CNEM: Cluster Based Network Evolution Model

SARWAT NIZAMANI*, AND NASRULLAH MEMON**

RECEIVED ON 21.08.2014 ACCEPTED ON 30.12.2014

ABSTRACT

This paper presents a network evolution model which is based on the clustering approach. The proposed approach depicts the network evolution, which demonstrates the network formation from individual nodes to fully evolved network. An agglomerative hierarchical clustering method is applied for the evolution of network. In this paper, we present three case studies which show the evolution of the networks from the scratch. These case studies include: terrorist network of 9/11 incidents, terrorist network of WMD (Weapons Mass Destruction) plot against France and a network of tweets discussing a topic. The network of 9/11 is also used for evaluation, using other social network analysis methods which show that the clusters created using the proposed model of network evolution are of good quality, thus the proposed method can be used by law enforcement agencies in order to further investigate the criminal networks.

Key Words: **Agglomerative Clustering, Communities, Cliques, Networks, Network Evolution.**

1. INTRODUCTION

There exists a number of networks in real world, which show the relationships among the members of the network. A network can be characterized by the role of its members, positions of the members, types of the members in the network and so on. Some networks are comprised of homogenous nodes (Members and nodes will be used interchangeably throughout the paper), while others may have different types of nodes. Each network describes a special kind of network, in which there are specific kinds of nodes, and they have their definite roles. For example, there may be a network of friends on a social media site, such as facebook or there may be a network of communication channels or a network of protein structure.

Apart from these networks, there also exist such terrorist networks, which need to be investigated. These are the criminal networks which are involved in the terrorist activities.

A network can be regarded as a terrorist network, which plans terrorism tactics, and potentially instigates a catastrophic incident. The members of the networks only communicate, when it is extremely indispensable. Often, the networks are evolved progressively, in the beginning there are individual members who may not have relationships among them. Afterwards, individuals make smaller groups, who take the shape of larger groups and then result in the form of a network. In this study, a network evolution model is presented, which is evaluated on a terrorist network of 9/11 incidents, a network of WMD plot against France and a

* Department of Computer Science, University of Sindh, Mirpur Khas Campus.
** The Maersk McKinney Moller Institute, University of Southern, Denmark.

network of twitter users discussing a topic. This paper proposes a CNEM (Cluster based Network Evolution Model), which uses agglomerative hierarchical clustering method for extracting evolutionary patterns of the network. The step by step process is discussed using the proposed approach, which initially determines the small groups of few members, then large groups of many members, then finally a network of all members.

We start our discussion with 9/11 network as illustrated in Fig. 1. The 9/11 network was first produced by Krebs [2] and then re-constructed by Memon, et. al. [3], with the help of iMiner prototype and its more details can be found at site (http://www.orgnet.com/tnet.html). For re-construction of the network metadata was used for every member of the network. The nodes in the network represent members of the network; while edges show the communication among the members. The network shown in Figure is comprised of 62 members and 153 communication links. The evolutionary patterns of the network are determined using CNEM, which provide details of the initiation of the formation of a network and its entire structure. Through CNEM, the systematic expansion of the network can be visualized. Even though, if the absolute network graph is available, however it would not be clear from the graph that how network was evolved? In the very beginning, the members of the network are isolated, but as soon as any kind of communication takes place among the members, the network begins to evolve. With the continuation of communication process among the network members, the evolution of the network proceeds and it persists until the objectives of the network are met. Therefore, it is foremost essential to explore the evolutionary patterns of the network for the comprehensive analysis. In the current study, we propose cluster based network evolution model which comprehensively details the network formation.

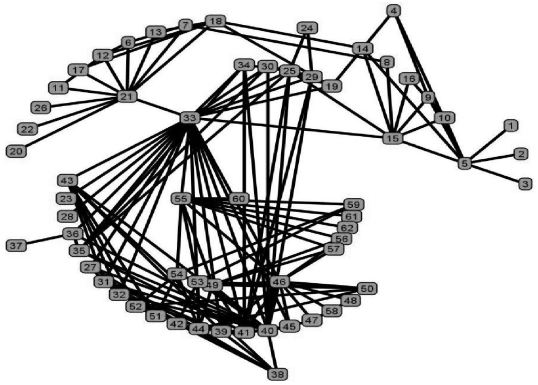

FIG. 1. THE 9/11 TERRORIST NETWORK

For clustering, the hierarchical agglomerative method is incorporated, applied and evaluated on three case studies. The detailed analysis of each case study is provided in Section 4.

