques. They tried to solve the problem still faced about the dynamic switching of IP addresses and URLs by terrorist users. Hence, in place of tracking terrorists on the basis of their IP addresses, they proposed a methodology by monitoring of all the ISPs traffic to detect the users accessing the terrorists' related information, keeping in mind the privacy issues.

They have given following design goals and recommend to be fulfilled for the methodology:

(i) Training of the detection algorithm should be based on content of the present terrorist sites and recognized terrorist traffic on Web.

(ii) Detection should be carried out in the real-time. This aim can be attained only if terrorist knowledge interests are presented in the compact manner for efficient processing.

The detection sensitivity should be skillful by user-defined parameters to permit calibration of the desired detection presentation.

8. PROPOSED METHODOLOGY

This Proposed Approach is based on the reduction of the graph or network, for this fuzzy rules have been used. First, a set of fuzzy rules are prepared by training data. Then these fuzzy rules are applied on the graph, which gives a reduced graph with less no. of nodes.

Here in this approach graph optimization or reduction of graph is done by Fuzzy rules. A input graph is given with N nodes, this graph is connected graph. In the graph a node is representing a person, so each has some properties. Five properties or characteristics are considered of each node in this approach. So a database X={A,B,C,D,E} is prepared for N nodes which has five attributes corresponding to five properties.

The structure of information associated with each node is shown in Table 1.

Table 1 Structure of information associated with each node

Age	Gender	Income Level	Health Condition	Crime Record
25	M	Low	Good	Serious
36	F	High	General	No Record
20	M	High	Poor	Ordinary
56	F	Med.	Good	Ordinary

In this approach Fuzzy Rules are being prepared for optimization of network. Once fuzzy rules has been prepared then these rules is used for reduction of graph. The fuzzy rules are prepared using training dataset X, which have five attributes and one decision attributes. The Sugeno membership function is used for preparing fuzzy rules. A membership function (MF) is a curve that defines how each point in the input space is mapped to a membership value (or degree of membership) between 0 and 1. The input space is sometimes referred to as the universe of discourse, a fancy name for a simple concept.

Based on the graph obtained as an output of first phase, during the second phase, tree hierarchy is generated by applying algorithm for destabilization of Terrorist Network. The inputs for the algorithm are optimized graph (output of first phase) and centralities value. The centrality measure i.e. degree centrality measure for graph is used for destabilization of Terrorist Network.

Degree Centrality
A basic measure of SNA that turns out to be important in IDM is the degree of a node - that is, the number of other nodes directly connected to it by edges. In a graph (network) describing a terrorist network, nodes of high degree represent "well connected" people, often leaders.

Algorithm for Destabilization of Terrorist Network
The framework of the proposed algorithm is as follows:

1. Take any node n of graph G and find neighbors N
2. Take a node m such that $m \in N$
3. Compare Dcentralityof each node to its neighbor node

   If (Dcentralityof m > Dcentralityof n

   Add node m to parent set of n

   Else if (Dcentralityof m < Dcentralityof n)

   Add node m to children set of n

   Else

   Ignore the link
4. After calculating the Parent and Children sets, find the hierarchy.
5. If a node has no parent, add root of tree T as its parent and mark n as children of root.
6. For Parent set with one value, node is the child of that set value node.
7. For node with Parent set with more than one value, maximum $[N(P1) \cap N(n)]$ is estimated and the parent node with maximum value is set as parent of a node. For $N(P1) \cap N(n) = 0$, node is overlooked.
8. Even then the Parent set has multiple values the node is attached to root.
9. Repeat steps 1-2 and steps 5-8 for all nodes of graph G
10. Draw tree T

9. EXPERIMENTAL RESULTS

For testing the usefulness of developing an optimization mechanism, experimentation has been performed using Matlab (version R2012a). For experimental purposes, synthetic dataset (containing 60 nodes and connections between them) has been utilized as shown in fig. 1. The graph/ Social network corresponding to consider dataset. In the graph each node is assigned with certain weights such as age, gender, health condition, income level and crime record. Fuzzy rules are used to optimize the graph so that the graph contains only the set of potential nodes.Reduced or optimized graph contains 15 nodes as depicted in the fig 2.

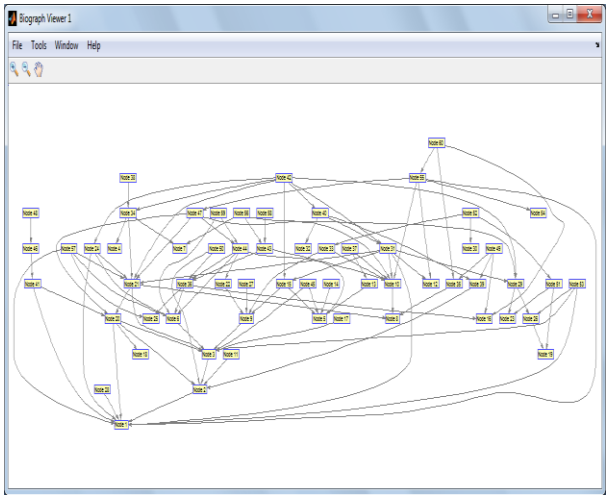


Fig.1 Graph representing 60 nodes with connections between them

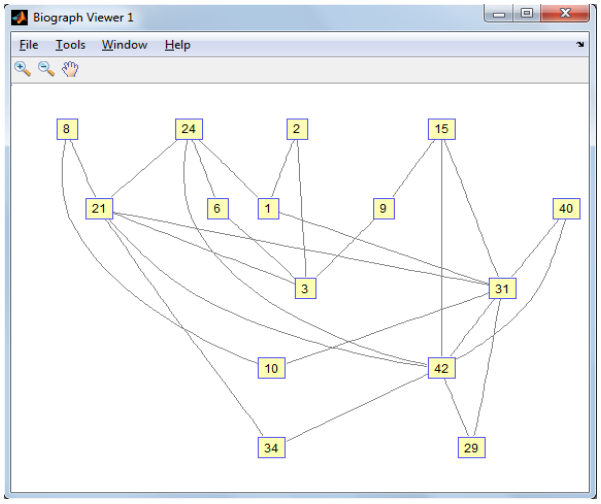


Fig2. Reduced /optimized graph containing 15 nodes.

With the hhierarchy of tree generated the crucial node among the reduced graph can be identified. The output obtained after accesing the algorithm could be visualized through fig 4.

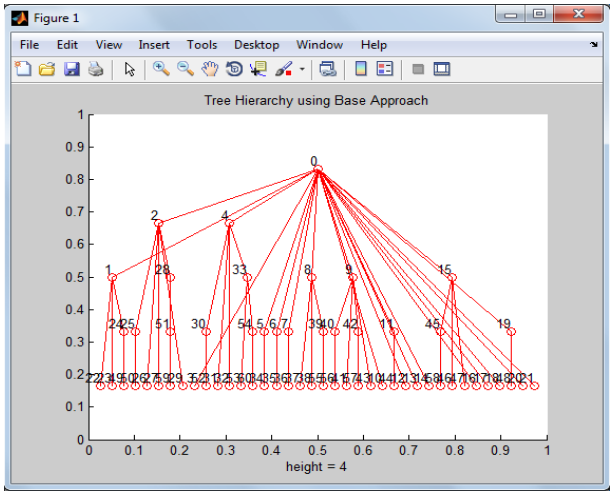


Fig 3. Hierarchy of Tree generated without optimization of graph.

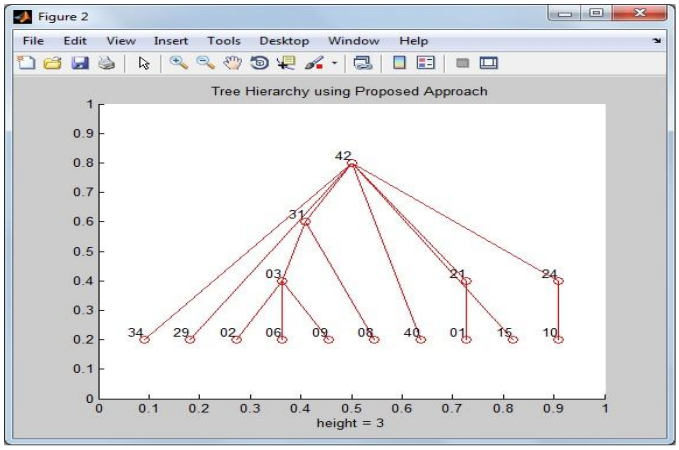


Fig 4. Hierachy obtained after applying algorithm on reduced/ optimized graph.

The comparison of execution time of algorithms (without optimization and with optimization) is shown in fig 5.

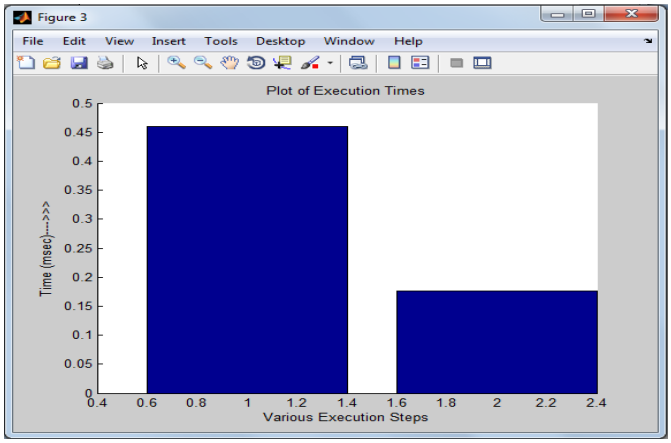


Fig 5. Execution time of algorithms in milliseconds

10. CONCLUSION

This study proposes a fuzzy rule based the cyber indicator that warns administrators of a system for probable the cyber threats. It has been found that the works of the system well when useful with a particular cyber threat scenario. This simplifies particular warning signals produced by the rules. The model's aim is not to protect a system; however, its goals at warning the system administrator for the expected cyber threats.