In the literature clustering [4] is studied in a number of ways. The applications of clustering include: text categorization [5], information extraction and information retrieval [6], clustering in hardware and software [7] and detection of communities and evolution of networks [4] to name a few.

Apart from the 9/11 network case study, CNEM is applied on the terrorist network of WMD plot against France. Additionally, the cluster based network evolution approach is also applied on a network of social media site (twitter) users, discussing a topic. The networks and experimental analysis on these networks is discussed in Section 4.

In the literature, there are different techniques of network evolution, but CNEM provides clear evolutionary patterns, which are easy to understand and analyze. Thus, it can be argued that, CNEM provides deep understanding of the network, which is straightforward, simple to analyze and comprehend. Through CNEM, the role of the individuals in the network can be scrutinized from the start until the complete evolution of the network. With the help of CNEM, all the steps of the network evolution can easily be envisaged.

For experimentation, NetMiner3 [8] is used, which is a social network analysis tool and is used for investigative analysis of the data of the network.

The rest of the paper is organized as follows: Section 2 presents related work; whereas Section 3 discusses clustering approach to network evolution. Section 4 demonstrates experimental work; while Section 5 evaluates the model with other social network analysis techniques and Section 6 concludes the paper with future work.

2. RELATED WORK

After the unfortunate incidents of September 11, a number of researchers [4,9-11] have focused on this sensitive area of counterterrorism from different perspectives. A few researchers analyzed the terrorism plots by employing the tools of social network analysis [10]; whereas others used techniques for finding communities [4]; while a few other researchers analyzed the criminal networks to determine the key

individuals [11]. The authors [12] studied the detection of communities in social networks with the help of local information. The study also introduced few measures for detecting local community structure, which initially determine the individuals, afterwards optimize the hierarchical structure present in the community hierarchy. In this study, fusion level is used at different levels of hierarchy which visibly demonstrates the community building from scratch to the complete structure of the network. In an article [13], Ressler presented a comprehensive study of counterterrorism using social network analysis. The study describes the ways SNA may be employed in the research to combat the terrorism and also discussed the limitations of SNA in this regard. The study [14] discusses the importance of sophisticated social network analysis methods for the research in counterterrorism domain. The article [4] presents the methods of web structural mining, in order to analyze the networks. We kept into account the studies presented above and employed the techniques from social network analysis and data mining for studying the evolutionary patterns of the network. In the literature, apart from the techniques from SNA, the researcher [15] also have analyzed the electronic documents for exploring the evidences of the terrorism. In the study [16], the authors analyzed the documents by constructing the ontologies specific to the domain of counterterrorism. A group of researchers from university of Arizona, developed a project named COPLINK [17]. The aim of the project was to create knowledge management techniques which are suitable for gathering, analysis, visualization, and distribution of law enforcement concerned information in organizational and social framework. Allanach, et. al. [18] proposed ASAM (Adaptive Safety Analysis and Monitoring), which is based on HMM (Hidden Markov Model). The ASAM was aimed at detecting terrorist networks with the support of temporal suspicious blueprints present in the information, captured from distinguished sources such as: financial institutions, intelligence reports, news reports, electronic mails etc. In this study, we have only used the information on the members of the network and communication among them, which provides deeper understanding of the evolution of a network.

The evolution of the social networks is studied from different viewpoints in the literature. For instance, the authors [19] embedded the spatial behavior of the members of the network in order to study the network evolution. In an article Leskovec, et. al. [20] proposed the microscopic based social network evolution technique, which used the temporal information of the members' addition to the network. This paper employs CNEM, which is distinguishes from the rest of the methods as follows:

- CNEM is straightforward, simple to comprehend and investigate
- All the evolutionary patterns of the network can be envisioned clearly
- The behavior of the individuals members can be analyzed different levels of hierarchy from beginning to complete network evolution

3. CLUSTERING APPROACH TO NETWORK EVOLUTION

Generally, a network is consists of small and large groups of individuals called clusters. The agglomerative hierarchical clustering approach applied to the networks explores the evolutionary patterns of the network too. Initially, the members of the network are isolated, the hierarchical clustering method first computes the best cuts [22], then based on similarity among the members, small groups are formed and finally a network is constructed.

Hierarchical clustering creates a network of individuals in the evolutionary pattern, which involves the creation of sub-groups. Thus, a network is mathematically defined as:

$$N(\mathrm{M}, L) = \sum_{i=1}^{d} Cl_i(\mathrm{M}, L) \quad (1)$$

While N(M,L) represents a network which is consist of members M and links L (communication links) among the members. Cl_i(M,L) is the i^{th} sub-group (cluster) of members in the network; whereas d represents the total number of sub-groups found in the network. Every member of the network is placed in one sub-group at a time.

The network evolution model which is based on the agglomerative hierarchical clustering **Algorithm-1**, is presented in Algorithm-1. In the algorithm, in the beginning, the initialization of n clusters takes place, i.e. each member is assigned to its own cluster (line 3 and 4). The small clusters are amalgamated repetitively into large clusters of members until one cluster of all the network members is formed (lines 5-15). Merging of the clusters is performed when distance function's value is less than cutset (only those clusters are merged whose distance value is less than cutset). All the steps are demonstrated in Algorithm-1.

The proposed model applied on three case studies is described in the following section

4. EXPERIMENTAL WORK

Three case studies on which the experiments are performed include: the 9/11 network, the terrorist network of WMD plot against France (http://www.foreignpolicy.com/articles/2010/01/25/al_qaedas_pursuit_of_weapons_of_mass_destruction); and the network of users who are discussing a topic on a social media site (Twitter). The experiments on the case studies are presented in the subsequent section:

4.1 Case Study 1: Terrorist Network of 9/11 Incidents

In this section experimental analysis on the 9/11 terrorist network is presented. When hierarchical agglomerative clustering is applied on the 9/11 network, it is observed that the network evolved in 23 levels of hierarchies. Hierarchical evolution steps are illustrated using Dendrogram (Dendrogram is a diagram, which shows the hierarchical construction of clusters) in Fig. 2. Dendrogram also demonstrates all the steps of community detection in the form of clusters. The clustering approach used in this paper uses bottom-up approach, which shows the evolution of the network from individual members, then to the formation of small communities and large communities and finally construction of a network. The parameter which is used for clustering is the cutset, when dist() returns the distance among the clusters less than the cutset, clusters are merged to make the larger clusters. In the dendrogram, the fusion level is used to show the merging of clusters. The fusion (Fusion is the process of combining scattered sources into the single source) level decreases as the hierarchical levels are moved up and more clusters are combined. Table 1 shows that when fusion level is 2, there are 61 clusters in total, when fusion level decreased to 0.006, all the clusters are combined into the single large cluster, which is the network.

ALGORITHM-1

```
Agglomerative (N,M,L)//Each M is a actor or node and L is a Link
between any two members in network
//Initialize n Clusters
1.      Level = 0
2.      |C|=n//|C| total number of Cluster
3.      For (i=n)
4.              Ci=Mi
5.      While (not |C|=1)
6.              find cutset
7.                      For (each pair of clusters)
8.              if (dist(Ci,Cj)<cutset)//where dist(Ci,Cj) is a
                distance function
9.                      C = Ci,U,Cj
10.                     remove Ci
11.                     |C|=|C|-1
12.                     endif
13.             endfor
14.             Level = Level + 1
15.     Endwhile
16.     End
```

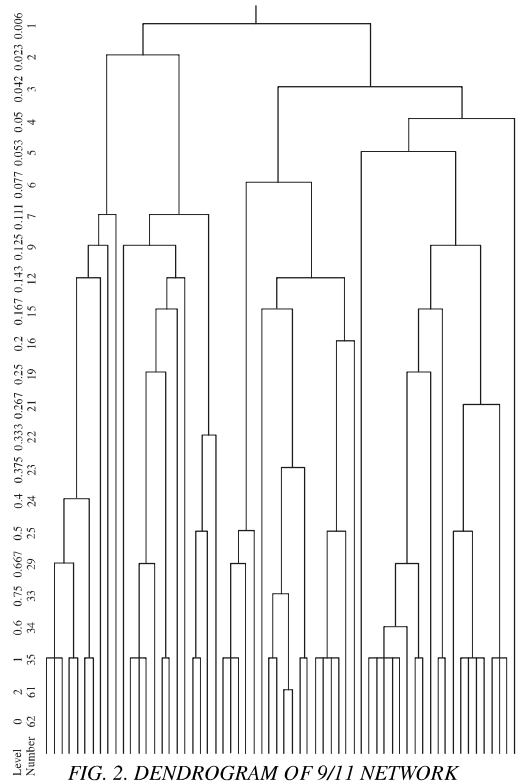

FIG. 2. DENDROGRAM OF 9/11 NETWORK

TABLE 1. LEVELS OF CLUSTERING

Level	No. of Clusters	Fusion Level	Level	No. of Clusters	Fusion Level
0	62	0	12	18	0.2
1	61	2	13	15	0.1667
2	35	1	14	12	0.143
3	34	0.8	15	9	0.125
4	33	0.75	16	7	0.111
5	29	0.667	17	6	0.077
6	25	0.5	18	5	0.053
7	24	0.4	19	4	0.05
8	23	0.375	20	3	0.042
9	22	0.333	21	2	0.023
10	21	0.267	22	1	0.006
11	19	0.25			

Fig. 2 illustrates the process of network evolution, from single member clusters to a large cluster of all the members. It is clearly shown in Figure that at lowest level of hierarchy, there are many clusters of few members; while at the highest level of hierarchy, there is a single cluster of all the members. It can also be observed that at 19^{th} level of hierarchy, there are four clusters, which are also verified from the community detection algorithms discussed in the evaluation section. The communities (clusters) detected at this level are depicted in Fig. 3.