The proposed model shows its superiority in the development flexibility areas and also fast response for the cyber threats. Present paper explores the very useful aspect of social networking and focuses on the use of Fuzzy algorithm for the effective optimization of the large network. Proposed Fuzzy based optimization mechanism is efficient (in terms of accurate removal of unwanted nodes) and reveals only the potential suspicious (terrorists) nodes. This study will be helpful in offering the ease to law enforcement agencies for flexibly refining networks and concentrating in a focused direction during detection and destabilization of terrorist nodes/networks. This paper introduces a significant algorithm for destabilization of terrorist networks. The algorithm is expected as the most beneficial strategy for revealing patterns of the terrorist activities. The output obtained from experimental analysis on 26/11 dataset as already discussed

uncovers Wassi as the dominating node with maximum communication flowed through it. Hence, in view to this, the proposed algorithm can be considered as the most effective algorithm for uncovering the network hierarchy and neutralizing network activities.

11. REFERENCES

[1] Arun K. Pujari (2001), "*Data Mining Techniques*", Universities Press.

[2] Jiawei Han & Micheline Kamber (2006) *Data Mining;Concepts and Techniques*, Second Edition, MorFAn Kaufmann Publishers.

[3] Muhammad Akram Shaikh, Wang Jiaxin, (2006) "*InvestiFAtive Data Mining: Identifying Key Nodesin Terrorist Networks*".

[4] M. A. Shaikh, and W. Jiaxin, (2006), "InvestiFAtive Data Mining: Identifying Key Nodes in Terrorist Networks", Multitopic Conference, INMIC '06, pp. 201-207 IEEE 2006.

[5] U. K. Wiil, N. Memony, and P. Karampelas, (2010), "Detecting New Trends in Terrorist Networks", In Proceedings of International Conference on Advances in Social Networks Analysis and Mining, 2010.

[6] K. M. Carley, J. ReminFA, and N. Kamneva, (2003), "Destabilizing Terrorist Networks", In Proceedings of the 8th International Command and Control Research and Technology Symposium, 2003.

[7] P. V. Fellman and R. Wright: Modeling, (2003), "Terrorist Networks - Complex Systems at the Mid-Range", In: Proceedings of Complexity, Ethics and Creativity Conference, LSE (2003).

[8] Y. Elovici, A. Kandel, M. Last, B. Shapira and O. Zaafrany, (2004), "Using Data Mining Techniques for Detecting Terror-Related Activities on the Web", In: Proceedings of Journal of Information Warfare (2004).

[9] N. Memon and H. L. Larsen, (2006), "Structural Analysis and Destabilizing Terrorist Networks", In Proceedings of The First International Conference on Availability, Reliability and Security, 2006. ARES 2006, IEEE 2006.

[10] N. Memon, H. L. Larsen, D. L. Hicks, and N. Harkiolakis, (2008), "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.

[11] L.A. Zadeh, "Outline of a New Approach to the Analysis of Complex Systems and Dccision Processes," IEEE Trans. Systems, Man and Cybmzetics, pp. 28-44.

[12] Zadeh, L. A. et al. 1996 Fuzzy Sets, Fuzzy Logic, Fuzzy Systems, World Scientific Press, ISBN 981-02-2421-4.

[13] L.A. Zadeh, "Fuzzy sets", Information Control, vol.8, pp.338-353,1965.

[14] E.H. Mamdani, and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller", Int. J. Man-Mach. Stud., vol.7, pp.1-13, 1975.

[15] P. Chapman, J. Clinton, T. Khabaza, T. Reinartz, and R. Wirth. The CRISP-DM Process Model, 1999 Available from http://www.ncr.dk/CRISP/.

[16] J.C. Bezdek, J.M. Keller, R. Krishnapuram, and N. Pal. Fuzzy Models and Algorithms for Pattern Recognition and Image Processing. The Handbooks on Fuzzy Sets. Kluwer, Dordrecht, Netherlands 1999

[17] F. H¨oppner, F. Klawonn, R. Kruse, and T. Runkler. Fuzzy Cluster Analysis. J. Wiley & Sons, Chichester, United Kingdom 1999.

[18] Maheshwari S., Tiwari A: "A Novel Genectic based Framework for the Detection and Destabilization of Influencing Nodes in Terrorist Network," Computational Intelligence in Data Mining- Vol. 1, Smart Innovation, System and Technologies 31, DOI 10.1007/978-81-322-2205-7_53, pp 573-582(2015).