For the sake of clarity the assignment of members to four clusters is given below:

Cluster-1: 5,9,14,4,10,15,16,1,2,3

Cluster-2: 42,44,45,46,49,53,50,54,47,56,58,59, 57,60,61,62,48,55

Cluster-3: 24,33,24,30,34,35,40,41,31,38,32,39, 43,23,27,28,36,37,51,52,29

Cluster-4: 12,21,6,7,11,18,19,8,13,17,20,22,26

The evaluation of the proposed method on the 9/11 is presented in Section 5.

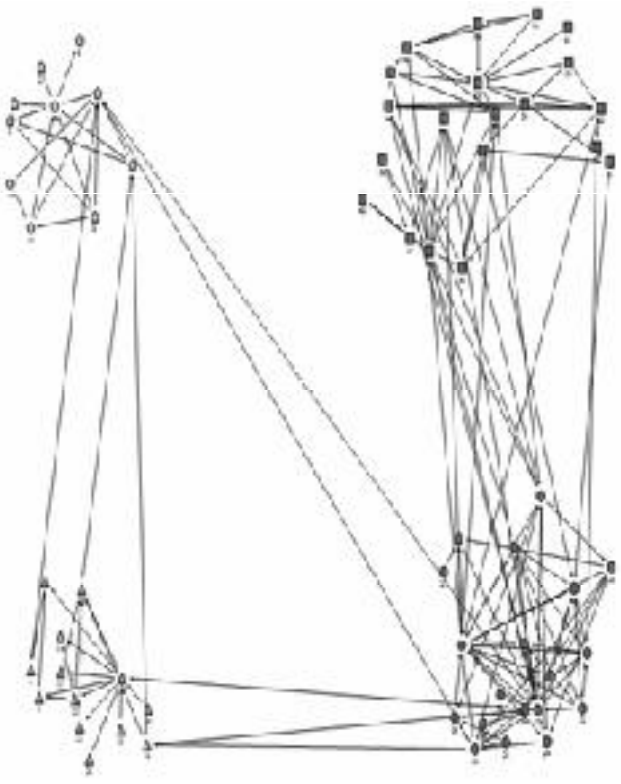

FIG. 3. FOUR CLUSTERS DETECTED AT 19^{TH} LEVEL OF HIERARCH

4.2 Case Study 2: Terrorist Network of WMD Plot against France

The other network which is considered in this case study is the terrorist network of WMD plot against France. The information about the network is collected from the different open information sources (http://www.theguardian.com/world/2004/jan/12/alqaida.france). The network is comprised of 25 nodes and 25 links, and includes people and organizations. The hierarchical structure of the network shows that the network is fully evolved in 13 levels of hierarchy. The network begins to evolve around the key nodes and the key nodes are grouped in cluster up in the hierarchy and finally a single cluster is formed, which is comprised of all the nodes in the network. Fig. 4 illustrates the hierarchical structure which shows that how the network is evolved from single node clusters to single network of all nodes.

Fig. 4 clearly shows that the network begin to evolve with the link between nodes labeled "1" and "2", which then takes a form of cluster. The other nodes also join the cluster which then becomes the largest sub-group in the network. At the same level of hierarchy other clusters also begin to evolve such as the link between the nodes "12" and "23". Beside these two large sub-groups other two small communities also begin to evolve. All of the sub-groups are then linked to form the network with the specific goal of making a WMD plot against France.

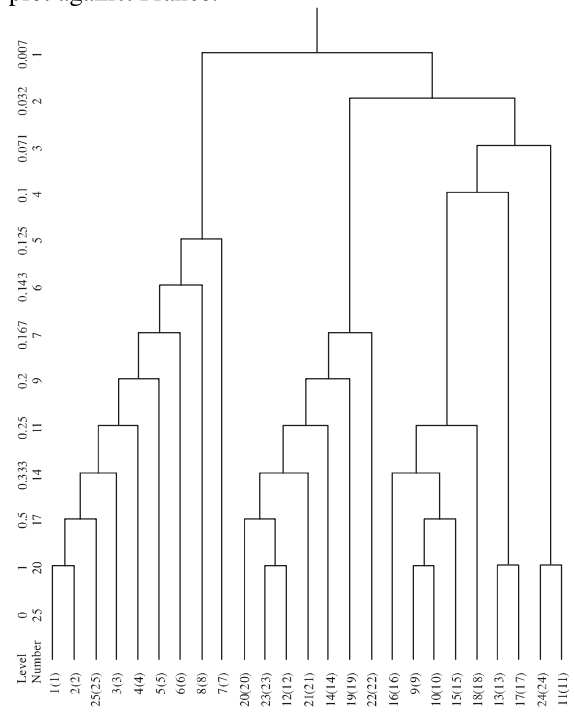

FIG. 4. HIERARCHICAL EVOLUTION OF TERRORIST NETWORK OF PLOT OF FRANCE WMD

4.3 Case Study 3: Evolution of a Network of Users Discussing a Topic on Social Media (Twitter)

In this section, a case study is presented on the network of Twitter users, who are discussing a topic. Twitter data was extracted using the R data mining tools, twitteR package. The network evolves when a specific topic is tweetted by a user, then other users start following that user on that particular tweet. In this manner, the discussion continues and takes the form of a network. The clustered evolution shows all the steps of network evolution of certain topics of interest by specific users. The network of the users discussing a particular topic is given in Fig. 5, whereas the evolution patterns of the same network are depicted in Fig. 6. The Figure shows the network of users and communities which are formed based on the discussion of the particular topic by specific users. Fig. 6 shows that at a lower level of hierarchy, small groups of those members are formed, who are directly connected to each other. Figure shows that the clusters of users created in the lower level of hierarchy have the close relationships (following tweets of each others). As the hierarchy level gets higher, the relationship gets weakened but the size of the clusters increase. At the top level of hierarchy, all the members of the clusters are grouped into one large cluster discussing the same topic (issue).

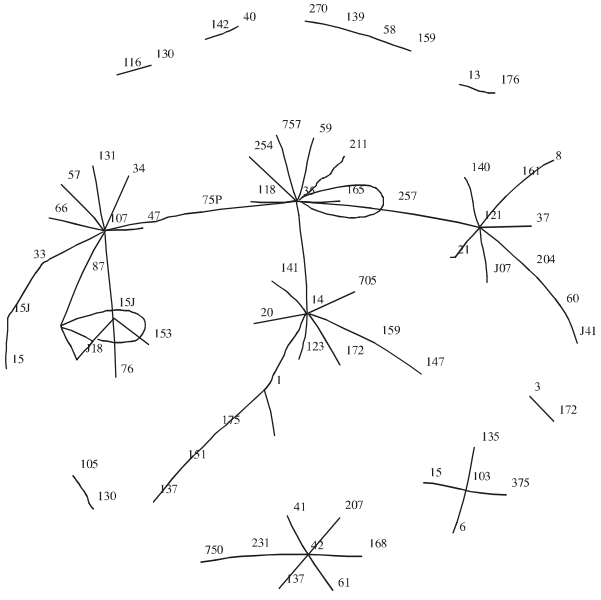

FIG. 5. NETWORK OF USERS DISCUSSING A TOPIC ON TWITTER

5. EVALUATION

In order to evaluate the model, conventional social network analysis methods are also applied on the 9/11

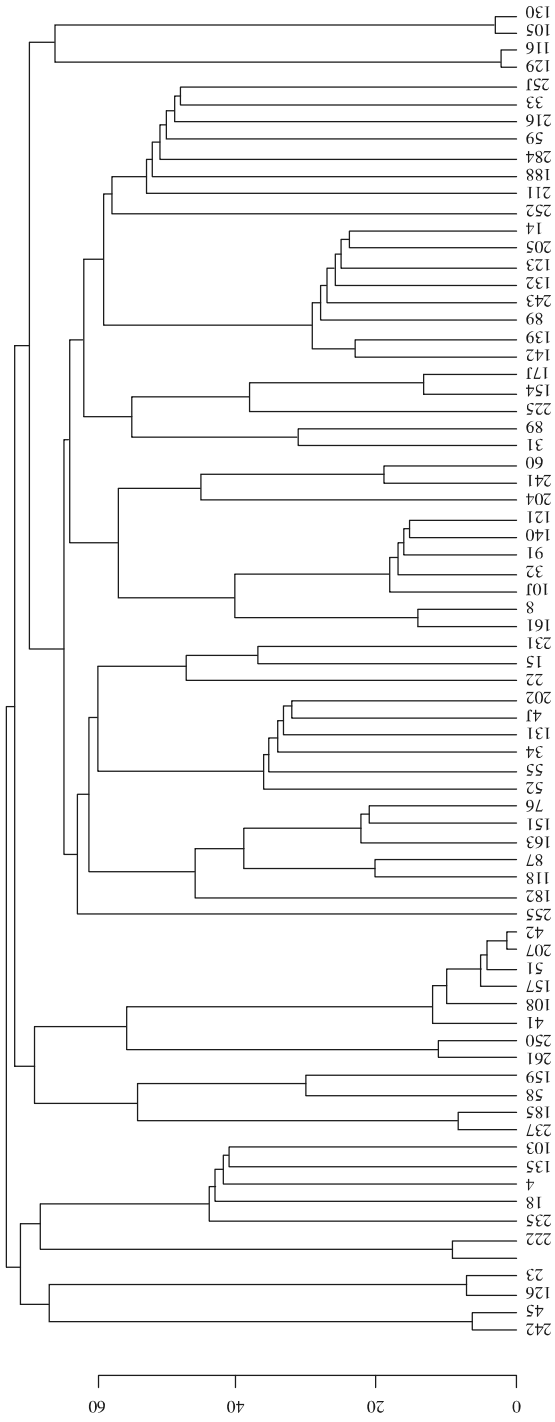

FIG. 6. EVOLUTION OF NETWORK OF USERS DISCUSSING A TOPIC ON TWITTER

network. Reason for using only the 9/11 network for evaluation is that this network is also used by other researchers in the literature.

5.1 Evaluation Using Cluster Quality Measures

For analyzing the clusters created in the process of network evolution, some cluster quality measures are often kept into account. These measures are described by Leskovec, et. al. [21], which are given as follows:

Conductance: $$f(S) = \frac{cs}{2ms + cs} \quad (2)$$

Normalized Cut: $$f(S) = \frac{cs}{2ms + cs} + \frac{cs}{2(ml - ms) + cs} \quad (3)$$

Where f(S) represents a function, which is defined on cluster S derived from network N(M,L). All of the terms of function f(S) with definitions are given as follows:

Terms	Description
S	S is a cluster (sub-group) of network N
ml	ml represent total number of links in network N
ms	ms is the total number of links in cluster S
cs	cs shows the total number of links is the number of links on the boundary of S i.e. an edge (u,v), u∈ S, v∉ S

These measures are computed on the 9/11 network and the results are given in Table 2.

In order to evaluate the quality of clusters (communities) found at 19th level of hierarchy in the 9/11 network (Fig. 2), cluster quality measures are computed, which are given in Table 2. These are the measures described by Leskovec, et. al. [21].

The study [21] suggests that the lower values of function f(S) show the good quality clusters, with the constant size of clusters. Even though the cluster size is not constant in the clusters detected using hierarchical approach, but we got clusters of good quality having low f(S) scores. The f(S) scores of all the clusters are less than 0.5, which confirm that the clusters detected during the evolution of the network are of good quality.

TABLE 2. MEASURES FOR CLUSTER QUALITY

Cluster No.	Conductance	Normalized Cut
1	0.135	0.153
2	0.172	0.3
3	0.15	0.24
4	0.14	0.165

5.2 Evaluation Using Community Detection

The 9/11 network is also analyzed using the community detection algorithm NE [23] for the evaluation purpose, and the communities detected are demonstrated in Fig. 7. The member assignment to the communities is given below, which shows that these communities are identical to the clusters detected at level 19 of the hierarchy (Fig. 2).

Community-1: 5,6,14,4,10,15,16,19,1,2,3
Community-2: 42,44,46,49,53,51,52,50,54,47,56, 58, 59, 57, 60, 61, 62, 48, 25
Community-3: 25, 33, 24, 30, 34, 35, 40, 41, 31, 38, 32, 39, 43, 23, 27, 28, 36, 45, 37, 29
Community-4: 12,21,6,7,11,18,8,13,17,20,22,26

It is observed that there is one to one correspondence of clusters to communities with only few omissions.

Another method of social network analysis is cliques detection, which detects the strong sub-groups in the network. Therefore, the proposed method for network evolution is also evaluated on 9/11 network using the cliques detection, which is described in the following sub-section.

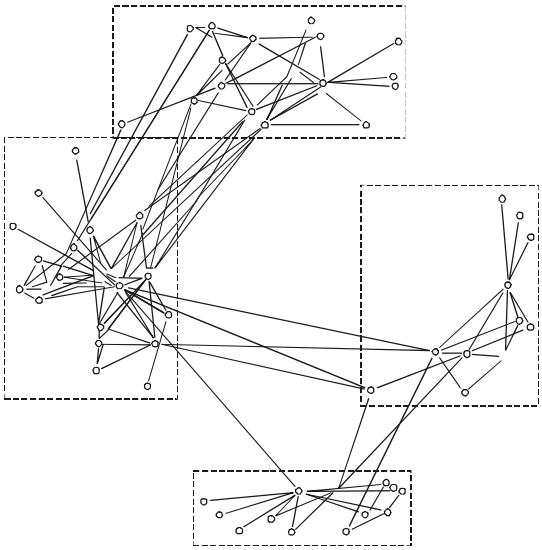

FIG. 7. COMMUNITY STRUCTURE FOUND IN THE NETWORK WITH THE HELP OF NE ALGORITHM

5.3 Evaluation using Cliques Detection

The use of cliques detection is to evaluate the CNEM, in terms of clusters created using agglomerative process and compare them with the cliques (which are the closely related sub-groups). Cliques [3] are the sub-groups in a network with close relationship, such that every member in the sub-group is directly linked to the rest of the members in the sub-group.

It is observed that, most of the cliques detected in the network are comprised of the member, which are grouped together in the hierarchical clusters and are shown in Table 3. Each column in the Table 3 shows the cliques, which correspond to particular clusters. From Table 3 it is clear that most of the cliques found are pure. Purity of a clique is defined the proportion of the cliques, in which each member is part of the same cluster. Mathematically, the purity of the cliques is computed with the help of following equation:

$$P = C/T^* 100 \quad (4)$$

While C represents the total cliques whose members are originated from same cluster, and T represents the number of all the cliques detected in the network at a particular hierarchical level. In the experiments, level 19 (Fig. 2) is considered, in which 75% of the clusters are pure clusters.

The experiments show that, even though clustering is used for analyzing network evolution, but we also get sub-groups, which include the cliques that are defined from these groups.

TABLE 3. VARIOUS CLUSTERS CONTAINING THE CLIQUES

Cluster-1	Cluster-2	Cluster-3	Cluster-4	Mix Clusters
15,9,10,50	49,44,50	33,40,41,25,35,34	12,21,6	33,40,41,45,46
9,5,4	53,54,59,55	33,40,41,25,29	12,21,11	0,39,46
14,5,15	53,54,44	33,40,30,35,25	12,21,18	33,25,19
10,15,16	47,46,45	33,40,31,27	18,21,13	33,41,44
-	47,46,58	33,30,36,35	18,21,17	14,18,19
-	47,46,48	24,25,29	-	49,46,40,41
-	56,55,62,61	34,40,31,32,39,43	-	49,46,50
-	49,46,56,57,55	38,40,31,27	-	49,44,41
-	-	-	-	51,52,54

6. CONCLUSIONS

This paper presented a cluster based network evolution model and applied on case studies of September 11 network, terrorist network of WMD plot against France and a network of users of social network twitter. The study implies that a terrorist network can well be analyzed using proposed method of network evolution. The experiments illustrate all the steps of the network evolution. It can be observed from the experiments that how individuals become the part of the network. This will help law enforcements agencies to investigate the terrorist network. The September 11 network is then evaluated on cluster quality measures, the cliques detection as well as on the community detection methods. The experiments performed on the network demonstrate that there is correspondence in the social network analysis techniques and the analysis performed using CNEM and vice versa. While detecting the cliques, it is observed that in many of the cliques, all of the cliques members are from the common cluster determined using CNEM. In the experiments, a community detection algorithm 'NE' is also applied, which shows that the clusters found using CNEM also resemble to each other. Thus, the outcome of the investigation of social networks with the assistance of detection of community using NE algorithm, detection of cliques and the agglomerative hierarchical clustering technique have much similarity, however CNEM provides detailed insight of the network on all the three case studies. One can have better visualization of the networks, which depicts all steps of formation of the network. Apart from the above discussed contributions, in the paper, there are some limitations, which is, that at the moment no temporal data of the communication links among the members is incorporated. We are intended to embed such information of the communication links, so that more exploratory patterns of the network evolution can be explored.

ACKNOWLEDGMENT

This research was conducted during the Ph.D. study of the first author, at University of Southern Denmark. This paper is an extension of our paper “Evolution of Terrorist Network using Clustered Approach: A Case Study”, European Intelligence and Security Information, IEEE Computer Society, Athens Greece, 2011.

REFERENCES

[1] Hicks, D.L., Memon N., Farley, J.N., and Rosenorn, T., "Mathematical Methods in Counterterrorism: Tools and Techniques for a New Challenge", Mathematical Methods in Counterterrorism, Springer, 2009.

[2] Krebs, V., "Mapping Networks of Terrorist Cells", Connections, Volume 24, No. 3, pp. 45-52, 2002.

[3] Memon, N., Hicks, D.L., Larsen, H.L., and Uqaili, M.A., "Understanding the Structure of Terrorist Networks", International Journal of Business Intelligence and Data Mining, Volume 2, No. 4, pp. 401-425, 2007.

[4] Falkowski, T., "Community Analysis in Dynamic Social Networks", Dissertation, University Magdeburg, 2009.

[5] Kyriakopoulou, A., "Text Classification Aided by Clustering: A Literature Review", I-Tech Education and Publishing KG, Vienna, Austria, 2008.

[6] Clustering in Information Retrieval http://nlp.stanford.edu/IR-book/html/htmledition/clustering-in-information-retrieval-1.html. Accessed on 28.05.2011.

[7] Andritsos, P., and Tzerpos, V., "Information-Theoretic, Software Clustering", IEEE Transactions on Software Engineering, Volume 31, pp. 50-165, 2005.

[8] Cyram, "NetMiner 3.3.0", Seoul, Cyram Co., Ltd., 2008.

[9] Memon, N., Larsen, H.L., Hicks, D.L., and Harkiolakis, N., "Detecting Hidden Hierarchy in Terrorist Networks: Some Case Studies", In Intelligence and Security Informatics, pp. 477-489, Springer Berlin Heidelberg, 2008.

[10] Sal, V., and Rethemeyer, R.K., "Social Network Analysis for Combating Terrorist Networks", http://www.start.umd.edu/start/research/projects/project.asp

[11] Memon, N., and Hicks, D.L., "Detecting Key Players in 11-M Terrorist Network: A Case Study", 3rd International Conference on Availability, Reliability and Security, 2008.

[12] Chen, J., Zaïane, O.R., and Goebel, R., "Detecting Communities in Social Networks Using Local Information", pp. 197-214, Springer, Vienna, 2010.

[13] Ressler, S., "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research", Homeland Security Affairs, Volume 2, No. 2, pp. 1-10, 2006.

[14] Qin, J., Xu, J.J., Hu, D., Sageman, M., and Chen, H., "Analyzing Terrorist Networks: A Case Study of the Global Salafi Jihad Network", Intelligence and Security Informatics, pp. 287-304, Springer, Berlin Heidelberg, 2005.

[15] Qureshi, A.R., Memon, N., and Wiil, U.K., "Detecting Terrorism Evidence in Text Documents", Proceedings of Social Com/PASSAT, pp.521-527, 2010.

[16] Jiang, X., and Tan, A.H., "CRCTOL, "A Semantic-Based Domain Ontology Learning System", Journal of the American Society for Information Science and Technology, Volume 61, No. 1, pp. 150-168, 2010.

[17] Chen, H., Roslin H., Homa, A., Harsh, G., Chris, B., Jennifer, S., and Linda, R., "COPLINK: Information and Knowledge Management for Law Enforcement", Proceedings of SPIE, The International Society for Optical Engineering, Volume. 4232, pp. 293-304. 2001.

[18] Allanach, J., Tu, H., Singh, S., Willet, P., and Pattipati, K., "Detecting, Tracking and Counteracting Terrorist Networks via Hidden Markov Model", IEEE Aerospace Conference, 2004.

[19] Metcalf, S., and Paich, M., "Spatial Dynamics of Social Network Evolution", 23rd International Conference of the System Dynamics Society, 2005.

[20] Leskovec, J., Backstrom, L., Kumar, R., and Tomkins, A., "Microscopic Evolution of Social Networks", Proceedings of 14th International Conference on Knowledge Discovery and Data Mining pp. 462-470. ACM, August, 2008.

[21] Leskovec, J., Lang, K.J., and Mahoney, M.W., "Empirical Comparison of Algorithms for Network Community Detection", International World Wide Web Conference Committee, pp. 631-640, 2010.

[22] Breiger, R.L., Boorman, S.A., and Arabie, P., "An Algorithm for Clustering Relational Data with Applications to Social Network Analysis and Comparison with Multidimensional Scaling", Journal of Mathematical Psychology, pp. 328-383, 1975.

[23] Wakita, K., and Tsurumi, T., "Finding Community Structure in Megascale Social Networks", Computers and Society, 2007.